



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Visto el estado que guarda el expediente de verificación citado al rubro, se procede a dictar la presente resolución, en razón de los siguientes antecedentes:

ANTECEDENTES

1. El treinta de junio de dos mil diecisiete, la otrora Dirección General de Investigación y Verificación adscrita a la Secretaría de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, acordó con fundamento en los artículos 6, apartado A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos, séptimo transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, 3, fracción XIII y primero transitorio del Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, 1, 2, fracciones I, IV y V, 3, fracción XVIII, 4, 89, fracciones I, VI y XIV, 146 y 147, último párrafo, primero y cuarto transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, segundo y octavo transitorios de la Ley Federal de Transparencia y Acceso a la Información Pública, 1, 3, fracción XI, 38 y 39, fracción I de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 1, 2, 3, fracción VIII, 5, fracción X, letra p., 29, fracciones XVI, XXX y XXXVIII, 41, fracciones I, VI, VII y IX del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; así como, 1, 2, 3, fracciones XI y XVI, 5, 7 y 52 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones, **iniciar**, de oficio, el expediente de investigación preliminar con número **INAI.3S.08.03-003/2017**:

[...]

PRIMERO. La Dirección General de Investigación y Verificación, adscrita a la Secretaría de Protección de Datos Personales, del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, es competente para dictar el presente acuerdo con fundamento en los artículos 6, apartado A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos, séptimo transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, 3, fracción XIII y primero transitorio del Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, 1, 2, fracciones I, IV y V, 3, fracción XVIII, 4, 89, fracciones I, VI y XIV, 146 y 147, último párrafo, primero y cuarto



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, segundo y octavo transitorios de la Ley Federal de Transparencia y Acceso a la Información Pública, 1, 3, fracción XI, 38 y 39, fracción I de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 1, 2, 3, fracción VIII, 5, fracción X, letra p., 29, fracciones XVI, XXX y XXXVIII, 41, fracciones I, VI, VII y IX del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; así como, 1, 2, 3, fracciones XI y XVI, 5, 7 y 52 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

SEGUNDO. *De conformidad con los hechos y elementos descritos, en relación con la presunta existencia de espionaje y ciber vigilancia a través del software (malware) identificado como "Pegasus", conforme a lo señalado en el comunicado INAI/193/17 del veintiséis de junio de dos mil diecisiete, y en cumplimiento a lo instruido por el Secretario de Protección de Datos Personales de este Instituto mediante oficio INAI/SPDP/454/17 del veintiocho del mismo mes y año, se ordena **iniciar**, de oficio, **el expediente de investigación preliminar**, de carácter mixto, con el número **INAI.3S.08.03-003/2017**, en contra de los sujetos obligados del sector público, así como las personas físicas y/o morales del sector privado que pudieran resultar con el carácter de responsables del tratamiento de los datos personales que, en su caso, se haya efectuado en el presente caso.*

TERCERO. *Con objeto de allegarse de evidencias o elementos de prueba que permitan esclarecer los hechos de conocimiento de este Instituto y, en su caso, la existencia o no de un probable incumplimiento en materia de protección de datos personales, con fundamento en los artículos 1, 2, fracciones I, IV y V, 89, fracciones I, VI y XIV, 146 y 147, último párrafo, Primero y Cuarto Transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 38 y 39, fracción I, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 5, fracción X, letra p., 29, fracciones XVI y XXX, y 41, fracciones I, VI y VII, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; 1, 3, fracción XVI, 5, y 52 a 59 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones; practíquense todas y cuantas diligencias resulten necesarias y, en el momento procesal oportuno, procédase a emitir la determinación que conforme a Derecho corresponda.*

CUARTO. *Agréguese al expediente el presente acuerdo, así como copia simple: de las 6 (seis) notas periodísticas referidas previamente; del informe titulado "GOBIERNO ESPIA. Vigilancia sistemática a periodistas y defensores de derechos humanos en México"; de la denuncia presentada el diecinueve de junio de dos mil diecisiete ante la Procuraduría General de la República; del comunicado de prensa DGC/203/17 del veintiuno de junio de dos mil diecisiete, emitido por la Comisión Nacional de los Derechos Humanos; del comunicado INAI/193/17 del*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

veintiséis de junio de dos mil diecisiete, emitido por este Instituto; así como el oficio INAI/SPDP/454/17 del veintiocho del mismo mes y año, emitido por el Secretario de Protección de Datos Personales, para todos los efectos legales a que haya lugar.

[...]

a) Adjunto al acuerdo de inicio descrito, obra:

- Comunicado INAI/193/17¹ del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado el veintiséis de junio de dos mil diecisiete:

EL INAI INICIARÁ INVESTIGACIONES POR PRESUNTOS HECHOS DE ESPIONAJE

EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES (INAI) REPRUEBA CUALQUIER TRANSGRESIÓN EN CONTRA DE LOS DERECHOS HUMANOS DE COMUNICACIÓN, INFORMACIÓN, LIBERTAD DE EXPRESIÓN, Y PROTECCIÓN DE DATOS PERSONALES Y ACTUARA EN LOS TÉRMINOS DE LEY QUE CORRESPONDAN.

COMO ÓRGANO GARANTE DE LOS DERECHOS DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, RECUERDA QUE ESTOS ÚLTIMOS DEBEN OBTENERSE Y RESGUARDARSE DE ACUERDO A LAS LEYES DE LA MATERIA Y TRATARLOS CUANDO SEA ADECUADO Y PERTINENTE Y NUNCA CON PROPÓSITOS DIFERENTES PARA LOS CUALES HAYAN SIDO OBTENIDOS.

CON EL ALCANCE DE SU COMPETENCIA, EN EL MARCO DE LAS ATRIBUCIONES Y OBLIGACIONES, EL INAI, INICIARÁ LAS INVESTIGACIONES PERTINENTES, Y EN SU CASO, LA VERIFICACIÓN OFICIOSA EN CONTRA DE LAS INSTANCIAS PÚBLICAS Y PRIVADAS QUE RESULTEN INVOLUCRADAS EN LA RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES MEDIANTE USO DE SOFTWARE MALICIOSO, PARA DETERMINAR LO QUE EN DERECHO PROCEDA.

EL INAI REAFIRMA SU COMPROMISO CON LA SOCIEDAD DE SALVAGUARDAR RIGUROSAMENTE LOS DATOS PERSONALES DE CUALQUIER PERSONA E INVITA A QUIENES SIENTAN AFECTADOS SUS DERECHOS A PRESENTAR A ESTA INSTANCIA

¹ <http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-193-17.pdf> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

SU DENUNCIA Y, EN SU CASO, A APORTAR ELEMENTOS QUE PERMITAN ENRIQUECER LA INVESTIGACIÓN.

[...]

- Seis notas periodísticas:
 - *Activistas presentarán denuncia en PGR por espionaje*, publicada el trece de febrero de dos mil diecisiete, en el portal electrónico de Animal Político².
 - *Impulsores de impuesto al refresco interpondrán denuncia ante PGR por espionaje del gobierno*, publicada el trece de febrero de dos mil diecisiete, en el portal electrónico de Proceso³.
 - *Denuncian ante PGR el espionaje a periodistas y activistas mexicanos*, publicada el diecinueve de junio de dos mil diecisiete, en el portal electrónico de Animal Político⁴.
 - *En manos de PGR, denuncia por espionaje gubernamental a periodistas y activistas*, publicada el veinte de junio de dos mil diecisiete, en el portal electrónico de Aristegui Noticias⁵.
 - *Los 5 casos de espionaje del gobierno mexicano*, publicada el veinte de junio de dos mil diecisiete, en el portal electrónico de El Economista⁶.
 - *Espionaje sin control*, publicada el veinticinco de junio de dos mil diecisiete, en el portal electrónico de Reforma⁷.

² <https://www.animalpolitico.com/2017/02/activistas-presentaran-denuncia-pgr-espionaje/> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

³ <https://www.proceso.com.mx/474246/impulsores-impuesto-al-refresco-interpondran-denuncia-ante-pgr-espionaje-del-gobierno> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

⁴ <https://www.animalpolitico.com/2017/06/pgr-espionaje-activistas-periodistas/> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

⁵ <https://aristeginoticias.com/2006/mexico/en-manos-de-pgr-denuncia-por-espionaje-gubernamental-a-periodistas-y-activistas/> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

⁶ <https://www.eleconomista.com.mx/politica/Los-5-casos-de-espionaje-del-gobierno-mexicano-20170620-0101.html> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

⁷

<https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?id=1145789&v=6&urlredirect=https://www.reforma.com/aplicaciones/articulo/default.aspx?id=1145789&v=6> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Informe *#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México*⁸, publicado el diecinueve de junio de dos mil diecisiete por R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19⁹¹⁰ y SocialTIC.
- Comunicado DGC/203/17¹¹ de la Comisión Nacional de los Derechos Humanos, publicado el veintiuno de junio de dos mil diecisiete.
- Comunicado 986/17¹² de la entonces Procuraduría General de la República, publicado el veintiuno de junio de dos mil diecisiete.
- Versión pública de la denuncia presentada ante el agente del Ministerio Público de la Federación, adscrito a la Fiscalía Especial para la atención de delitos cometidos contra la libertad de expresión, en la que diversas personas denuncian hechos perpetrados en su contra, constitutivos de delitos consistentes en la intervención de comunicaciones privadas; así como, el acceso ilícito a sistemas y equipos de informática.
- Oficio número INAI/SPDP/454/17 del veintiocho de junio de dos mil diecisiete, emitido por el secretario de protección de datos personales, dirigido al entonces director general de investigación y verificación, ambos de este Instituto, a través del cual hizo de su conocimiento lo siguiente:

[...]

⁸ <https://r3d.mx/2017/06/19/gobierno-espia/> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

⁹ Oficina para México y Centroamérica.

¹⁰ <https://articulo19.org/wp-content/uploads/2017/06/Reporte-Gobierno-Espi%CC%81a-Final.pdf> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

¹¹ http://www.cndh.org.mx/sites/all/doc/Comunicados/2017/Com_2017_203.pdf vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.

¹² <https://www.gob.mx/pgr/prensa/pgr-abre-carpeta-de-investigacion-por-delitos-intervencion-de-comunicaciones-privadas-y-acceso-ilicito-a-sistemas-y-equipos-de-informatica> vínculo consultado el veintitrés de enero de dos mil dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Como es de su conocimiento, con fecha 26 de junio de 2017 este Instituto emitió el comunicado número INAI/193/17 en el que se informó que en el marco de su respectiva competencia y conforme a sus atribuciones y obligaciones, iniciaría las investigaciones pertinentes, y en su caso, la verificación oficiosa en contra de las instancias públicas y privadas que resulten involucradas en el presunto tratamiento de datos personales mediante el uso de un programa malicioso, a efecto de determinar lo que en derecho proceda.

Lo anterior, motivado por una serie de presuntos acontecimientos en los que se ha señalado que diversas instancias del Gobierno Federal han utilizado un programa malicioso para tener acceso a información personal, de un conjunto de particulares, sin que se tenga certeza sobre la observancia de los mecanismos constitucionales y legales establecidos al efecto para que las instancias gubernamentales realicen este tipo de actividades.

Es por ello, que a partir de lo manifestado en el comunicado número INAI/193/17, le instruyo para que inicie una investigación con la finalidad de que este Instituto se allegue de elementos para determinar si resulta factible iniciar un procedimiento de verificación, en su caso, que permita corroborar si efectivamente alguna instancia del Gobierno Federal incurrió en alguna situación que hubiera podido contravenir el marco jurídico aplicable, en el ámbito federal, en materia de protección de datos personales.

Considerando que a la fecha del presente documento no se cuenta con denuncias presentadas ante este Instituto y apenas se iniciaría alguna actividad de colaboración con otras instancias gubernamentales, que permita a este Instituto tener certeza sobre la temporalidad de los hechos presuntamente ocurridos, le solicito que inicie dos procedimientos de investigación, uno teniendo como sustento lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento, los Lineamientos de Protección de Datos Personales, el Reglamento Interior de Interior del Instituto Federal de Acceso a la Información y Protección de Datos y demás disposiciones que resulten aplicables al caso, y, otro, fundando su actuación en lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Lo anterior, con fundamento en lo establecido en los artículos 33, 34, 37, fracciones IX y XIX, 63 y 64 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, primero, cuadragésimo tercero, cuadragésimo cuarto de los Lineamientos de Protección de Datos Personales, artículo 24, fracción VIII, XIX y XXV del Reglamento Interior de Interior del Instituto Federal de Acceso a la Información y Protección de Datos, así como en lo establecido en los artículos 89 fracciones I, VI, VII, VIII, XIV, XXX, XXXIV y XXXVII, 146, 147, 148, 149, 150, 151, 163, 164, 165 y 167 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y artículo 25, fracciones XXI y XXIV del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

A partir de las investigaciones que desarrolle, será posible para este Instituto determinar si los presuntos acontecimientos son materia de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental o de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, si los presuntos acontecimientos forman parte ámbito material de validez de las leyes citadas, si son imputables a alguna dependencia, entidad u órgano del Estado mexicano, así como las consecuencias jurídicas que correspondan en el ámbito de la legislación federal en materia de protección de datos personales.

Entre los órganos del Estado mexicano que han realizado pronunciamientos oficiales se encuentra la Comisión Nacional de los Derechos Humanos y la Procuraduría General de la República.

La Comisión Nacional de los Derechos Humanos, en su comunicado número 207/2017, de fecha 23 de junio de 2017, reitero la necesidad de que la Procuraduría General de la República realice una investigación pronta, objetiva, integral imparcial que permita determinar si los actos que se señalan efectivamente se realizaron; precisar los responsables de los mismos, así como el destino o uso que se dio a la información que, en su caso, se hubiera obtenido. Asimismo, señaló la apertura de un expediente sobre este caso, así como solicitará a las dependencias e instancias señaladas como responsables la información que le permita realizar, en el ámbito de la protección y defensa de los derechos fundamentales, una investigación puntual sobre las posibles violaciones de derechos humanos que se hubiesen verificado para emitir, en su oportunidad, el pronunciamiento que corresponda.

Por su parte, la Procuraduría General de la República, en su comunicado 1006/17, de fecha 26 de junio de 2017, se manifestó sobre la importancia que representa para la Procuraduría General de la República el que equipos de telefonía de periodistas y defensores de derechos humanos hubieran sido intervenidos -en sus comunicaciones privadas, así como accesados de manera ilícita a sistemas y equipos de informática-, lo cual ha dado como resultado que se desarrolle una investigación ministerial. Asimismo, se informó que todas las medidas cautelares que le fueron solicitadas por parte de la Comisión Nacional de los Derechos Humanos ya han sido cumplidas, desde el 24 de junio. Aunado a lo anterior indica que los hechos vertidos en la prensa son serios y que agotará las líneas de investigación a efecto de asegurar que las y los periodistas y defensores de derechos humanos en México puedan ejercer su profesión de manera libre y con todas las garantías que la ley les otorga.

Considerando que la Comisión Nacional de los Derechos Humanos y la Procuraduría General de la República han dejado constancia pública y oficial de contar con elementos vinculados al caso de referencia, para efectos de atender la instrucción dictada, le solicito que inicie las actividades de colaboración institucional a que haya lugar, con ambas instancias, para el mejor desarrollo de la investigación requerida.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Teniendo en cuenta que en el comunicado número INAI/193/17 también se señaló que este Instituto promoverá la rendición de cuentas y la transparencia de oficio y proactiva sobre toda información relacionada con los contratos y operaciones en la adquisición de cualquier sistema o equipo de software en los términos de la ley aplicable, le solicito que inicie las actividades de colaboración que corresponda con las unidades administrativas competentes de este Instituto, para el mejor desarrollo de la investigación requerida.

[...]

2. Mediante el oficio número **INAI/SPDP/DGIV/1380/17** del treinta de junio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de tecnologías de la información de este Instituto, lo siguiente:

[...]

Hago referencia a las diversas notas periodísticas publicadas en días pasados, las cuales refieren la presunta existencia del espionaje y ciber vigilancia por parte del Gobierno Federal de los Estados Unidos Mexicanos, a través del software (malware) identificado como "Pegasus" del fabricante NSO Group Technologies Ltd., entre las cuales se encuentran, de manera enunciativa más no limitativa, las siguientes:

- *"Activistas presentarán denuncia en PGR por espionaje", publicada el trece de febrero de dos mil diecisiete, en el sitio web "Animal Político".*
- *"Denuncian ante PGR el espionaje a periodistas y activistas mexicanos", publicada el diecinueve de junio de dos mil diecisiete, en el sitio web "Animal Político".*
- *"En manos de PGR, denuncia por espionaje gubernamental a periodistas y activistas", publicada el veinte de junio de dos mil diecisiete, en el sitio web "Aristeguinoticias".*
- *"Impulsores de impuesto al refresco interpondrán denuncia ante PGR por espionaje del gobierno", publicada el trece de febrero de dos mil diecisiete, en el sitio web "Proceso".*
- *"Los 5 casos de espionaje del gobierno mexicano", publicada el veinte de junio de dos mil diecisiete, en el sitio web "El Economista".*

En ese sentido, el veinticuatro de agosto de dos mil dieciséis, los investigadores del Citizen Lab de la Universidad de Toronto documentaron el método de infección del malware "Pegasus", En términos generales, se indica que el modus operandi de la infección consiste en el envío de un mensaje SMS (short message service – servicio de mensajes cortos) al objetivo con un texto que busca engañarlo, mediante el uso de técnicas de ingeniería social, para hacer clic en un enlace adjunto.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Asimismo, el diecinueve de junio de dos mil diecisiete la "R3D: Red en Defensa de los Derechos Digitales", junto con "ARTICLE 19", oficina para México y Centroamérica, y "Social TIC", presentaron el informe #GobiernoEsplá en el cual se documentan 76 (setenta y seis) supuestos intentos de infección utilizando el software malicioso "Pegasus", en contra de periodistas y defensores de derechos humanos en México, entre enero de dos mil quince y julio de dos mil dieciséis.

De igual forma, el veinticinco de junio de dos mil diecisiete, se publicó en el sitio web del periódico "Reforma", una nota de prensa con el encabezado "Espionaje sin control", en la cual se hace referencia a los hechos descritos previamente en relación con el uso del malware "Pegasus".

Aunado a lo anterior, el veintiséis de junio de dos mil diecisiete, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales emitió el comunicado INAI/193/17 con el encabezado "EL INAI INICIARÁ INVESTIGACIONES POR PRESUNTOS HECHOS DE ESPIONAJE, en el cual se señala que, en el marco de las atribuciones y obligaciones, este Instituto iniciaría las investigaciones pertinentes en contra de las instancias públicas y privadas que resultaran involucradas en la recolección y tratamiento de datos personales mediante la utilización de software malicioso.

Al respecto, cabe señalar que, de la lectura a los documentos de referencia, se desprende que los hechos descritos, presumiblemente, pudieron haber ocurrido durante dos mil quince y dos mil dieciséis; por tal motivo, es indispensable precisar que, en términos de lo dispuesto por los artículos 6, apartado A, fracción VIII, párrafos primero y cuarto, de la Constitución Política de los Estados Unidos Mexicanos; este Instituto es el organismo constitucional autónomo competente para garantizar el derecho a la protección de datos personales en posesión de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, así como de cualquier persona física y/o moral de carácter privado que lleve a cabo el tratamiento de datos personales.

Del mismo modo, en el artículo Segundo Transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, se dispuso que el Congreso de la Unión debía expedir la Ley General del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, así como las reformas correspondientes al Código Federal de Instituciones y Procedimientos Electorales, la Ley General del Sistema de Medios de Impugnación en Materia Electoral y



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

demás ordenamientos necesarios en un plazo de un año contado a partir de la publicación del referido Decreto.

*En ese sentido, el veintiséis de enero de dos mil diecisiete se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, misma que **entró en vigor el veintisiete de enero de dos mil diecisiete**, derogando todas aquellas disposiciones en materia de protección de datos personales, de carácter federal, estatal y municipal que contravengan dicho ordenamiento, de acuerdo lo establecido en sus artículos Primero y Cuarto Transitorios.*

*Por tal motivo, no debe pasar desapercibido que de la lectura integral a las diversas notas periodísticas mencionadas en el presente oficio, se desprende fundamentalmente que **los hechos** relatados que, en su caso, podrían estar relacionados con algún incumplimiento en materia de protección de datos personales, **presuntamente ocurrieron durante dos mil quince y dos mil dieciséis**; sin embargo, podría tratarse de actos u omisiones de tracto sucesivo que pueden continuar teniendo efectos con posterioridad a la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (**veintisiete de enero de dos mil diecisiete**).*

*Consecuentemente, atendiendo a la temporalidad en que probablemente ocurrieron los hechos relatados (**dos mil quince y dos mil dieciséis**) y considerando que podría tratarse de actos u omisiones de tracto sucesivo, con la finalidad de evitar cualquier tipo de vulneración al principio de irretroactividad de la ley, previsto en el artículo 14, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos, se estima que, en el presente expediente de investigación, resulta procedente aplicar el marco jurídico en materia de protección de datos personales que se encuentra vigente actualmente, es decir, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*Por tal motivo, sin prejuzgar sobre la probable comisión o no de las conductas referidas en las notas periodísticas de mérito y con la finalidad de que este Instituto se allegue de elementos para determinar si resulta factible iniciar un procedimiento de verificación, en su caso, que permita corroborar la existencia de alguna contravención al marco jurídico aplicable en materia de protección de datos personales, hago de su conocimiento que mediante acuerdo del treinta de junio de dos mil diecisiete, se ordenó iniciar, de oficio, el expediente de investigación preliminar, de carácter mixto, con el número **INAI.3S.08.03-003/2017** en contra de los sujetos obligados del sector público, así como las personas físicas y/o morales del sector privado que pudieran resultar con el carácter de responsables del tratamiento de los datos personales que, en su caso, se haya efectuado en el presente caso, al considerar que podría desprenderse un probable incumplimiento en materia de protección de datos personales.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En ese sentido, con fundamento en los artículos 6, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos; Séptimo Transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia; 3, fracción XIII, del Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública; 1, 2, fracciones I, IV y V, 3, fracción XVIII, 4, 89, fracciones I, VI y XIV, 146 y 147, último párrafo, Primero y Cuarto Transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Segundo y Octavo Transitorios de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 3, fracción XI, 38 y 39, fracción I, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 1, 2, 3, fracción VIII, 5, fracción X, letra p., 29, fracciones XVI, XXX y XXXVIII, y 41 fracciones I, VI, VII y IX, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; 1, 2, 3, fracciones XI y XVI, 5, 7 y 52 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- 1. Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*
- 2. Sírvase remitir un informe en el que se describa en que consiste, como opera el software (malware) identificado como "Pegasus", así como las afectaciones e implicaciones que puede ocasionar a los dispositivos afectados.*
- 3. Describa cuáles son los alcances e implicaciones del uso del software (malware) identificado como "Pegasus"; precisando si a partir de su operación es posible tener acceso, extraer y utilizar la información y/o datos personales contenidos en los dispositivos comprometidos.*
- 4. Manifieste si a partir de la utilización del software (malware) identificado como "Pegasus", es factible llevar a cabo el tratamiento de datos personales y determinar quién es el responsable del mismo.*
- 5. Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

*Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

El requerimiento se notificó a la Dirección General de Tecnologías de la Información, el treinta de junio de dos mil diecisiete.

3. Mediante el oficio número **INAI/SPDP/DGIV/1381/17** del treinta de junio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó a la directora general de atención al pleno de este Instituto, lo siguiente:

[...]

En ese sentido, con fundamento en los artículos 6, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos; Séptimo Transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia; 3, fracción XIII, del Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública; 1, 2, fracciones I, IV y V, 3, fracción XVIII, 4, 89, fracciones I, VI y XIV, 146 y 147, último párrafo, Primero y Cuarto Transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Segundo y Octavo Transitorios de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 3, fracción XI, 38 y 39, fracción I, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 1, 2, 3, fracción VIII, 5, fracción X, letra p., 29, fracciones XVI, XXX y XXXVIII, y 41 fracciones I, VI, VII y IX, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; 1, 2, 3, fracciones XI y XVI, 5, 7 y 52 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*
2. *Mencione si algún recurso de revisión en materia de acceso a la información y/o protección de datos personales, resuelto por el pleno de este Instituto, se encuentra vinculado con información referente al uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente y el nombre del sujeto obligado en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el treinta de junio de dos mil diecisiete.

4. Mediante el oficio número **INAI/SPDP/DGIV/1382/17** del treinta de junio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó a la directora general de prevención y autorregulación de este Instituto, lo siguiente:

[...]

En ese sentido, con fundamento en los artículos [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*
2. *Remita un informe en el que se describa en qué consiste, cómo opera el software (malware) identificado como "Pegasus", así como las afectaciones e implicaciones que puede ocasionar a los dispositivos afectados.*
3. *Describa cuáles son los alcances e implicaciones en materia de protección de datos personales del uso del software (malware) identificado como "Pegasus"; precisando si a partir de su operación es posible tener acceso, extraer y utilizar la información y/o datos personales contenidos en los dispositivos comprometidos.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

4. *Manifieste si a partir de la utilización del software (malware) identificado como "Pegasus", es factible llevar a cabo el tratamiento de datos personales y determinar quién es el responsable del mismo.*
5. *Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Prevención y Autorregulación, el treinta de junio de dos mil diecisiete.

5. Mediante el oficio número INAI/SPDP/DGIV/1383/17 del treinta de junio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de protección de derechos y sanción de este Instituto, lo siguiente:

[...]

En ese sentido, con fundamento en los artículos [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*
2. *Mencione si algún procedimiento de protección de derechos y/o de imposición de sanciones, se encuentra vinculado con información referente al uso del software (malware) identificado como "Pegasus" de ser el caso, indique el número de expediente y el nombre del sujeto obligado (responsable o encargado) en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo, o bien de las documentales respectivas.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Manifieste si a partir de la información con que cuenta, es factible señalar si derivado del uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", se lleva a cabo el tratamiento de datos personales y se puede determinar quién es el responsable del mismo.*
4. *Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

*Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Dirección General de Protección de Derechos, el treinta de junio de dos mil diecisiete.

6. Mediante el oficio número **INAI/SPDP/DGIV/1389/17** del treinta de junio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al secretario de acceso a la información de este Instituto, lo siguiente:

[...]

En ese sentido, con fundamento en los artículos [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- *Toda vez que de conformidad con lo previsto por el artículo 70, fracciones XXVII y XXVIII de la Ley General de Transparencia y Acceso a la Información Pública, los sujetos obligados deben poner a disposición del público y mantener actualizada la información relacionada con las contrataciones que lleven a cabo, en donde desde luego queda involucrado lo relacionado con adquisiciones de cualquier sistema o equipo de software; es que de conformidad con las atribuciones que el Artículo 24 fracciones II y XVIII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, confieren a esa Secretaría de Acceso a la Información*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

*a su digno cargo, le solicito atentamente tenga a bien proporcionar un informe en el que, a partir de la información disponible en el Sistema de Portales de Obligaciones de Transparencia -SIPOT- se identifiquen los **contratos o cualquier instrumento jurídico, mediante los cuales, cualquier dependencia de la Administración Pública Federal y de manera específica, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Gobernación; por sí o por conducto del Centro de Investigación y Seguridad Nacional y la Procuraduría General de la República, hubieren celebrado para la adquisición de software de espionaje -spyware- y/o geolocalización, con la empresa NSO Group.***

Al corresponder a información que debe estar en disponible en el Sistema de Portales de Obligaciones de Transparencia -SIPOT-, no se limita la temporalidad de búsqueda, por lo que mucho agradeceré se tenga a bien proporcionar todas las referencias que se localicen en relación con el tema antes referido.

- Ahora bien, en el supuesto de que posterior a la búsqueda en comentario, se advierta que los datos relacionados con los contratos celebrados para el objeto que se precisa en el punto anterior, no se encuentren disponibles en el Sistema de Portales de Obligaciones de Transparencia -SIPOT-, agradeceré que, en el ámbito de sus atribuciones, se sirva formular los requerimientos correspondientes a la **Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Gobernación; el Centro de Investigación y Seguridad Nacional y la Procuraduría General de la República, a efecto de que dichas dependencias del Ejecutivo Federal, remitan a este Organismo Garante, la información en comentario.***

*Para tal efecto, mucho agradeceré la información en comentario se pueda proporcionar en un término de **cinco días hábiles**, contados a partir del día hábil siguiente de la notificación del presente. Lo anterior, con la finalidad de que esta Dirección General a mi cargo, se encuentre en posibilidades de ejercer sus facultades de investigación.*

[..]

El requerimiento se notificó a la Secretaría de Acceso a la Información, el tres de julio de dos mil diecisiete.

7. Mediante el oficio número **INAI/SPDP/DGIV/1392/17** del tres de julio de dos mil diecisiete, en alcance al oficio número **INAI/SPDP/DGIV/1389/17** del treinta de junio de dos mil diecisiete descrito en el **antecedente 6**, la entonces Dirección General de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Investigación y Verificación informó al secretario de acceso a la información de este Instituto, lo siguiente:

[...]

En alcance al similar de número INAI/SPDP/DGIV/1389/17, entregado a esa H. Secretaría a su digno cargo el día tres de julio del año en curso, por virtud del cual se le solicita:

[...]

A este respecto, con el objeto de precisar los alcances de la atenta solicitud previamente citada, mucho agradeceré que la búsqueda de la información considere como parámetro, la adquisición del software PEGASUS por parte de cualquier instancia del Gobierno Federal, celebrado con cualquier empresa; esto es, sin restringirlo a las contrataciones celebradas, en su caso, con NSO Group.

[...]

Para tal efecto, mucho agradeceré la información en comento se pueda proporcionar en un término de cinco días hábiles, contados a partir del día hábil siguiente de la notificación del presente. Lo anterior, con la finalidad de que esta Dirección General a mi cargo, se encuentre en posibilidades de ejercer sus facultades de investigación.

[...]

El alcance se notificó a la Secretaría de Acceso a la Información, el tres de julio de dos mil diecisiete.

8. El tres de julio de dos mil diecisiete, el subdirector de verificación del sector público B, adscrito a la entonces Dirección General de Investigación y Verificación, emitió una constancia a través de la que se constató la consulta de cinco direcciones electrónicas¹³,

¹³ <http://www.iedf.org.mx/ut/ucs/INFORMA/septiembre16m/INFOM120916/K7.PDF>,
<http://www.especialistas.com.mx/saiweb/viewer.aspx?file=4ejBjxeato5yStCGOR9vKg40Agpd@@fFw4ptxyISYIGPUB52qEJfCu4MpXyknA0hPGoo8YBYuycaHRAi2ylz17g==&opcion=0&encrip=1>, http://www.milenio.com/politica/pgr-arely-gomez-pegasus-espionaje-milenio-noticias_0_983302062.html,
<http://www.eluniversal.com.mx/articulo/nacion/seguridad/2017/06/29/pgr-compro-software-de-espionaje-pegasus-en-32-mdd-revela> y <http://www.proceso.com.mx/492923/revelan-contrato-demuestra-la-pgr-compro-pegasus-en-2014>.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

con la finalidad de allegarse de notas periodísticas relacionadas con los hechos materia de la investigación, las cuales se integraron al expediente.

a) Adjunto obran las siguientes notas periodísticas, las cuales se mencionan en la constancia, cuyos títulos de destacan a continuación:

- *Adquiere la Procuraduría General de la República equipo para espiar*, publicada el doce de septiembre de dos mil dieciséis, en el portal electrónico del periódico Reforma.
- *Espionaje y acoso*, publicada el veinticinco de junio de dos mil diecisiete, en el portal electrónico del periódico Reforma.
- *PGR recibió Pegasus en 2015*, publicada el veintiocho de junio de dos mil diecisiete, en el portal electrónico del periódico Milenio.
- *PGR compró software de espionaje Pegasus en 32 mdd, revela contrato*, publicada el veintinueve de junio de dos mil diecisiete, en el portal electrónico del periódico El Universal.
- *Revelan contrato que demuestra que la PGR compró "Pegasus" en 2014*, publicada el veintinueve de junio de dos mil diecisiete, en el portal electrónico de Proceso.

9. Mediante el oficio número **INAI/SPDP/DGIV/1410/17** del cuatro de julio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

En ese sentido, con fundamento en los [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique, si la Procuraduría General de la República ha tenido conocimiento de los hechos materia de la presente investigación, específicamente en relación con la presunta utilización del software (malware) identificado como "Pegasus" por parte del*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Gobierno de los Estados Unidos Mexicanos y/o cualquier persona física o moral de carácter privado.

2. *Manifieste, si la Procuraduría General de la República ha recibido alguna denuncia o querrela relativa a la presunta utilización del software (malware) identificado como "Pegasus", en contra de cualquier persona.*
3. *De ser el caso, señale quienes son las personas físicas y/o morales denunciantes, querellantes y/o víctimas, así como aquellas a quienes se atribuyen los hechos probablemente constitutivos de delito, precisando cual es el número de averiguación previa o carpeta de investigación que se haya iniciado, sirviéndose indicar el estado procesal respectivo.*
4. *Señale, en su caso, las acciones que ha llevado a cabo la Procuraduría General de la República en relación con la presunta utilización del software (malware) identificado como "Pegasus".*
5. *Asimismo, se solicita que se brinden las facilidades para que este Instituto tenga acceso a las constancias que integran la averiguación previa y/o carpeta de investigación que se haya iniciado por los hechos de mérito.*

Le agradeceré haga del conocimiento de este Instituto referido con anterioridad, en el domicilio abajo indicado, en un término mínimo de cinco días hábiles, contados a partir de que surta efecto la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el seis de julio de dos mil diecisiete.

10. El seis de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP/972/2017** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1381/17** descrito en el **antecedente 3**, indicando lo siguiente:

[...]

Al respecto, me permito hacer de su conocimiento lo siguiente, por cada punto requerido:

En este tenor, la Dirección General de Atención al Pleno manifiesta que conforme a lo dispuesto en el artículo 33, fracciones IX y XV del Estatuto Orgánico del Instituto Nacional de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Transparencia, Acceso a la Información y Protección de Datos Personales, en las que se establece que esta Unidad Administrativa tendrá entre otras, la función de turnar a las Ponencias los medios de impugnación y demás asuntos que correspondan, de conformidad con el procedimiento establecido para tal efecto; así como elaborar la estadística de los asuntos sometidos a consideración del Pleno del Instituto.

Así las cosas, respecto de los contenidos de información identificados con los números 1 y 2, esta Dirección General advierte que el único documento por medio del cual puede identificar asuntos dentro de su competencia que se relacionen con la "adquisición, posesión, uso u operación del software (malware) identificado como Pegasus, por parte de algún sujeto obligado del sector público", es la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público.

Lo anterior, debido a que esta Unidad Administrativa no conoce de algún medio de impugnación que se tramite ante sujetos obligados del sector privado, como los cualquier persona física o moral de derecho privado. Además, respecto de los medios de impugnación en materia de protección de datos personales, esta Dirección General no concentra el contenido de las solicitudes interpuestas por los particulares, sino únicamente almacena los datos de identificación de los expedientes que son turnados a las Ponencias de este Instituto.

Así las cosas, se realizó una búsqueda dentro de la base de datos referida previamente, en la que se localizaron los siguientes recursos de revisión en materia de acceso a la información vinculados con información referente al uso del software (malware) identificado como "Pegasus":

Expediente, Autoridad y Comisionado	Solicitud	Ingreso	Fecha de sesión en que se resolvió	Sentido
RRA 3762/16 PROCURADU RÍA GENERAL DE LA REPÚBLICA Oscar Mauricio Guerra Ford	<i>Los detalles de cualquier contrato y manuales de uso, relacionados con el programa de cibervigilancia "Pegasus" o similar [...] El equipo fue adquirido en 2014 y 2015.</i>	28/10/2016	07/12/2016	Confirma
RRA 4265/17 SECRETARÍA DE	<i>requiero cualquier documento (contrato, convenio, oficio, memorándum, correo electrónico, entre otros) que</i>	27/06/2017	En sustanciación	En sustanciación



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

GOBERNACIÓN (SEGOB) Areli Cano Guadiana	<i>de cuenta de la adquisición del malware pegasus, mediante el cual se está realizando espionaje</i>			
----------------------------------------------------------	-------------------------------------------------------------------------------------------------------	--	--	--

Así las cosas, la Dirección General de Atención al Pleno anexa al presente, copia simple de la resolución correspondiente al expediente RRA 3762/16, sin dejar de mencionar que el recurso RRA 4265/17 se encuentra en sustanciación a cargo de la Ponencia de la Comisionada Areli Cano Guadiana.

Resulta necesario recalcar que, dentro de las actividades competencia de esta Dirección General, no se encuentra la de llevar a cabo análisis normativo o de cualquier otro tipo del cuerpo de las resoluciones emitidas por el Pleno de este Instituto, de tal manera que la única fuente de información con la que cuenta esta Unidad Administrativa, para efectos de la atención a su requerimiento, es la base de datos previamente indicada.

Ahora bien, en cuanto al requerimiento identificado con el número 3, esta Dirección General sugiere remitir su requerimiento de información a la Dirección General de Evaluación, Unidad Administrativa que podría contar con mayores elementos que pudieran ser de su interés, conforme a lo dispuesto en el artículo 38, fracción X del Estatuto Orgánico de este Instituto, en el que se establece que entre otras funciones, tendrá la de analizar y generar reportes derivados del Sistema de Información y Seguimiento, con el objetivo de identificar el comportamiento de los sujetos obligados en materia de transparencia y acceso a la información.

Aunado a lo anterior, esta Unidad Administrativa informa que los documentos de carácter público tales como solicitudes, estudios, resoluciones, entre otros, que pudiesen ser de su interés pueden ser localizados y consultados en el Zoom, Buscador de Solicitudes de Información y Recursos de Revisión.

A través de ese buscador, es posible ubicar aquellos documentos relacionados adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus".

Para acceder al Zoom, Buscador de Solicitudes de Información y Recursos de Revisión, debe seleccionarse el apartado Acceso a Información Pública, el cual despliega un menú en el que se encuentra la opción denominada Instrumentos, en el cual se muestra el icono del Zoom.



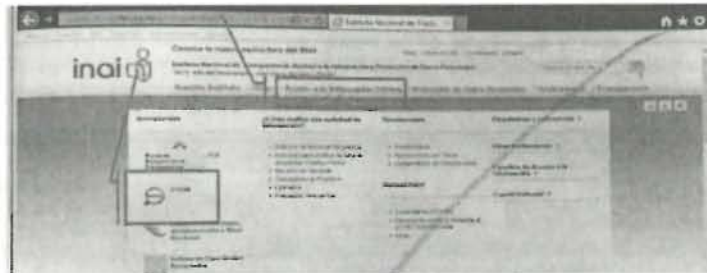
Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018



También puede accederse a dicho buscador utilizando la siguiente electrónica:
<http://buscador.ifai.org.mx/buscador/bienvenido.do>.

En cualquier caso, se muestra la siguiente pantalla:



En este sistema electrónico podría identificar mayor información a la otorgada en el presente oficio y que resulte de su interés, en razón de que permite realizar búsquedas, por palabra, de las solicitudes que se han presentado, y en su caso de recursos de revisión relacionados con el tema que nos ocupa.

[...]

- a) Adjunto, se remitió la resolución en la que se determinó **confirmar** la respuesta de la entonces Procuraduría General de la República, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el **RRA 3762/16**, el siete de diciembre de dos mil dieciséis.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

11. El seis de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SPDP/DGPDS/434/2017** de la misma fecha, emitido y signado por el director general de protección de derechos y sanción de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1383/17** descrito en el **antecedente 5**, indicando lo siguiente:

[...]

Hago referencia a sus oficios INAI/SPDP/DGIV/1383/17 y INAI/SPDP/DGIV/1387/17 de fecha 30 de junio de 2017, por medio de los cuales refiere las notas periodísticas publicadas en días pasados, respecto de la presunta existencia de espionaje y ciber vigilancia por parte del Gobierno Federal de los Estados Unidos Mexicanos, a través del software (malware) identificado como "Pegasus" del fabricante NSO Group Technologies Ltd., y por los que solicita a esta Dirección General diversa información al respecto.

En atención a lo antes señalado, anexo al presente le remito copia de los oficios INAI/SPDP/DGPDS/ds/018/17, INAI/SPDP/DGPDS/dgspd"A"/009/17 y INAI/SPDP/DGPDS/dspd"B"/009/17, correspondientes a las Direcciones de Área que conforman esta Dirección General en los que se menciona que no se cuenta con información y documentación relacionada con el tema en cuestión.

[...]

a) Adjunto a la atención al requerimiento de información se remitió:

- Oficio número **INA/SPDP/DGPDS/dspd"B"/009/17** del cuatro de julio de dos mil diecisiete, emitido por el director de sustanciación de protección de derechos "B", dirigido al director general de protección de derechos y sanción:

[...]

Me refiero a los oficios INAI/SPDP/DGIV/1383 y INAI/SPDP/DGIV/1387/17, en virtud de los cuales la Dirección General de Investigación y Verificación de este Instituto requiere información a la Dirección General de Protección de Derechos y Sanción, con respecto a diversas notas relacionadas con la presunta existencia de espionaje y cyber vigilancia a través del software (malware) identificado como Pegasus, del fabricante NSO Group Technologies Ltd.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Al respecto, informo a usted lo siguiente:

1.- *Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*

R.- No existe en los archivos de esta Dirección de Sustanciación de Protección de Derechos "B" a mi cargo, asunto alguno vinculado con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus".

2.- *Mencione si algún procedimiento de protección de derechos y/o de imposición de sanciones, se encuentra vinculado con información referente al uso de software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente y el nombre del sujeto obligado (responsable o encargado) en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo, o bien, de las documentales respectivas.*

R.- No existe en los archivos de la referida Dirección de área, ningún procedimiento de protección de derechos vinculados con información referente al uso de software (malware) identificado como "Pegasus", por lo tanto, no existen resoluciones.

3.- *Manifieste si a partir de la información con que cuenta, es factible señalar si derivado del uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", se lleva a cabo el tratamiento de datos personales y se puede determinar quién es el responsable del mismo.*

R.- No se cuenta con información relacionada con el uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", por lo que no existe información para determinar si se lleva a cabo el tratamiento de datos personales ni quién es responsable del mismo.

4.- *Remita copia simple de los documentos que acrediten la información que procede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

R. No se cuenta con información ni con documentación relacionada con el tema.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Oficio número INAI/SPDP/DGPDS/dgspd"A"/009/17 del cuatro de julio de dos mil diecisiete, emitido por el director de sustanciación de protección de derechos "A", dirigido al director general de protección de derechos y sanción:

[...]

Me refiero a los oficios INAI/SPDP/DGIV/1383 y INAI/SPDP/DGIV/1387/17, en virtud de los cuales la Dirección General de Investigación y Verificación, requiere información a la Dirección General de Protección de Derechos y Sanción, con respecto a diversas notas relacionadas la presunta existencia de espionaje y cyber vigilancia a través del software (malware) identificado como Pegasus, del fabricante NSO Group Technologies.

Al respecto, informo a usted lo siguiente:

1.- Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.

R.- No existe en los archivos de esta Dirección de Sustanciación de Protección de Derechos "A" a mi cargo, asunto alguno vinculado con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus".

2.- Mencione si algún procedimiento de protección de derechos y/o de imposición de sanciones, se encuentra vinculado con información referente al uso de software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente y el nombre del sujeto obligado (responsable o encargado) en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo o bien, de las documentales respectivas.

R.- No existe en los archivos de la referida Dirección de área, ningún procedimiento de protección de derechos vinculado con información referente al uso de software (malware) identificado como "Pegasus" por lo tanto, no existen resoluciones.

3.- Manifieste si a partir de la información con que cuenta, es factible señalar si derivado del uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", se lleva a cabo el tratamiento de datos personales y se puede determinar quién es el responsable del mismo.

R.- No se cuenta con información relacionada con el uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

"Pegasus", por lo que no existe información para determinar si se lleva a cabo el tratamiento de datos personales ni quién es responsable del mismo.

4.- Remita copia simple de los documentos que acrediten la información que procede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.

R- uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", se lleva a cabo el tratamiento de datos personales y se puede determinar quién es el responsable del mismo.

R- No se cuenta con información ni con documentación relacionada con el tema.

[...]

- Oficio número INAI/SPDP/DGPDS/ds/018/17 del cuatro de julio de dos mil diecisiete, emitido por el director de sanciones, dirigido al director general de protección de derechos y sanción:

[...]

Me refiero a los oficios INAI/SPDP/DGIV/1383 y INAI/SPDP/DGIV/1387/17, a través de los cuales la Dirección General de Investigación y Verificación, requiere información a la Dirección General de Protección de Derechos y Sanción, respecto a diversas notas relacionadas la presunta existencia de espionaje y cyber vigilancia a través del software (malware) identificado como Pegasus, del fabricante NSO Group Technologies.Ltd.

Al respecto, informo a usted lo siguiente:

1.- Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.

R.- No existe en los archivos de esta Dirección de Sanciones, asunto alguno vinculado con la adquisición, posesión, uso u operación de software (malware) identificado como "Pegasus".

2.- Mencione si algún procedimiento de protección de derechos y/o de imposición de sanciones, se encuentra vinculado con información referente al uso de software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente y el nombre del



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

sujeto obligado (responsable o encargado) en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo o bien, de las documentales respectivas.

R.- No existe en los archivos de la referida Dirección de área, ningún procedimiento de imposición de sanciones vinculado con información referente al uso de software (malware) identificado como "Pegasus".

3.- Manifieste si a partir de la información con que cuenta, es factible señalar si derivado del uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", se lleva a cabo el tratamiento de datos personales y se puede determinar quién es el responsable del mismo.

R.- No se cuenta con información relacionada con el uso de software de espionaje (spyware) y/o geolocalización, especialmente en relación con el software (malware) identificado como "Pegasus", por lo que no existe información para determinar si se llevó a cabo el tratamiento de datos personales ni quién es responsable del mismo.

4.- Remita copia simple de los documentos que acrediten la información que procede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.

R.- No se cuenta con información ni con documentación relacionada con el tema.

[...]

12. El seis de julio de dos mil diecisiete, se recibió en la entonces Dirección General de Investigación y Verificación el oficio número **INAI/SPDP/DGPA/089/2017** de la misma fecha, emitido y signado por la directora general de prevención y autorregulación de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1382/17** descrito en el **antecedente 4**, indicando lo siguiente:

[...]

Me refiero a los oficios INAI/SPDP/DGIV/1382 y INAI/SPDP/DGIV/1386/17, ambos de fecha 30 de junio de 2017, vinculados a los expedientes INAI.3S.08.03-002/2017 y INAI.3S.08.03-003/2017, mediante los cuales requiere información relacionada con el software (malware) denominado "Pegasus".

Sobre el particular, me permito informar lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En primera instancia, es importante señalar que esta respuesta se emite con base en las funciones que prevé el artículo 45 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Estatuto Orgánico del INAI para la Dirección General de Prevención y Autorregulación (DGPAR), las cuales son las siguientes:

[...]

En particular, el requerimiento se responde en ejercicio de la función establecida en la fracción XV antes citada, relativa a la elaboración de estudios y análisis técnicos en materia de autorregulación y seguridad de los datos personales, así como en lo dispuesto en la fracción XVII del artículo 29 de Estatuto Orgánico del INAI, que faculta a las direcciones generales para asesorar y emitir opiniones en los asuntos de su competencia.

Asimismo, es importante señalar que, a partir del artículo 45 antes citado, se advierte que esta unidad administrativa no cuenta con facultades de investigación, verificación o vigilancia del cumplimiento de las obligaciones en materia de protección de datos personales, que establecen la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley Federal) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General).

Dicho lo anterior, a continuación, se procede a dar respuesta a cada uno de los requerimientos realizados en los oficios señalados en el primer párrafo de este oficio:

1. Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.

Al respecto, me permito informarle que esta unidad administrativa tuvo conocimiento de la presunta existencia de espionaje y ciber vigilancia por parte del Gobierno Federal de los Estados Unidos Mexicanos, a través del uso del software (malware) identificado como "Pegasus", por medio de las mismas notas periodísticas que menciona en sus oficios INAI/SPDP/DGIV/1382/17 e INAI/SPDP/DGIV/1386/17.

No obstante, esta Dirección General de Prevención y Autorregulación, en ejercicio de sus atribuciones y competencias, no ha sido notificada oficialmente o por autoridad competente alguna, sobre hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus" por parte de algún sujeto obligado del sector público o privado.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En suma, la información que ha sido del conocimiento y a la que ha tenido acceso esta unidad administrativa es la que se encuentra disponible públicamente en los medios de comunicación que han dado a conocer y difundido los presuntos hechos vinculados con el software (malware) identificado como "Pegasus".

2. Remita un informe en el que se describa en qué consiste, cómo opera el software (malware) identificado como "Pegasus", así como las afectaciones e implicaciones que puede ocasionar a los dispositivos afectados.

Se envía como Anexo Uno de este oficio el informe solicitado, en el que se describe, a partir de información que se obtuvo de documentos y sitios de Internet de acceso abierto para el público en general, cómo opera el software (malware) identificado como "Pegasus", así como las afectaciones e implicaciones que puede ocasionar a los dispositivos afectados.

3. Describa cuáles son los alcances e implicaciones en materia de protección de datos personales del uso del software (malware) identificado como "Pegasus"; precisando si a partir de su operación es posible tener acceso, extraer y utilizar la información y/o datos personales contenidos en los dispositivos comprometidos.

De conformidad con la información contenida en el Anexo Uno de este oficio, la cual describe la forma en cómo opera el software (malware) identificado como "Pegasus", se puede advertir que a través del uso de esta herramienta se podría tener acceso, extraer y utilizar información y/o datos personales contenidos en los dispositivos comprometidos, por lo que las posibles implicaciones en materia de protección de datos personales dependerán del contexto en el que ocurra el tratamiento de los datos personales que se obtengan de los dispositivos comprometidos y del caso en concreto.

Ahora bien, es importante reiterar que la información con la que cuenta esta unidad administrativa, se obtuvo de información que está disponible públicamente en sitios de Internet y medios de comunicación, por lo que lo antes dicho se trata de una conclusión lógica que deriva de la descripción que se tiene de cómo opera el software (malware) identificado como "Pegasus", no así de pruebas periciales o de uso que se hayan aplicado de manera directa a dicha herramienta.

4. Manifieste si a partir de la utilización del software (malware) identificado como "Pegasus", es factible llevar a cabo el tratamiento de datos personales y determinar quién es el responsable del mismo.

De conformidad con lo antes expuesto, se advierte que es factible el tratamiento a partir del acceso que se podría tener a datos personales contenidos en los dispositivos comprometidos



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

por una herramienta tecnológica que opere como se dice que lo hace el software (malware) identificado como "Pegasus".

*En cuanto a quién es el responsable del tratamiento, esta unidad administrativa no cuenta con información suficiente para dar respuesta a dicho cuestionamiento, pues de conformidad con los artículos 3, fracción XIV de la Ley Federal y 3, fracción XXVIII de la Ley General, el responsable es la persona física o moral o el sujeto obligado **que decide sobre el tratamiento**, por lo que para determinar dicha figura es necesario analizar el caso concreto a fin de conocer quién está decidiendo sobre el tratamiento, y en muchas ocasiones puede haber más de un responsable.*

5. Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.

Al respecto, en el Anexo Dos del presente oficio, se envían en Disco Compacto los documentos que se citan en el Anexo Uno, de los cuales se obtuvo la información que describe cómo opera el software (malware) identificado como "Pegasus", y que son los siguientes:

- 1. Artículo 19, Red en Defensa de los Derechos Digitales y Social TIC, Tecnología Digital para el Cambio Social, Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México, junio de 2017.*
- 2. Información contenida en el sitio de Internet de The Citizen Lab, que es un laboratorio interdisciplinario con sede en la Universidad de Toronto, Canadá, el cual centra su investigación y desarrollo en la intersección de las Tecnologías de la Información y Comunicación, los derechos humanos y la seguridad global.*
- 3. The Citizen Lab, The Million Dollar Dissident: NSO Groups iPhone Zero-Days used against a UAE Human Rights Defender.*
- 4. The Citizen Lab, Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links.*

No se omite señalar que tres de los documentos antes citados están en idioma inglés, no obstante, esta unidad administrativa no cuenta con personal para realizar la traducción de los mismos al castellano, como lo solicitó en sus oficios.

No obstante, se sugiere consultar a la Dirección General de Asuntos Internacionales si cuenta con algún contrato para realizar traducciones, ya que dicha área es la que ha tenido esos contratos en años anteriores.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

a) Adjunto a la atención al requerimiento de información se remitió:

- Anexo uno, oficio número INAI/SPDP/089/2017 del cinco de julio de dos mil diecisiete, emitido por la Dirección General de Prevención y Autorregulación de este Instituto:

[...]

I. Introducción

El 19 de junio de 2017 la R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19, oficina para México y Centroamérica, y SocialTIC, presentaron el informe #GobiernoEspía en el cual se documentan 76 supuestos intentos de infección utilizando el software malicioso Pegasus, en contra de periodistas y defensores de derechos humanos en México, esto entre enero de 2015 y julio de 2016.

II. ¿Qué es Pegasus?

En agosto de 2016, Citizen Lab reveló a través de su sitio web información respecto a Pegasus, un software de vigilancia comercializado a gobiernos por la empresa israelí NSO Group, la cual se describe como una empresa líder en ciber guerra móvil y celular

La compañía, en general, mantiene un perfil bajo y hay poca información pública oficial de la misma.

NSO GROUP

NSO Group is a leader in the field of Cyber warfare. The company works with military and homeland security organizations in order to enhance their technological abilities in both the offensive and defensive cyber warfare arenas. NSO Group is backed by large organization and Israeli technology.

The company's focus is on the mobile and cellular Cyber Warfare field, where it now offers state of the art, advanced solutions.

Our offering includes coverage of the most popular handset Operating Systems, surgical activity monitoring solution exclusively for the use of Government, Law Enforcement and Intelligence Agencies.

The system introduces a powerful and unique monitoring tool, called Pegasus, which allows remote and stealth monitoring and full data extraction from remote targets devices via untraceable commands.

Figura 1. Imagen de un folleto de comercialización de NSO Group presentado por Citizen Labs

Pegasus puede clasificarse como un **software malicioso (malware) por licenciamiento**, en virtud, de que es una herramienta diseñada para infectar, monitorear, extraer información y



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

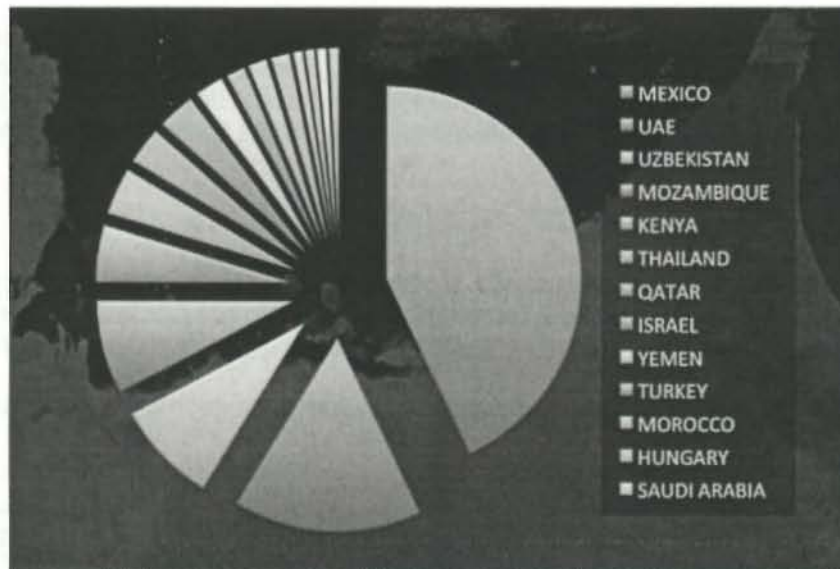
EXPEDIENTE: INAI.3S.07.01-007/2018

ganar control de dispositivos móviles, y que sólo se comercializa con gobiernos, agencias de inteligencia o de impartición de justicia.

Según reportes de *The New York Times*, referidos en #GobiernoEspía, el costo por infección exitosa se encuentra alrededor de los \$77, 000.00 USD.

Adicionalmente, *Citizen Labs* señala que México era el país donde se identificó mayor parte de la infraestructura dedicada a Pegasus, como se aprecia en la imagen:

COUNTRY THEMES IN EXPLOIT INFRASTRUCTURE NAMES



From Marczak & Scott-Railton
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE
Human Rights Defender

CITIZEN LAB 2016

Figura 2. Distribución de dominios asociados a la infraestructura de Pegasus

III. ¿Cómo funciona Pegasus?

El modus operandi de la infección es por medio de mensajes de texto SMS, en los cuales se busca que, a través de engaños, un usuario dé clic en un enlace para descargar dicho malware, como puede verse en la figura siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

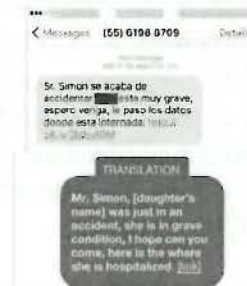


Figure 2. SMS message sent to Dr. Simon Barquera, telling him that his daughter was in a serious car accident, and to click the link to learn about the hospital.

Figura 3. Ejemplo de mensaje fraudulento con la liga de descarga para Pegasus

Si el usuario daba clic en el enlace, se daba oportunidad a Pegasus de instalarse en el dispositivo, debido a una vulnerabilidad de día cero que existía en el sistema operativo iOS de Apple.

Así, a través del malware un atacante gana acceso tanto a la información almacenada (archivos, mensajes, contactos y correos), como al control del micrófono, la cámara y a la configuración general del dispositivo móvil, como puede verse en la imagen siguiente:



Figura 4. Diagrama de datos recabados y permisos de acceso de Pegasus, presentado por Citizen Labs

- Anexo dos. Se remitieron los siguientes documentos en disco compacto:
 - *#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México*, publicado el diecinueve de junio de dos mil diecisiete por R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19 y SocialTIC.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Información contenida en el sitio de *The Citizen Lab*.
- *The Million Dollar Dissident: NSO Groups iPhone Zero-Days used against a UAE Human Rights Defender*, publicado el veinticuatro de agosto de dos mil dieciséis en el portal electrónico de *The Citizen Lab*.
- *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, publicado el once de febrero de dos mil diecisiete en el portal electrónico de *The Citizen Lab*.

13. El siete de julio de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/1410/17**, descrito en el **antecedente 9**.

14. El diez de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SE/DGTI/523/17** del siete de julio de dos mil diecisiete, emitido y signado por el director general de tecnologías de la información de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1380/17** descrito en el **antecedente 2**, indicando lo siguiente:

[...]

Me refiero al diverso INAI/SPDP/DGIV/1380/17 del treinta de junio del presente año, mediante el cual solicita se proporcione información diversa en relación al expediente de investigación preliminar, de carácter mixto, con el número INAI.3S.08.03-003/2017. Sobre el particular, con fundamento en el Artículo 48, fracciones IX y XVI del Estatuto Orgánico del Instituto. Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el Diario Oficial de la Federación el 17 de enero de 2017. a continuación, se remite la información solicitada respondiendo cada uno de los numerales en los siguientes términos:

1. *Indique si derivado de algún asunto de su competencia ha tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*

RESPUESTA: *Se informa que no he tenido conocimiento de hechos vinculados con la adquisición, posesión, uso u operación del software identificado como "Pegasus", por*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

parte de algún sujeto obligado del sector público o privado, en el ámbito de mis atribuciones y funciones en este Instituto.

2. *Sírvase remitir un informe en el que se describa en qué consiste, cómo opera el software (malware) identificado como "Pegasus", así como las afectaciones e implicaciones que puede ocasionar a los dispositivos afectados.*

RESPUESTA: *Pegasus es un software de espionaje que contiene código malicioso, procesos y aplicaciones que se utilizan para espiar, recopilar datos e informar sobre lo que hace el usuario en su dispositivo móvil. Se trata de uno de los productos más sofisticados de software de vigilancia y espionaje que existen en la actualidad. Tiene un novedoso mecanismo para instalar, ocultar y obtener persistencia en el sistema operativo del dispositivo infectado. Una vez que logra residir en el aparato de la víctima, utiliza numerosas formas de ocultar sus comunicaciones y protegerse de ser descubierto, a la vez que se conecta con un gran número de funciones del teléfono móvil con el fin de recopilar datos e interceptar mensajes de texto y llamadas telefónicas.*

EN QUÉ CONSISTE

De acuerdo con el reporte presentado por la empresa de seguridad Lookout "Technical Analysis of Pegasus Spyware - An Investigation Into Highly Sophisticated Espionage Software" que se encargó de analizar muestras, desde agosto de 2016, del programa malicioso conocido como "Pegasus", éste es catalogado como un programa de vigilancia hacia los dispositivos móviles donde es instalado, a través de la búsqueda de información contenida en el dispositivo, utilizando incluso la activación remota de los medios periféricos del propio dispositivo como micrófono y cámara. Para funcionar, "Pegasus" requiere de realizar el tratamiento conocido en la jerga técnica como "Jailbreak" o modificaciones no autorizadas sobre los dispositivos con sistema operativo iOS, de esta forma evita las restricciones impuestas por el fabricante de los dispositivos tanto de la marca Apple, para la instalación de aplicaciones que no se encuentren en sus sitios o tiendas oficiales, además el malware "Pegasus" se aprovecha de 3 vulnerabilidades o fallas en su momento desconocidas por Apple (vulnerabilidades de día 0) y solventadas a partir de la versión 9.3.5 del sistema operativo iOS.

CÓMO OPERA

El ataque se compone de tres etapas separadas que contienen tanto el software de explotación como el software de espionaje. Las etapas son secuenciales. Cada etapa es necesaria para decodificar, explotar, instalar y ejecutar la etapa posterior.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Cada etapa aprovecha una de las vulnerabilidades conocidas como Trident o trio de "Vulnerabilidades de día cero" de los dispositivos móviles de la marca Apple, para poder ejecutarse correctamente, estas vulnerabilidades son:

- CVE-2016-4657: Corrupción de memoria en el Webkit de Safari
- CVE-2016-4655: Fuga de información del Kernel KASLR
- CVE-2016-4656: Corrupción de memoria en el Kernel lleva a Jailbreak

A continuación, se describe cada una de las etapas del ataque:

ETAPA 1. Entrega y vulnerabilidad del WebKit: Esta etapa consiste en enviar la URL inicial en forma de un archivo HTML al teléfono de la víctima. Se utiliza una vulnerabilidad (CVE-2016-4657) del WebKit, utilizado en Safari y otros navegadores. Prácticamente el atacante envía una URL del sitio web, a través de un SMS, correo electrónico, medios sociales o cualquier otro mensaje o mecanismo de ingeniería social, a un equipo móvil identificado, El usuario (víctima) sólo tiene que tomar una acción "hacer clic en el enlace". Una vez que el usuario hace clic en el enlace, el software ejecuta de manera silenciosa una serie de exploits contra el dispositivo de la víctima para hacer jailbreak, en el teléfono.

ETAPA 2. Jailbreak: Esta etapa se ocupa de descargar con el código de la primera etapa, basado en el tipo de dispositivo, ya sea de 32 bits o de 64-bits, dependiendo del modelo del teléfono. En la etapa 2 se descarga software malicioso como un paquete difuso y cifrado. Cada paquete está cifrado con claves únicas para cada descarga, haciendo ineficaces los controles de seguridad tradicionales basados en la red. Contiene el código que se necesita para explotar las vulnerabilidades del kernel iOS (CVE-2016-4655 y CVE-2016-4656) y un componente de software que descarga y descifra un paquete de software para la etapa 3.

ETAPA 3. Software de espionaje: El software que activa esta etapa se descarga en la etapa 2 y también se basa en el tipo de dispositivo, ya sea de 32 bits o de 64 bits. La etapa 3 contiene el software de espionaje, daemons y otros procesos que se utilizan después de que el dispositivo ha pasado por el jailbreak en la etapa 2. La etapa 3 instala las modificaciones y cambios en las aplicaciones que el atacante desea espiar.

Adicionalmente, en la etapa 3 se detecta si el dispositivo pasó previamente por un jailbreak a través de otro método y, de ser así, elimina cualquier acceso al dispositivo que proporciona el jailbreak, como es a través de comandos SSH. El software también contiene una rutina a prueba de fallos para eliminarse a sí mismo, del equipo móvil infectado, si detecta que ciertas condiciones están presentes.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Este programa espía puede acceder y extraer mensajes de texto, llamadas telefónicas, correos electrónicos, registros y bitácoras de las aplicaciones instaladas, incluyendo, pero no limitado a las siguientes:

- Gmail
- Facetime
- Facebook
- Line
- Mail.Ru
- Calendar
- WeChat
- Surespot
- Tango
- WhatsApp
- Viber
- Skype
- Telegram
- KakaoTalk

AFECTACIONES EN EL DISPOSITIVO

Las afectaciones que se presentan en el dispositivo comprometido son las siguientes:

- *Jailbreak al kernel en el dispositivo afectado, lo que implica una transgresión a las condiciones normales de operación del equipo.*
- *Desactivación de las actualizaciones automáticas en el software del dispositivo.*
- *Con el fin de mantener su capacidad para ejecutar, comunicar y monitorear su propio estado, el software deshabilita la función de "Deep Sleep".*
- 3. *Describe cuáles son los alcances e implicaciones del uso del software (malware) identificado como "Pegasus"; precisando si a partir de su operación es posible tener acceso, extraer y utilizar la información y/o datos personales contenidos en los dispositivos comprometidos.*

RESPUESTA: *Un usuario infectado con el spyware identificado como "Pegasus" está bajo vigilancia completa por el atacante porque, además de las aplicaciones listadas arriba también espía:*

- Llamadas telefónicas



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Registros de llamadas*
- *Mensajes SMS que la víctima envía o recibe*
- *Textos que la víctima teclea en otras aplicaciones de su teléfono.*
- *Comunicaciones de audio y video que (en palabras de un fundador de NSO Group) convierten el teléfono en un "walkie-talkie".*

El acceso a este contenido podría ser utilizado para llegar a obtener, indebidamente, un mayor acceso a otras cuentas propiedad de la víctima, como aplicaciones móviles de banca electrónica, cuentas de correo electrónico y otros servicios que el usuario puede acceder mediante el dispositivo infectado o fuera de él.

En la actualidad los teléfonos móviles están estrechamente integrados en nuestras vidas personales y laborales, por lo que un sofisticado software malicioso que puede funcionar en los dispositivos sin el conocimiento del usuario, que tiene la capacidad de extraer los mensajes SMS de la víctima, los datos de contacto, registrar sus llamadas, acceder a sus registros de llamadas o activar remotamente el micrófono y la cámara de un dispositivo para captar de manera subrepticia audio y video, tiene indudablemente implicaciones en la privacidad e integridad de los datos personales de la víctima,

De lo anterior se deduce que, sí es posible tener acceso, extraer y utilizar la información y/o los datos personales contenidos en los dispositivos comprometidos.

4. *Manifieste si a partir de la utilización del software (malware) identificado como "Pegasus", es factible llevar a cabo el tratamiento de datos personales y determinar quién es el responsable del mismo,*

RESPUESTA: *Derivado de las características del software identificado como "Pegasus", mediante el cual es posible tener acceso, extraer y utilizar la información y los datos personales contenidos en los dispositivos comprometidos, se infiere que, a partir de su utilización, sí es factible llevar a cabo el tratamiento de datos personales. Sin embargo, la posible identificación del responsable para el tratamiento de datos personales que se vean afectados, derivado de la infección en los dispositivos móviles iOS por el malware "Pegasus", no puede determinarse simplemente a partir de la utilización de este software.*

5. *Remita copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

Se adjunta copia simple del documento titulado "Technical Analysis of Pegasus Spyware. An Investigation Into Highly Sophisticated Espionage Software", así como una traducción simple al español.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

- a) Adjunto a su respuesta, remitió la investigación *Technical Analysis of Pegasus Spyware. An Investigation Into Highly Sophisticated Espionage Software* realizada por Lookout y su traducción al español.

15. El diez de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SAI/0755/2017** de la misma fecha, emitido y signado por el secretario de acceso a la información de este Instituto, mediante el cual en relación con los oficios **INAI/SPDP/DGIV/1389/17** y **INAI/SPDP/DGIV/1392/17** descritos en los **antecedentes 6 y 7**, precisó siguiente:

[...]

*Me refiero a sus oficios **INAI/SPDP/DGIV/1388/17**, **INAI/SPDP/DGIV/1389/17**, **INAI/SPDP/DGIV/1391/17** e **INAI/SPDP/DGIV/1392/17**, por medio de los cuales solicitó el apoyo de esta Secretaría de Acceso a la Información para que, a partir de la información disponible en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), se identificaran los contratos o instrumentos jurídicos, celebrados entre cualquier instancia del Gobierno Federal y cualquier empresa, para la adquisición del software de espionaje -spyware- y/o geolocalización denominado PEGASUS, en virtud de las investigaciones con número de expedientes **INAI.3S.08.03-002/2017** e **INAI.3S.08.03-003/2017** que se encuentran en trámite.*

Al respecto, hago de su conocimiento que las Direcciones Generales de Enlace con sujetos obligados adscritas a esta Secretaría, se encuentran realizando una búsqueda de la información requerida en el SIPOT; sin embargo, considerando el volumen de los documentos de su interés, resulta necesario la ampliación del plazo otorgado para atender su requerimiento.

Por lo anterior, agradeceré se nos conceda una prórroga de dos días hábiles para finalizar la búsqueda respectiva y, en su caso, integrar y sistematizar adecuadamente la información que sea localizada por las Direcciones Generales de Enlace con sujetos Obligados.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

16. El diez de julio de dos mil diecisiete, el subdirector de verificación del sector público B, adscrito a la entonces Dirección General de Investigación y Verificación, emitió una constancia a través de la cual se procedió a obtener una copia simple del oficio **INAI/SPDP/DGPA/089/2017** remitido por la directora general de prevención y autorregulación de este Instituto (**antecedente 12**) y un duplicado del disco compacto anexo, puesto que únicamente se recibió un original de los mismos, los cuales fueron integrados al expediente de investigación **INAI.3S.08.03.002/2017**.

a) Adjunto a la constancia obran los documentos siguientes:

- *#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México*, publicado el diecinueve de junio de dos mil diecisiete por R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19 y SocialTIC.
- Información contenida en el sitio de *The Citizen Lab*.
- *The Million Dollar Dissident: NSO Groups iPhone Zero-Days used against a UAE Human Rights Defender*, publicado el veinticuatro de agosto de dos mil dieciséis en el portal electrónico de *The Citizen Lab*.
- *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, publicado el once de febrero de dos mil diecisiete en el portal electrónico de *The Citizen Lab*.

17. El once de julio de dos mil diecisiete, el entonces director general de investigación y verificación, emitió un acuerdo a través del cual tuvo por recibido el oficio **INAI/SAI/0755/2017** (**antecedente 15**) y otorgó al secretario de acceso a la información de este Instituto una prórroga para dar respuesta a los requerimientos formulados.

18. El once de julio de dos mil diecisiete, el entonces director general de investigación y verificación emitió el oficio **INAI/SPDP/DGIV/1465/17** a través del cual notificó al secretario de acceso a la información del Instituto, el acuerdo descrito en el **antecedente 17**.

El oficio se notificó a la Secretaría de Acceso a la Información, el once de julio de dos mil diecisiete.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

19. Mediante el oficio número **INAI/SPDP/DGIV/1482/17** del trece de julio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de asuntos internacionales de este Instituto, lo siguiente:

[...]

En ese sentido, cabe destacar que mediante oficio INAI/SPDP/DGPA/089/2017, del seis de julio de dos mil diecisiete, y por el cual Dirección General de Prevención y Autorregulación dio respuesta al requerimiento que le fue formulado a través del diverso oficio INAI/SPDP/DGIV/1382/17, expresando entre otras cosas lo siguiente:

“ ...

Al respecto, en el Anexo Dos: del presente oficio, se envían en Disco Compacto los documentos que se citan en el Anexo Uno, de los cuales se obtuvo la información que describe cómo opera el software (malware) identificado como “Pegasus”, y que son los siguientes:

...
2.

Información contenida en el sitio de Internet de The Citizen Lab, que es un laboratorio interdisciplinario con sede en la Universidad de Toronto Canadá, el cual centra su investigación y desarrollo en la intersección de las Tecnologías de la Información y Comunicación, los derechos humanos y la seguridad global.

3. The Citizen Lab, The Million Dollar Dissident: NSO Groups iPhone Zero -Days used against a UAE Human Rights Defender.

4. The Citizen Lab, Bitter Sweet: Supporters of Mexicos Soda Tax Targeted With NSO Exploit Links.

*No se omite señalar que tres de los documentos antes citados están en **idioma inglés**, no obstante esta unidad administrativa no cuenta con personal para realizar la traducción de los mismos al castellano, como lo solicitó en sus oficios.*

No obstante, se sugiere consultar a la Dirección General de Asuntos Internacionales si cuenta con algún, contrato para realizar traducciones, ya que dicha área es la que ha tenido esos contratos en años anteriores.”

Por tal motivo, [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda se sirva proporcionar la siguiente información:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

1. *Indique si la Dirección General de Asuntos Internacionales ha celebrado, gestionado y/o participado de forma alguna en la contratación de cualquier persona física y/o moral de carácter público o privado para la realización de traducciones.*
2. *Señale si la Dirección General de Asuntos Internacionales cuenta con facultades y personal capacitado y autorizado para llevar a cabo traducciones de documentos, de ser así, mencione los fundamentos legales aplicables.*
3. *De ser posible, sírvase proporcionar una traducción al castellano de los documentos adjuntos al oficio INAI/SPDP/DGPA/089/2017 del seis de julio de dos mil diecisiete, mismo que se adjunta al presente con los anexos respectivos; o bien, describa el procedimiento a seguir para solicitar dicha traducción.*

Le agradeceré haga del conocimiento de este título lo referido con anterioridad, en el domicilio abajo indicado, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Asuntos Internacionales, el trece de julio de dos mil diecisiete.

20. El trece de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **DGAJ/8823/2017** de la misma fecha, emitido y signado por el director general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1410/17** descrito en el **antecedente 9**, indicando lo siguiente:

[...]

Con fundamento en los artículos 7, 10, fracción VI, de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Director General de Asuntos Jurídicos me refiero a su diverso INAI/SPDP/DGIV/1410/17, correspondiente al expediente INAI.3S.08.03-003-2017 por el que solicita se proporcione la siguiente información:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Sobre el particular, me permito comunicarle que no es posible obsequiar favorablemente su solicitud, en atención a las siguientes consideraciones:

De conformidad con lo dispuesto por el artículo 6o., apartado A, fracción VIII, párrafo cuarto, de la Constitución Política de los Estados Unidos Mexicanos, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ese organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación.

Por su parte, el constituyente permanente en el artículo 102, apartado A, párrafo tercero, fracción VI, párrafo segundo, constitucional, dispuso que corresponde al Ministerio Público de la Federación la persecución, ante los tribunales, de todos los delitos del orden federal; y, por lo mismo, solicitará las medidas cautelares contra los imputados; buscará y presentará las pruebas que acrediten la participación de éstos en hechos que las leyes señalen como delito; procurará que los juicios federales en materia penal se sigan con toda regularidad para que la impartición de justicia sea pronta y expedita; pedirá la aplicación de las penas, e intervendrá en todos los asuntos que la ley determine.

De la lectura de los preceptos constitucionales invocados, válidamente se arriba a la conclusión de que la utilización de la herramienta tecnológica que menciona en su oficio, se vierte en hechos que se encuentran sujetos a investigación ministerial, siendo ésta una facultad y atribución que, en términos del invocado artículo 102 del Pacto Federal y en la Ley Orgánica de la Procuraduría General de la República, corresponde al Ministerio Público de la Federación, de lo que se sigue que la materia de la investigación preliminar radicada bajo el expediente INAI.3S.08.03-003-2017, colisiona con la facultad persecutora de delitos; pues como se ha dicho, a ese organismo constitucional autónomo le corresponde conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales.

Cito por su aplicación, el criterio orientador emitido por la Primera sala de la Suprema Corte de Justicia de la Nación, cuyos datos de registro, fuente, rubro y texto son del tenor siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

"MINISTERIO PÚBLICO. ES EL ÚNICO ÓRGANO DEL ESTADO COMPETENTE PARA FORMULAR E IMPULSAR LA ACUSACIÓN PENAL. Conforme a los artículos 21 y 102 de la Constitución Política de los Estados Unidos Mexicanos, el Ministerio Público tiene a su cargo la persecución e investigación de los delitos lo que significa que es el único órgano estatal competente para formular e impulsar la acusación o imputación delictiva. Así, la persecución e investigación de los delitos es una labor de carácter administrativo que por definición excluye a la judicial. Esto es, los artículos constitucionales aludidos deben leerse en el sentido de que establecen obligaciones a cargo del Ministerio Público, de manera que la investigación y persecución de los delitos no constituyen una prerrogativa a su cargo y, por tanto, no puede renunciar a su ejercicio, el cual es revisable en sede constitucional. Por otra parte, la posesión del monopolio no debe entenderse en el sentido de que la Constitución General de la República prohíbe la intervención de la víctima o del ofendido en el proceso penal como partes del mismo, en términos del artículo 20, apartado B, constitucional, pues el reconocimiento de este derecho coexiste con el indicado mandato constitucional a cargo del Ministerio Público. Así, a nivel constitucional también se dispone que deben existir medios de defensa que posibiliten la intervención de la víctima o del ofendido para efectos de impugnar, por ejemplo, el no ejercicio de la acción penal. Es decir, la división competencial es clara en el sentido de que el único órgano del Estado facultado para intervenir como parte acusadora en un proceso penal es el Ministerio Público; en su carácter de representante social, y de manera concomitante, aunque no necesaria- con la propia sociedad (cuando se trate de la víctima o el ofendido), en los términos que establece la propia Constitución Federal.

[...]

Con independencia de lo anterior, es oportuno precisar que la utilización no autorizada de la herramienta tecnológica que menciona en su requerimiento, en la actualidad se encuentra en etapa de investigación por parte del Ministerio Público de la Federación, de ahí que de conformidad con lo dispuesto por el artículo 218 del Código Nacional de Procedimientos Penales. Los registros de ésta, así como todos los documentos, independientemente de su contenido o su naturaleza, los objetos, los registros de voz e imágenes o cosas que le están relacionados a una investigación, son estrictamente reservados, por lo que, con los límites establecidos en el precepto invocado y demás disposiciones aplicables, únicamente son asequibles a las partes.

Adicionalmente, estimo oportuno precisar que las publicaciones periodísticas que dice sirvieron de sustento para iniciar de oficio la investigación preliminar radicada bajo el expediente INAI.3S.08.03-003-2017, sólo acreditan que tales publicaciones periodísticas tuvieron realización en el modo, tiempo y lugar que de las mismas aparezca, más en forma alguna son aptas para demostrar los hechos que en tales publicaciones se contienen, amén de que el estándar de veracidad del "sustento fáctico" de una nota periodística o un reportaje donde concurren información y opiniones, no es equivalente a la prueba en juicio de los hechos



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

en que se basa la nota, sino a un mínimo estándar de diligencia en la investigación y comprobación de hechos objetivos, lo cual no tiene por objeto apartarse de la distinción entre opiniones y hechos, ni limitar el derecho a la libertad de expresión, de manera que la manifestación de ideas y opiniones esté sujeta a la demostración con el mismo grado de exactitud que los hechos, sino fijar un parámetro objetivo y efectivo para identificar los casos en los que se abusa de la libertad de expresión.

En apoyo a lo anterior, cito por su aplicación los criterios orientadores cuyos datos de registro, fuente, rubro y texto, establecen:

[...]

NOTAS PERIODÍSTICAS, INEFICACIA PROBATORIA DE LAS. Las publicaciones en los periódicos únicamente acreditan que tuvieron realización en el modo, tiempo y lugar que tuvieron realización en el modo, tiempo y lugar de las mismas aparezca, más en forma alguna son aptas para demostrar los hechos que en tales publicaciones se contengan, pues no reúnen las características de documento público a que se refiere el artículo 795 de la Ley Federal del Trabajo, ni tampoco puede ser considerado como documental privada conforme a los artículos 796 y 797 del propio ordenamiento legal, en cuyo caso surge la posibilidad de formular las objeciones respectivas; consecuentemente, el contenido de una nota periodística, -generalmente redactada y dada a conocer por profesionales de la materia, cuyas fuentes no son necesariamente confiables, amén de que cabe la posibilidad de que sean producto de la interpretación e investigación personal de su autor- no puede convertirse en un hecho público y notorio, pues aunque aquélla no sea desmentida por quien puede resultar afectado, el contenido de la nota solamente le es imputable al autor de la misma, así a quienes se ven involucrados en la noticia correspondiente.

[...]

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

[...]

21. El trece de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SAI/0780/2017** de la misma fecha, emitido y signado por el secretario de acceso a la información de este Instituto, mediante el cual remitió el desahogo a los requerimientos formulados a través de los oficios **INAI/SPDP/DGIV/1389/17** y **INAI/SPDP/DGIV/1392/17** descritos en los **antecedentes 6 y 7**, indicando lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Me refiero a sus oficios **INAI/SPDP/DGIV/1388/17**, **INAI/SPDP/DGIV/1389/17**, **INAI/SPDP/DGIV/1391/17** e **INAI/SPDP/DGIV/1392/17**, por medio de los cuales solicitó el apoyo de esta Secretaría de Acceso a la Información para que, a partir de la información disponible en el Sistema de Portales de obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), se identificaran los contratos o instrumentos jurídicos, celebrados entre cualquier instancia del Gobierno Federal y cualquier empresa, para la adquisición del software de espionaje -spyware- y/o geolocalización denominado PEGASUS, en virtud de las investigaciones con número de expedientes **INAI.3S.08.03-002/2017** e **INAI.3S.08.03-003/2017** que se encuentran en trámite.

Al respecto a continuación se señalan las acciones que se llevaron a cabo para realizar la búsqueda de la información solicitada por esa Dirección General.

- La Dirección General de investigación y Verificación (DGIV) remitió los oficios **INAI/SPDP/DGIV/1388/17**, **INAI/SPDP/DGIV/1389/17** a la Secretaría de Acceso a la Información (SAI), recibido el 30 de junio de 2017 y el 03 de julio de 2017, respectivamente, mediante los cuales solicitó el apoyo para que, a partir de la información disponible en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), se identificaran los contratos o cualquier instrumento jurídico, mediante los cuales, cualquier dependencia de la Administración Pública Federal y de manera específica, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Gobernación; por sí o por conducto del Centro de Investigación y Seguridad Nacional y la Procuraduría General de la República, hubieren celebrado para la adquisición de software de espionaje -spyware- y/o geolocalización, con la empresa NSO Group.
- El 03 de julio de 2017, la DGIV envió a la SAI los oficios **INAI/SPDP/DGIV/1391/17** e **INAI/SPDP/DGIV/1392/17**, en alcance a los oficios **INAI/SPDP/DGIV/1388/17**, **INAI/SPDP/DGIV/1389/17** respectivamente, precisando que la búsqueda de la información considerara como parámetro, la adquisición del software PEGASUS por parte de cualquier instancia del Gobierno Federal, celebrado con cualquier empresa; esto es, sin restringirlo a las contrataciones celebradas, en su caso, con NSO Group. Dicha información se solicitó proporcionarla en un término de cinco días hábiles contados a partir del día hábil siguiente de su notificación.
- La SAI remitió el 04 de julio de 2017 los oficios **INAI/SAI/0718/2017**, **INAI/SAI/0719/2017**, **INAI/SAI/0720/2017** e **INAI/SAI/0721/2017** a las Direcciones Generales de Enlace con Partidos Políticos, Organismos Electorales y Descentralizados (DGEPPPOED); con Organismos Públicos Autónomos, Empresas Paraestatales,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Entidades Financieras, Fondos y Fideicomisos (DGOAEEF); con Autoridades Laborales, Sindicatos, Universidades, Personas Físicas y Morales (DGEALSUPFM), y; con la Administración Pública Centralizada y Tribunales Administrativos (DGEAPCTA), respectivamente, mediante los cuales se solicitó realizaran la búsqueda solicitada por la DGIV en la información publicada en el SIPOT por los sujetos obligados de su competencia.

- *La SAI remitió a la DGIV el oficio INAI/SAI/0755/2017 de fecha 10 de julio de 2017 mediante el cual hizo conocimiento que las Direcciones Generales de Enlace adscritas a la SAI, se encontraban realizando una búsqueda de la información requerida en el SIPOT; sin embargo, considerando la cantidad registros, se solicitó una prórroga de dos días hábiles para finalizar con lo requerido.*
- *El 11 de julio de 2017, la DGIV notificó a la SAI mediante los oficios INAI/SPDP/DGIV/1463/17 y INAI/SPDP/DGIV/1465/17, los acuerdos correspondientes a los expedientes INAI.3S.08.03-002/2017 e INAI.3S.08.03-003/2017, respectivamente, en los que se otorgó una prórroga de dos días hábiles para dar respuesta a los requerimientos formulados.*
- *Las Direcciones Generales de Enlace remitieron a esta Secretaría el resultado de la búsqueda solicitada, misma que se detalla a continuación:*
- *DGEPOED Mediante oficio INAI/SAI/DGEPOED/0365/2017 informó lo siguiente:*
"[...] se realizó una búsqueda de la información solicitada en el SIPOT, específicamente en los apartados de las fracciones XXVII y XXVIII del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, que hacen referencia a los procedimientos de adjudicación directa, invitación restringida y licitación de cualquier naturaleza, así como a la información respecto a las concesiones, contratos, convenios, permisos, licencias o autorizaciones otorgados, sin encontrar instrumento jurídico que vincule a alguno de los sujetos obligados bajo la responsabilidad de esta Dirección General con la adquisición del software materia de la solicitud".
- *DGOAEEF Mediante oficio INAI/SAI/DGOAEEF/0365/2017 informó lo siguiente:*
"[...] se realizó la búsqueda de la información publicada en el SIPOT por los sujetos obligados competencia de la Dirección General a mi cargo, que hiciera referencia a la adquisición del Software con la empresa NSO Group. En la búsqueda realizada a los 211 sujetos obligados ninguno de los contratos que se registraron en el SIPOT hacen alusión a la compra del mencionado software con la empresa NSO Group [...]"



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *DGEALSUPFM* Mediante oficio INAI/SAI/DGEALSUPFM/1668/2017, informó lo siguiente:

"[...] de la búsqueda realizada por personal adscrito a esta Dirección General de Enlace con Autoridades Laborales, Sindicatos, Universidades, Personas Físicas y Morales, en los diversos apartados que tienen asignados los sujetos obligados materia de su competencia en el referido sistema electrónico, no se localizó información alguna que se relacione con el requerimiento".

- *DGEAPCTA* Mediante oficio INAI/SAI/DGEAPCTA/0969/2017 informó lo siguiente:

"[...] se realizó la búsqueda de la información publicada en la fracción XXVIII. Las concesiones, contratos, convenios, permisos, licencias, o autorizaciones otorgadas, de los siguientes sujetos obligados:

- *Secretaría de Hacienda y Crédito Público*
- *Secretaría de Marina*
- *Secretaría de la Defensa Nacional*
- *Oficina de la Presidencia de la República*
- *Procuraduría General de la República*
- *Centro de investigación y Seguridad Nacional*
- *Secretaría de Gobernación*

Derivado de lo anterior le informo que se obtuvo un hallazgo de acuerdo a las siguientes palabras que mediante correo electrónico nos indicó como criterio de búsqueda

- *Pegasus*
- *NSO*
- *OBSES*
- *Citizen Lab*
- *Finfisher*
- *Hacking Team*
- *Finspy*
- *R3D*
- *Tecnología digital para el cambio social*
- *Spyware*
- *intervención telefónica periodistas*
- *Espionaje*
- *intervención de comunicaciones privadas*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- AV y D Solutions
- Balam Security / Balam Seguridad Privada/ Balam Seguridad Privada S.A. de C.V.
- Comercializadora de Soluciones Integrales Mecale
- Grupo Tech Bull
- Hacking Team / HT Soluciones S.R.L.
- HT. S.R.L.
- NSO Group / NSO Group Technologies Ud.
- Proyectos y Diseños VME
- Security Tracking Devices
- Security Hacking Devices
- Rodrigo Ruiz
- Asaf Zanzuri
- Erick Banoun
- M. Luppi
- M. Bettini
- Centros de control y comando (Elbit)
- Reestructuración Centro de Comando y Control
- Instalación de Plataforma Pegasus
- Software malicioso o malware

El hallazgo encontrado es el siguiente:

No	Sujeto Obligado	Contrato	Año	Palabra encontrada	Monto
1	Secretaría de Hacienda y Crédito Público (SHCP)	102-ADN-41-090/2016	2016	Servicios para el Aplicativo de Gestión Institucional Electrónico Pegasus	\$ 232, 717.97

Asimismo, mediante correo electrónico, la DGEAPCTA, remitió el detalle de la información identificada en el SIPOT, a petición de la SAI.

Para mayor referencia se anexa, en versión electrónica, los, oficios y el correo electrónico remitidos por las Direcciones Generales de Enlace.

De conformidad con lo anteriormente expuesto, esta secretaría atiende la solicitud de la DGIV, para que a partir de la información disponible en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), se identificaran los contratos o instrumentos jurídicos, celebrados entre cualquier instancia del Gobierno Federal y cualquier empresa, para la adquisición del software de espionaje -spyware- y/o



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

geolocalización denominado PEGASUS, en virtud de las investigaciones con número de expedientes INAI.3S.0803-002/2017 e INAI.3S.08.03-003/2017.

[...]

- a) Anexo a la atención, se remitieron en disco compacto los oficios de respuesta de las unidades administrativas; así como, correo electrónico enviado el doce de julio de dos mil diecisiete y reenviado el trece del mismo mes y año, por la directora de coordinación y seguimiento de la secretaría de acceso a la información, dirigido al jefe de departamento de coordinación para la evaluación de la dirección general de evaluación.

22. Mediante el oficio número **INAI/SPDP/DGIV/1534/17** del catorce de julio de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al secretario de acceso a la información de este Instituto, lo siguiente:

[...]

Hago referencia a su oficio INAI/SAI/0780/20 17, recibido en la Dirección General de Investigación y Verificación de este Instituto el trece de julio de dos mil diecisiete, a través del cual dio respuesta al requerimiento que le fue formulado mediante los diversos oficios INAI/SPDP/DGIV/1389/17 e INAI/SPDP/DGIV/1392/17.

Al respecto, considerando la información proporcionada en relación con los contratos o cualquier instrumento jurídico, mediante los cuales cualquier instancia del Gobierno Federal haya celebrado con cualquier empresa para la adquisición de software de espionaje (malware y/o spyware) y/o geolocalización, en particular aquél denominado "Pegasus", a partir del Sistema de Portales Obligaciones de Transparencia (SIPOT), y con fundamento en los artículos [...]; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a las unidades administrativas de la Secretaría a su digno cargo, para lo siguiente:

1. *Realice las acciones pertinentes en torno a la evaluación y verificación del cumplimiento de las obligaciones de transparencia correspondientes a los sujetos obligados que presuntamente han sido señalados diversas notas periodísticas como vinculados con los hechos materia de la presente investigación (Procuraduría General de la República, Secretaría de Gobernación, Secretaría de la Defensa Nacional, Secretaría de Marina*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

y/o Centro de Investigación y Seguridad Nacional), específicamente sobre la publicación de contratos, convenios y cualquier Instrumento jurídico relacionado con la adquisición y utilización del software (malware) denominado "Pegasus".

2. *Lleve a cabo las gestiones que, resulten necesarias con la finalidad de que los sujetos obligados señalados como vinculados con los hechos materia de la presente investigación (Procuraduría General de la República, Secretaría de Gobernación, Secretaría la Defensa Nacional, Secretaría de Marina y Centro de Investigación y Seguridad Nacional) cumplan con sus obligaciones de transparencia y publiquen en sus portales de internet los contratos que, en su caso, se hayan celebrado. respecto de la adquisición y utilización del software (malware) denominado "Pegasus" o en su caso, justifiquen la clasificación de la información como reservada o confidencial.*
3. *Comunique a esta Dirección General de Investigación y Verificación el avance y resultado de las acciones que lleve a cabo derivado de los puntos anteriores.*

*Le agradeceré haga del conocimiento lo referido con anterioridad, en el domicilio abajo indicado, en un término máximo de **cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Secretaría de Acceso a la Información, el catorce de julio de dos mil diecisiete.

23. El catorce de julio de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SE/DGAI/095/17** de la misma fecha, emitido y signado por el director general de asuntos internacionales de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1482/17** descrito en el **antecedente 19**, indicando lo siguiente:

[...]

Esta Dirección General de Asuntos Internacionales hace de su conocimiento que:

Respecto al numeral primero. *Esta Unidad Administrativa no ha formalizado contrato o pedido alguno en términos del Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Acceso a la Información y Protección de Datos, vigente. No obstante, se han erogado recursos al solicitar servicios de traducción de documentos, mediante pagos*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

directos a diversos proveedores por situarse en el supuesto del artículo 42, séptimo párrafo del citado reglamento.

***Respecto al numeral segundo.** De conformidad con el artículo 31, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, esta Dirección General no cuenta con estas atribuciones.*

***Respecto al numeral tercero.** El procedimiento para realizar la traducción parte de la solicitud de una cotización que depende del número de palabras; el precio varía según si se solicita una traducción simple o una traducción certificada por perito autorizado para ello. Si la cantidad cotizada no excede del supuesto señalado por el artículo 42, séptimo párrafo, del Reglamento citado, la Unidad Administrativa a su cargo puede escoger al perito de su confianza y erogar los recursos afectando la partida presupuestal 33601 relacionados con traducciones, de su presupuesto.*

Por otra parte, se advierte que el documento adjunto de ambos oficios es idéntico, aun cuando los expedientes son diferentes. Por lo que sugerimos que identifiquen con precisión las porciones que es necesario traducir, dado que figura diversa información que no es parte de la nota periodística, como anuncios, paneles con información de redes sociales y eventos de los sitios de los que se obtuvo la información y gráficos; con el fin de evitar que se realicen traducciones duplicadas o innecesarias que se reflejarían en el precio total del servicio.

[...]

24. El uno de agosto de dos mil diecisiete, el subdirector de verificación del sector público B, adscrito a la entonces Dirección General de Investigación y Verificación, emitió una constancia a través de la cual se procedió a obtener una copia simple del oficio **INAI/SAI/0780/2017** remitido por el secretario de acceso a la información de este Instituto (**antecedente 21**) y un duplicado del disco compacto anexo, puesto que únicamente se recibió un original de los mismos, los cuales fueron integrados al expediente de investigación **INAI.3S.08.03.002/2017**.

a) Adjunto a la constancia obran los documentos siguientes:

- Oficio número INAI/SAI/DGEALSUPFM/1668/2017 del diez de julio de dos mil diecisiete, suscrito por la directora general de enlace con autoridades laborales, sindicatos, universidades, personas físicas y morales, dirigido al secretario de acceso a la información.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Oficio número INAI/SAI/DGEAPCTA/0969/2017 del diez de julio de dos mil diecisiete, suscrito por el director general de enlace con la administración pública centralizada y tribunales administrativos, dirigido al secretario de acceso a la información.
- Oficio número INAI/SAI/DGEPPOED/0420/2017 del diez de julio de dos mil diecisiete, suscrito por el director general de enlace con partidos políticos, organismos electorales y descentralizados, dirigido al secretario de acceso a la información.
- Oficio número INAI/SAI/DGOAEEF/0365/2017 del diez de julio de dos mil diecisiete, suscrito por el director general de enlace con organismos públicos autónomos, empresas paraestatales, entidades financieras: fondos y fideicomisos, dirigido al secretario de acceso a la información.
- Correo electrónico enviado el doce de julio de dos mil diecisiete y reenviado el trece del mismo mes y año, por la directora de coordinación y seguimiento de la secretaría de acceso a la información, dirigido al jefe de departamento de coordinación para la evaluación de la dirección general de evaluación.

25. El tres de agosto de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SE/DGAI/098/17** de la misma fecha, emitido y signado por la directora de asuntos internacionales de acceso de este Instituto, mediante el cual remitió un alcance al oficio **INAI/SE/DGAI/095/17** descrito en el **antecedente 23**, indicando lo siguiente:

[...]

En alcance al oficio INAI/SE/DGAI/095/17 y derivado de la reunión sostenida entre la Secretaría Ejecutiva, la Secretaría de Protección de Datos Personales, la Dirección General de Investigación y Verificación y la Directora de Asuntos Internacionales de Acceso, hago de su conocimiento que esta unidad administrativa ha cotizado el costo de los servicios de traducción certificada de los siguientes documentos:

1. 2. *The Citizen Lab - University of Toronto*
2. 3. *The Million Dollar Dissident NSO Group's iPhone Zero-Days used against.*
3. 4. *Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit.*

Lo anterior, con el objeto de requerir dicho servicio al proveedor Ab Aeterno Traductores.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

No omito precisar que la traducción certificada será entregada a esta unidad administrativa en un plazo de cinco días hábiles.

[...]

26. El cuatro de agosto de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SAI/0827/2017** de la misma fecha, emitido y signado por el secretario de acceso a la información de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1534/17** descrito en el **antecedente 22**, indicando lo siguiente:

[...]

*Me refiero a sus oficios **INAI/SPDP/DGIV/1533/17** e **INAI/SPDP/DGIV/1534/17**, ambos de fecha 14 de julio del presente año, mediante los cuales solicita a esta Secretaría dar seguimiento a la publicación de los contratos, convenios o cualquier instrumento jurídico relacionado con la adquisición y utilización del software (malware) denominado "Pegasus", que hubieran sido celebrados por la Procuraduría General de la República, la Secretaría de Gobernación, la Secretaría de la Defensa Nacional, la Secretaría de Marina y el Centro de Investigación y Seguridad Nacional, en cumplimiento de sus obligaciones de transparencia.*

*Al respecto, me permito informarle que de conformidad con lo dispuesto en el artículo Tercero Transitorio de los Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el Título Quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia, publicados en el Diario Oficial de la Federación el cuatro de mayo de dos mil dieciséis, se establece que, **una vez fenecido el plazo** para que los sujetos obligados carguen sus obligaciones de transparencia, **los organismos garantes deben llevar a cabo una primera verificación diagnóstica sobre el cumplimiento de los sujetos obligados de su competencia**, la cual no tendrá efectos vinculantes conforme a lo establecido en el artículo 88 de la Ley General, pues tiene como finalidad detectar áreas de oportunidad para el cumplimiento a las obligaciones de transparencia.*

Dicho plazo feneció el cuatro de mayo de dos mil diecisiete, de conformidad con el Acuerdo por el cual se aprueba la modificación del plazo para que los sujetos obligados de los ámbitos Federal, Estatal y Municipal incorporen a sus portales de Internet y a la Plataforma Nacional de Transparencia, la información a la que se refieren el Título Quinto y la fracción IV del artículo



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

31 de la Ley General de Transparencia y Acceso a la Información Pública, así como la aprobación de la definición de la fecha a partir de la cual podrá presentarse la denuncia por la falta de publicación de las obligaciones de transparencia, a la que se refiere el Capítulo VII y el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública, publicado en el Diario Oficial de la Federación el dos de noviembre de dos mil dieciséis.

En este sentido, en el Acuerdo mediante el cual se aprueban las directrices a cabo la verificación diagnóstica establecida en el artículo tercero transitorio de los Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia; así como la atención a la denuncia por incumplimiento a las obligaciones de transparencia, publicado en el Diario Oficial de la Federación el once de mayo de dos mil diecisiete, aprobado por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, se estableció que la verificación de carácter diagnóstica se realizar entre el cinco de mayo y el último día hábil del año en curso para este Instituto; es decir, al veinte de diciembre.

De esta manera, se advierte que la verificación diagnóstica a los sujetos obligados del ámbito federal se encuentra en trámite actualmente, por lo que no será sino hasta que la misma se concluya que podrán elaborarse los requerimientos que resulten necesarios, tales como la publicación de los contratos o instrumentos jurídicos a los que se refiere en sus oficios. Lo anterior, considerando que, a través de la verificación en comento, es como se puede identificar la información faltante para cada sujeto obligado. Por lo anterior, en este momento no es posible atender favorablemente los requerimientos mencionados en los oficios que nos ocupan.

No obstante, le comparto que esta secretaría de Acceso a la Información elaboró una propuesta de intervención de transparencia proactiva sobre la contratación de servicios especializados en materia de vigilancia, con la finalidad de detonar la rendición de cuentas efectiva en el presunto caso de espionaje a activistas mexicanos, la cual una vez que sea aprobada podremos compartirlas. Sin embargo, toda vez que se han identificado diversas solicitudes y recursos de revisión relacionados con los contratos señalados, los cuales podrían resultar de su interés, se adjunta al presente el listado de los mismos.

[...]

- a) Adjunto a la atención, el Secretario de Acceso a la Información remitió en disco compacto un listado en formato *Excel* que contiene las solicitudes de información



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

ingresadas a los sujetos obligados sobre el tema de espionaje telefónico, del doce de junio de dos mil tres al cinco de junio de dos mil diecisiete. A manera de ejemplo se reproduce parte de la información:

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES SECRETARÍA DE ACCESO A LA INFORMACIÓN DIRECCIÓN GENERAL DE EVALUACIÓN												
Solicitudes de información ingresadas a los Sujetos Obligados del Orden Federal sobre el tema de espionaje telefónico*												
Criterio	Subjeto Obligado	Fecha de Ingreso	Fecha de Respuesta	Fecha de Cierre	Resumen	Estado de la Solicitud	Tipo de Solicitud	Fecha de Recibo	Procedente	Acción de Seguimiento	FEED	Fecha de Cierre
6	PROCURADURÍA GENERAL DE LA REPÚBLICA (PGR)	08/07/2017	05/07/2017	07/07/2017	Se solicitó la información en el formato de Excel de los datos de los sujetos obligados de la PGR que se encuentran a la espera de la información que se les ha solicitado. Cabe mencionar que la información de los sujetos obligados de la PGR que se encuentran a la espera de la información que se les ha solicitado, se encuentra en el formato de Excel de los datos de los sujetos obligados de la PGR que se encuentran a la espera de la información que se les ha solicitado. Cabe mencionar que la información de los sujetos obligados de la PGR que se encuentran a la espera de la información que se les ha solicitado, se encuentra en el formato de Excel de los datos de los sujetos obligados de la PGR que se encuentran a la espera de la información que se les ha solicitado.	Se ingresó						
8	COMISIÓN DE LA ASERTACIÓN FEDERAL (CAF)	08/07/2017	04/07/2017	07/07/2017	Se solicitó la información en el formato de Excel de los datos de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado. Cabe mencionar que la información de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado, se encuentra en el formato de Excel de los datos de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado.	Se ingresó						
7	COMISIÓN DE LA ASERTACIÓN FEDERAL (CAF)	08/07/2017	04/07/2017	07/07/2017	Se solicitó la información en el formato de Excel de los datos de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado. Cabe mencionar que la información de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado, se encuentra en el formato de Excel de los datos de los sujetos obligados de la CAF que se encuentran a la espera de la información que se les ha solicitado.	Se ingresó						

27. El siete de agosto de dos mil diecisiete, el subdirector de verificación del sector público B, adscrito a la entonces Dirección General de Investigación y Verificación, emitió una constancia a través de la cual se procedió a obtener una copia simple del oficio INAI/SAI/0827/2017 emitido y signado por el secretario de acceso a la información de este Instituto (**anexo 26**) y un duplicado del disco compacto anexo, puesto que únicamente se recibió un original de los mismos, los cuales fueron integrados al expediente de investigación INAI.3S.08.03.002/2017.

- a) Adjunto a la constancia obra el listado en formato Excel que contiene las solicitudes de información ingresadas a los sujetos obligados sobre el tema de espionaje telefónico, del doce de junio de dos mil tres al cinco de junio de dos mil diecisiete.

28. El quince de agosto de dos mil diecisiete, el subdirector de verificación del sector público B, adscrito a la entonces Dirección General de Investigación y Verificación, emitió una constancia a través de la que se constató la consulta de tres direcciones



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

electrónicas¹⁴, con la finalidad de allegarse de notas periodísticas relacionadas con los hechos materia de la investigación, las cuales se integraron al expediente.

a) Adjunto obran las siguientes notas periodísticas, las cuales se mencionan en la constancia, cuyos títulos de destacan a continuación:

- *Los 5 contratos de Sedena para espiar celulares y comunicación por internet*, publicada el dieciséis de julio de dos mil doce, en el portal electrónico Aristegui Noticias.
- *Recibió PGR Pegasus en 2015 para espiar 500 objetivos*, publicada el veintiocho de junio de dos mil diecisiete, en el portal electrónico El Diario.mx.
- *Fue legal el uso de Pegasus, justifica Arely Gómez, extitular de la PGR*, publicada el veintinueve de junio de dos mil diecisiete, en el portal electrónico de Proceso.

29. El quince de agosto de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SE/DGAI/102/17** de la misma fecha, emitido y signado por el director general de asuntos internacionales de este Instituto, mediante el cual remitió un alcance al oficio **INAI/SE/DGAI/095/17** descrito en el **antecedente 23**, indicando lo siguiente:

[...]

En seguimiento a los oficios INAI/SE/DGAI/095/17 e INAI/SE/DGAI/098/17 emitidos por esta unidad administrativa los días 14 de julio y 3 de agosto de 2017, hago envío de la de la traducción certificada de los siguientes documentos:

- 2 *The Citizen Lab-University of Toronto*
- 3 *The Million Dollar Dissident NSO Group's iPhone Zero-Days used against.*
- 4. *Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit.*

No omito precisar que los archivos digitales de los documentos referidos ya han sido entregados, vía correo electrónico, a su dirección general.

¹⁴ <http://m.aristeguinoticias.com/1607/mexico/a-detalle-los-5-contratos-de-sedena-para-espionaje-de-celulares-y-radios/>, http://diario.mx/Nacional/2017-06-28_a65dd86a/recibio-pgr-pegasus-en-2015-para-espiar-500-objetivos/, <http://www.proceso.com.mx/493045/fue-legal-uso-pegasus-justifica-arely-gomez-extitular-la-pgr>.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

a) Adjunto al alcance, se remitió la traducción realizada por la perito traductora del Tribunal Superior de la Ciudad de México, recibida en la Oficialía de Partes de este Instituto el catorce de agosto de dos mil diecisiete, de los documentos:

- *The Citizen Lab-University of Toronto.*
- *The Million Dollar Dissident: NSO Groups iPhone Zero-Days used against a UAE Human Rights Defender*, publicado el veinticuatro de agosto de dos mil dieciséis en el portal electrónico de *The Citizen Lab*.
- *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, publicado el once de febrero de dos mil diecisiete en el portal electrónico de *The Citizen Lab*.

30. Mediante el oficio número **INAI/SPDP/DGIV/1905/17** del diecisiete de agosto de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al a la directora general de atención al pleno de este Instituto, lo siguiente:

[...]

Hago referencia al oficio INAI/STP/DGAP/972/2017 del seis de julio de dos mil diecisiete, y recibido en esta Dirección General de Investigación y Verificación en la misma fecha, a través del cual desahogó el requerimiento que le fue formulado por medio del diverso INAI/SPDP/DGIV/1381/17.

En ese sentido, en el oficio de referencia se informó que, de la búsqueda efectuada dentro de la base de datos relativa a la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público, se localizaron dos recursos de revisión referentes al uso del software (malware) identificado como "Pegasus", a saber:

Expediente, Autoridad Comisionado	y	Solicitud	Ingreso	Fecha de sesión en que se resolvió	Sentido
-----------------------------------------	---	-----------	---------	------------------------------------------	---------



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

RRA 3762/16 PROCURADURÍA GENERAL DE LA REPÚBLICA Oscar Mauricio Guerra Ford	Los detalles de cualquier contrato y manuales de uso, relacionados con el programa de cibervigilancia "Pegasus" o similar [...] El equipo fue adquirido en 2014 y 2015.	28/10/2016	07/12/2016	Confirma
RRA 4265/17 SECRETARÍA DE GOBERNACIÓN (SEGOB) Arely Cano Guadiana	requiero cualquier documento (contrato, convenio, oficio, memorándum, correo electrónico, entre otros) que de cuenta de la adquisición del malware pegasus, mediante el cual se está realizando espionaje	27/06/2017	En sustanciación	En sustanciación

Por tal motivo, con fundamento en los artículos [...] me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda se sirva proporcionar la siguiente información:

1. *Comunique si la resolución del recurso de revisión RRA 3762/16, interpuesto en contra de la Procuraduría General de la República ha causado estado o bien, si la misma ha sido impugnada.*
2. *Indique cuál es el estado procesal actual del recurso de revisión RRA 4265/17, interpuesto en contra de la Secretaría de Gobernación*
3. *Señale si a la fecha del presente el Pleno de este Instituto ha emitido resolución respecto del recurso de revisión RRA 4265/17, sirviéndose remitir copia simple de la misma, en su caso*
4. *De ser el caso, precise si la resolución recaída al recurso de revisión RRA 4265/17, precisando si la misma ha causado estado o cuenta con algún medio de impugnación interpuesto.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. *Mencione si tiene conocimiento de algún otro recurso de revisión en materia de acceso a la información y/o protección de datos personales, que se encuentre vinculado con información referente al uso del software (malware) identificado como "Pegasus" de ser el caso, indique el número de expediente y el nombre del sujeto obligado en contra de quien se tramitó el asunto y sírvase remitir copia de la resolución recaída al mismo.*

*Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el diecisiete de agosto de dos mil diecisiete.

31. Mediante el oficio número **INAI/SPDP/DGIV/1548/17** del veintidós de agosto de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, lo siguiente:

[...]

En ese sentido, no se omite señalar que, de la búsqueda efectuada por este Instituto se advirtió que en el sitio web de "Aristegui Noticias", el dieciséis de julio de dos mil doce se publicó una nota periodística con el encabezado "Los 5 contratos de Sedena para espiar celulares y comunicación por internet" en la que se hace referencia de la adquisición de un software y equipo de comunicaciones y telecomunicaciones, presuntamente para intervenir comunicaciones y dispositivos de telefonía.

[...]

De tal forma, con fundamento en los [...], me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

1. *Indique si la Secretaría de la Defensa Nacional ha adquirido, comprado, arrendado o se encuentra en posesión, bajo cualquier figura jurídica, del software (malware) identificado como "Pegasus".*
2. *Precise el nombre, denominación y/o razón social de la persona física y/o moral de quien haya adquirido el software (malware) identificado como "Pegasus".*
3. *Describa en qué consiste y cómo opera el software (malware) identificado como "Pegasus".*
4. *Indique de forma detallada las acciones que pueden llevarse a cabo con el software (malware) identificado como "Pegasus", y describa puntualmente cuál es la información y datos personales a los que se puede tener acceso.*
5. *Señale quienes son los servidores públicos y/o personal, perteneciente o no a la Secretaría de la Defensa Nacional, autorizado para la utilización del software (malware) identificado como "Pegasus".*
6. *Describa los procedimientos técnicos, informáticos y, en su caso, legales seguidos para la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".*
7. *Proporcione copia simple de los convenios, contratos, fallo de licitaciones o cualquier documento físico y/o electrónico, independientemente de su denominación, relacionado con la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".*
8. *Señale si la Secretaría de la Defensa Nacional ha utilizado el software (malware) identificado como "Pegasus" y precise cuál es la información y datos personales que ha recabado.*
9. *De ser el caso, explique qué situaciones o circunstancias, para que finalidades y respecto que titulares ha utilizado el software (malware) identificado como "Pegasus"; y precise si ha llevado a cabo el tratamiento (obtención, uso, registro, reproducción, conservación, organización y modificación, transmisión y/o cancelación) de datos personales a partir del mismo.*
10. *Manifieste si la Secretaría de la Defensa Nacional ha tenido conocimiento de los hechos referidos en el acuerdo del treinta de junio de dos mil diecisiete, así como, de alguna queja, denuncia o inconformidad relacionada con los mismos y en su caso describa las acciones que ha llevado a cabo al respecto.*

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

El requerimiento se notificó a la Secretaría de la Defensa Nacional, el veintidós de agosto de dos mil diecisiete.

32. El veintitrés de agosto de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/1548/17**, descrito en el **antecedente 31**.

33. El veinticuatro de agosto de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP/DGAP/1180/2017** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1905/17** descrito en el **antecedente 30**, indicando lo siguiente:

[...]

Al respecto, me permito hacer de su conocimiento lo siguiente, por cada punto requerido:

[...]

Por lo que, al no contar con atribuciones o mayores elementos para identificar la información requerida por usted, esta Dirección General no puede determinar si las resoluciones de los recursos de revisión RRA 3762/16 y RRA 4265/17 han causado estado o si han sido impugnadas.

Respecto de los puntos identificados con los números 2 y 3, me permito hacer de su conocimiento que el recurso de revisión RRA 4265/17 fue resuelto por el Pleno de este Instituto; el pasado 9 de agosto del año en curso, en el que se confirmó la respuesta del sujeto obligado, y cuya resolución se anexa al presente en copia simple.

Ahora bien, en cuanto al requerimiento identificado con el número 5, me permito informarle que esta Dirección General advierte que el único documento por medio del cual puede identificar asuntos dentro de su competencia que se relacionen con el uso del software (malware) identificado como Pegasus", es la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público.

Además, respecto de los medios de impugnación en materia de protección de datos personales, esta Dirección General no concentra el contenido de las solicitudes interpuestas



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

por los particulares, sino únicamente almacena los datos de identificación de los expedientes que son turnados a las Ponencias de este Instituto.

Así las cosas, se realizó una búsqueda dentro de la base de datos referida previamente, en la que se localizaron hasta la fecha de presentación de su oficio, además de los ya informados en los Oficios INAI/STP/DGAP/972/2017 y INAI/STP/DGAP/973/2017, los siguientes recursos de revisión en materia de acceso a la información vinculados con información referente al uso del software (malware) identificado como "Pegasus":

Expediente, Autoridad y Comisionado	Solicitud	Ingreso	Fecha de sesión en que se resolvió	Sentido
RRA 4744/17 SECRETARÍA DE GOBERNACIÓN (SEGOB) Rosendoevgueni Monterrey Chepov	¿Con que objeto se contrató el programa Pegasus y cuanto costo? asimismo se solicita copia escaneada de los contratos relacionados con dicho programa. ¿Por que se espía a periodistas y a luchadores sociales con dicho programa?	12/07/2017	En sustanciación	En sustanciación
RRA 5259/17 CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL Areli Cano Guadiana	Contratos y Convenios adquiridos para el Sistema de Inteligencia Nacional Contratos y Convenios adquiridos para el Sistema de Inteligencia	09/08/2017	En sustanciación	En sustanciación



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

	<p>Nacional con empresas que venden Software para el espionaje especialmente del malware Pegasus por parte de las Secretaría de la Defensa Nacional, Secretaría de Gobernación y el Centro de Investigación y Seguridad. Nacional y cómo se utilizan estos software para espiar a la población mexicana</p>			
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Resulta necesario recalcar que, dentro de las actividades competencia de esta Dirección General, no se encuentra la de llevar a cabo análisis normativo o de cualquier otro tipo del cuerpo de las resoluciones emitidas por el Pleno de este Instituto, de tal manera que la única fuente de información con la que cuenta esta Unidad Administrativa, para efectos de la atención a su requerimiento, es la base de datos previamente indicada.

Ahora bien, en cuanto a los requerimientos identificados con el número 1 y 4, esta Dirección General sugiere remitir su requerimiento de información a la Dirección General de Asuntos Jurídicos, Unidad Administrativa que podría contar con mayores elementos que pudieran ser de su interés conforme a lo dispuesto en el artículo 32, fracciones I y II del Estatuto Orgánico de este Instituto.

Aunado a lo anterior, esta Unidad Administrativa informa que los documentos de carácter público tales como solicitudes, estudios, resoluciones, entre otros, que pudiesen ser de su interés pueden ser localizados y consultados en el Zoom, Buscador de Solicitudes de Información y Recursos de Revisión.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

A través de ese buscador, es posible ubicar aquellos documentos relacionados adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus".

[...]

- a) Adjunto, se remitió la resolución en la que se determinó **confirmar** la respuesta de la Secretaría de Gobernación, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el **RRA 4265/16**, el nueve de agosto de dos mil dieciséis.

34. El veintinueve de agosto de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **J-CONS-V-22056** de la misma fecha, emitido y signado por el jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, mediante el cual solicitó una prórroga para desahogar el requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1548/17** descrito en el **antecedente 31**, indicando lo siguiente:

[...]

En relación con su oficio No. INAI/SPDP/DGIV/1548/17 de fecha 22 de agosto de 2017, deducido del expediente INAI.3S.08.03-003/2017, por el que refiere a esta Unidad de Asuntos Jurídicos de la Secretaría de la Defensa Nacional, que inició una investigación de oficio, por un probable incumplimiento en materia de protección de datos personales por parte de este Instituto Armado; al respecto, me permito solicitar se otorgue una prórroga para estar en posibilidad de remitir la Información que atienda su requerimiento, en virtud de que la información no se cuenta en esta Unidad, sino que debe ser recabada de diversas áreas de esta Secretaría de la Defensa Nacional, a efecto de atenderla en los mejores términos.

[...]

35. El veintinueve de agosto de dos mil diecisiete, el entonces director general de investigación y verificación, emitió un acuerdo a través del cual tuvo por recibido el oficio **J-CONS-V-22056** (**antecedente 34**) y otorgó a la Unidad de Asuntos Jurídicos de la Secretaría de la Defensa Nacional una prórroga para dar respuesta al requerimiento formulado.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

36. El veintinueve de agosto de dos mil diecisiete, el entonces director general de investigación y verificación emitió el oficio **INAI/SPDP/DGIV/2060/17** a través del cual se informa al jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, el acuerdo descrito en el **antecedente 35**.

El oficio se notificó a la Secretaría de la Defensa Nacional, el treinta de agosto de dos mil diecisiete.

37. El treinta y uno de agosto de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/2060/17**, descrito en el **antecedente 36**.

38. El cuatro de septiembre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **J-CONS-V-22079** del uno de septiembre de dos mil diecisiete, emitido y signado por el jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1548/17** descrito en el **antecedente 31**, indicando lo siguiente:

[...]

En relación con su oficio No. INAI/SPDP/DGIV/1548/17 de fecha 22 Ago. de 2017, por el que informa a esta Unidad de Asuntos Jurídicos, que inició una investigación de oficio dentro del expediente INAI.3S.08.03-003/2017, el 30 de junio de 2017, al respecto, la Dirección General de Transmisiones dice a esta Unidad de Asuntos Jurídicos lo siguiente:

"...Esta Secretaría de la Defensa Nacional, en los periodos que refiere el requerimiento (2015 y 2016), no adquirió, arrendó o tuvo en posesión, el software identificado como "PEGASUS", ya que en dicho periodo no se contaba con esa herramienta informática; por lo que esta Secretaría se encontraba imposibilitada materialmente, para hacer uso del software en dicho periodo; y, en consecuencia, no se localizó información respecto a que se haya recabado, obtenido, transmitido, manejado o se haya dado algún tratamiento a datos personales que se hayan obtenido a través del citado software.

En consecuencia, se da respuesta a los cuestionamientos del INAI, de la forma que a continuación se indica:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

1. *Indique si la Secretaría de la Defensa Nacional ha adquirido, comprado, arrendado o se encuentra en posesión, bajo cualquier figura jurídica, del software (MALWARE) identificado como "PEGASUS".*

No se localizó información de que, del año 2015 a la fecha, esta Secretaría obtenido por alguna de las formas a que se refiere la pregunta o haya tenido, o tenga en posesión el software (MALWARE) identificado como "PEGASUS" que refiere.

2. *Precise el nombre, denominación y/o razón social de la persona física y/o moral de quien haya adquirido el software (MALWARE) identificado como "PEGASUS".*

En atención a la respuesta dada a la pregunta número uno, no existe información de ninguna persona física y/o moral de quien haya adquirido el software (MALWARE) identificado como "PEGASUS".

3. *describa en que consiste y como opera el software (MALWARE) identificado como "PEGASUS".*

En atención a la respuesta dada a la pregunta número uno, no existe información que describa en que consiste y como opera el software citado en su requerimiento.

4. *Indique de forma detallada las acciones que pueden llevarse a cabo con el software (MALWARE) identificado como "PEGASUS" y describa puntualmente cual es la información y datos personales a los que se puede tener acceso.*

En atención a la respuesta dada a la pregunta número uno, no se localizó información que indique de forma detallada las acciones que puede llevarse a cabo con el software (MALWARE) identificado como "PEGASUS" y/o cual es la información y datos personales a los que se puede tener acceso.

5. *Señale quienes son los servidores públicos y/o personal, perteneciente o no a la Secretaría de la Defensa Nacional, autorizado para la utilización del software (MALWARE) identificado como "PEGASUS".*

En atención a la respuesta a la pregunta número uno, no existen servidores públicos y/o personal, perteneciente a la Secretaría de la Defensa Nacional, autorizado para la utilización del software (MALWARE) identificado como "PEGASUS".



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

6. *Describa los procedimientos técnicos, informáticos y, en su caso, legales seguidos para la adquisición, instalación operación y utilización del software (MALWARE) identificado como "PEGASUS".*

En atención a la respuesta a la pregunta número uno, no se localizó información sobre los procedimientos señalados en la presente pregunta.

7. *Proporcione copia simple de los convenios, contratos, fallo de licitaciones o cualquier documento físico y/o electrónico, con independencia de su denominación, relacionado con la adquisición, instalación, operación y utilización del software (MALWARE) identificado como "PEGASUS",*

En atención a la respuesta a la pregunta número uno, no se cuenta con documentación como la que refiere en la pregunta que se contesta.

8. *Señale si la Secretaría de la Defensa Nacional ha utilizad el software (MALWARE) identificado como "PEGASUS", y precise cual es la información y datos personales que ha recabado.*

En atención a la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento, ya que como se indicó, en el periodo que se investiga hasta la fecha esta Secretaría no cuenta con el software citado.

9. *De ser el caso, explique en qué situaciones o circunstancias, para que finalidades y respecto de que titulares ha utilizado el software (MALWARE) identificado como "PEGASUS"; y precise si ha llevado a cabo tratamiento (obtención, uso, registro, reproducción, conservación, organización, modificación, transmisión y/o cancelación) de datos personales a partir del mismo.*

En atención a la respuesta a la pregunta número uno, no existe la información que se requiere en la presente pregunta.

10. *Manifieste si la Secretaría de la Defensa Nacional ha tenido conocimiento de los hechos referidos en el acuerdo de treinta de junio de dos mil diecisiete, así como de alguna queja, denuncia o inconformidad relacionada con los mismos y en su caso describa las acciones que ha llevado a cabo al respecto.*

En relación con la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento.

Por lo anterior se solicita:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

ÚNICO: Que la Dirección General de Investigación y Verificación del Instituto Nacional de Transparencia, archive el presente asunto sin ninguna responsabilidad para esta Secretaría de la Defensa Nacional, ya que no se localizó información respecto a los hechos que se investigan del 2015 a la fecha..."

[...]

Por lo que se solicita se fusione la presente investigación al expediente No. INAI.3S.08.03-002/2017, y en su oportunidad, con motivo de los argumentos vertidos en el presente escrito, se archive sin responsabilidad para esta Secretaría de la Defensa Nacional.

[...]

39. Mediante el oficio número **INAI/SPDP/DGIV/1552/17** del cuatro de septiembre de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

Por tal motivo, con la finalidad de contar con mayores elementos para estar en posibilidad de resolver lo que en Derecho corresponda en relación con la probable contratación, adquisición y/o utilización del software (malware) identificado como "Pegasus", con fundamento en los artículos [...], me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- 1. Indique si la Procuraduría General de la República ha adquirido, comprado, arrendado o se encuentra en posesión, bajo cualquier figura jurídica, de software (malware) identificado como "Pegasus".*
- 2. Precise el nombre, denominación y/o razón social, de la persona física y/o moral de quien haya adquirido el software (malware) identificado como "Pegasus".*
- 3. Describa en qué consiste y como opera" el software (malware) identificado como "Pegasus".*
- 4. Indique de forma detallada las acciones que pueden llevarse a cabo con el software (malware) identificado como "Pegasus", y describa puntualmente cuál es la Información y datos personales a los que se puede tener acceso.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. Señale quiénes son los servidores públicos y/o personal, perteneciente o no a la Procuraduría General de la República, autorizado para la utilización del software (malware) identificado como "Pegasus".
6. Describa los procedimientos técnicos, informáticos y en su caso, legales seguidos para la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".
7. Proporcione copia simple de los convenios, contratos, fallo de licitaciones o cualquier documento físico y/o electrónico, con independencia de su denominación, relacionado con la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".
8. Señale si la Procuraduría General de la República ha utilizado el software (malware) identificado como "Pegasus", y precise cuál es la información y datos personales que ha recabado.
9. De ser el caso, explique en qué situaciones o circunstancias, para qué finalidades y respecto de qué titulares ha utilizado el software (malware) identificado como "Pegasus"; y precise si ha llevado a cabo el tratamiento (obtención, uso, registro, reproducción, conservación, organización, modificación, transmisión y/o cancelación de datos personales a partir del mismo).
10. Manifieste lo que a su derecho convenga respecto de los hechos referidos en el acuerdo del treinta de junio de dos mil diecisiete y, en su caso describa las acciones que la Procuraduría General de la República ha llevado a cabo al respecto, sin limitarse a aquellas derivadas de alguna queja, denuncia o inconformidad relacionada con los mismos.

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad en el domicilio abajo indicado, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la entonces Procuraduría General de la República, el cinco de septiembre de dos mil diecisiete.

40. Mediante el oficio número INAI/SPDP/DGIV/2120/17 del cuatro de septiembre de dos mil diecisiete, en alcance al oficio número INAI/SPDP/DGIV/1410/17 del cuatro de julio de dos mil diecisiete descrito en el **antecedente 9**, la entonces Dirección General de Investigación y Verificación solicitó al director general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Hago referencia al oficio DGAJ/8823/2017 del trece de julio de dos mil diecisiete, recibido en esta Dirección General de Investigación y Verificación en la misma fecha, a través del cual se desahogó el requerimiento que le fue formulado mediante el diverso oficio INAI/SPDP/DGIV/1410/17.

[...]

Por tal motivo, con la finalidad de contar con mayores elementos para estar en posibilidad de resolver lo que en Derecho corresponda, con fundamento en los artículos [...], me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. Señale las personas físicas y/o morales involucradas en los procedimientos que conozca o esté tramitando con motivo de presunta utilización del software (malware) identificado como "Pegasus", precisando el carácter con el que intervienen (denunciante, querellante, víctima, Imputado, Probable responsable, etcétera); puntualizando el número de expediente y el estado procesal de los mismos.
2. Indique qué actividades ha desarrollado la Procuraduría General de la República en relación con los presuntos hechos materia de la presente investigación
3. Asimismo, se requiere que indique lugar y fecha para realizar la consulta de los expedientes que esté tramitando en relación con los hechos vinculados con la presunta utilización del software (malware) identificado como "Pegasus"

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad. En el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento en alcance se notificó a la entonces Procuraduría General de la República, el cinco de septiembre de dos mil diecisiete.

41. El doce de septiembre de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/1552/17**, descrito en el **antecedente 39**.

42. El doce de septiembre de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/2120/17**, descrito en el **antecedente 40**.

43. El doce de septiembre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **DGAJ/10814/2017** de la misma fecha, emitido y signado por el director general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/1552/17** descrito en el **antecedente 39**, indicando lo siguiente:

[...]

*Con fundamento en los artículos 7, 10, fracción VI, de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso fracción II, y 49, fracción V, de su Reglamento, así como en el artículo Primero fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos concentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Director General de Asuntos Jurídicos me refiero a su diverso **INAI/SPDP/DGIV/1552/17**, relativo al expediente **INAI.3S.08.03-003/2017** por el que solicita se proporcione diversa información:*

Sobre el particular, me permito reiterarle que no es posible obsequiar favorablemente su solicitud, en atención a las siguientes consideraciones:

*De la lectura de los artículos 6° y 102, apartado A de la Constitución Política de los Estados Unidos Mexicanos que rigen la actuación de ese órgano garante y de esta Institución, válidamente se arriba a la conclusión de que la utilización de la herramienta tecnológica que menciona en sus oficios, se vierte en hechos que se encuentran sujeto a investigación ministerial, siendo ésta una facultad y atribución exclusiva del Ministerio Público de la Federación, en términos del invocado artículo 102 del Pacto Federal y en la Ley Orgánica de la Procuraduría General de la República, motivo por el cual, se debe insistir en que la materia de investigación del expediente **INAI.3S.08.03-003/2017**, colisiona con la facultad persecutora de delitos que corresponde a la representación social de la Federación.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora bien, en el tema de la información que sobre la base de la investigación que ese órgano garante realiza, estimo de suma importancia destacar el ánimo del legislador permanente que lo llevó a redactar el contenido del artículo 218 del Código Nacional de Procedimientos Penales, mismo que expresamente dispone lo siguiente:

[...]

De la lectura del numeral citado, conviene establecer que el Código Nacional de Procedimientos Penales se vierte en una legislación única que regula, por mandato constitucional, la actividad del Ministerio Público, teniendo el carácter de obligatoria, por ser una cuestión de orden público y de observancia general en toda la República, por los delitos que sean competencia de los órganos jurisdiccionales federales y locales, en el marco de los principios y derechos consagrados en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de los que el Estado mexicano sea parte.

En efecto, a la luz de la reforma al artículo 73, fracción XXI, inciso c), el legislador permanente estableció como facultad exclusiva del Congreso de la Unión, la de expedir la legislación única en materia procedimental penal, de mecanismos alternativos de solución de controversias en materia penal, de ejecución penas y de justicia penal para adolescentes, que regirá en la República en el orden federal y en el fuero común.

*Derivado del texto constitucional invocado, se advierte que el legislador, estableció un régimen especial al calificar como **estrictamente reservados** los registros de la investigación, es decir, en lo atinente al contenido del artículo 218, este dispositivo se expidió atendiendo los principios que se refieren en el párrafo primero del artículo 20 de la Constitución Política de los Estados Unidos Mexicanos, es decir, de publicidad, contradicción, concentración, continuidad e inmediación que rigen para el proceso penal.*

A mayor abundamiento, debe decirse que, en el caso, no se está ante la presencia de alguna de las hipótesis que refiere el último párrafo del citado artículo 218 del Código Nacional de Procedimientos Penales, es decir, en lo tocante a la entrega de una versión pública de las determinaciones de no ejercicio de la acción penal, archivo temporal o de aplicación de un criterio de oportunidad, pues para que ello así ocurriera, deberá haber transcurrido un plazo igual al de prescripción de los delitos de que se trate, de conformidad con lo dispuesto en el Código Penal Federal.

De lo anterior se sigue que el proceso penal, en su fase de investigación, no puede vincularse o equipararse a la garantía de acceso a la información, pues ésta se trata de un derecho guarda relación de forma directa con el principio administrativo de transparencia de la información pública gubernamental.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

*Lo anterior, evidencia que, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y la Procuraduría General de la República, se ubican en ramas opuestas del derecho, es decir, mientras que ese Instituto actúa con base en normas de derecho administrativo, la investigación que realiza esta Procuraduría se circunscribe en el ámbito del derecho penal de ahí que, ante el conflicto que se presenta entre las funciones que constitucionalmente tiene conferidas ese Instituto y esta Procuraduría, priva el principio de especialidad de la norma, es decir, en el caso, prevalece la disposición de **reserva estricta** a que hace referencia el artículo 218 del Código Nacional de Procedimientos Penales.*

Lo anterior es así, máxime si tomamos en consideración que por la acepción "estricta" se entiende todo aquello que es estrecho o que está ajustado a la necesidad o a la ley que por ese hecho no admite interpretación.

Los principios que regulan la actuación del personal que conforma el Ministerio Público de la Federación, son la diferencia de lo que acontece con el personal de este Instituto, materia de continua evaluación y certificación, es decir, la reserva estricta de la información que se contienen las carpetas de investigación está garantizada por los procesos y políticas de evaluación permanente del cumplimiento de los principios que, en el ejercicio de su cargo, se deben observar.

El incumplimiento o inobservancia de los principios será investigado por la Procuraduría General de la Institución, por ser ésta el órgano de vigilancia encargado de sancionar cualquier desvío de los principios que rigen para el personal de esta Procuraduría.

Es oportuno precisar que el Código de Conducta de la Procuraduría General de la República, Base 12.- Deber de confidencialidad, en el comentario sobre este rubro, refiere que la información en el ámbito de la procuración, de justicia requiere de un especial cuidado porque la revelación o mal uso de la misma puede ocasionar serias afectaciones a los aspectos más valiosos para las personas, que son sus libertades, derechos y bienes. De ahí, la importancia de garantizar la ética y diligencia de las y los servidores públicos de la Procuraduría, evitaron cualquier indiscreción, acción u omisión que ponga en riesgo la seguridad de las personas, e incluso de la Institución, la seguridad pública o nacional.

Conviene señalar que si bien la Procuraduría General de la República está obligada a observar las disposiciones generales en materia de reserva de la información contenidas en la Ley General de Transparencia y Acceso a la Información Pública, así como las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, también lo es que está obligada a cumplir con las disposiciones específicas que le marcan las leyes en materia de seguridad nacional y reserva de la información.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

La fracción I del artículo 51 de la Ley de Seguridad Nacional establece que "además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de Seguridad Nacional aquella "cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignent ..." (el subrayado es propio).

Asimismo, el artículo 54 del ordenamiento en cita señala que "la persona que por algún motivo participe o tenga conocimiento de productos, fuentes, métodos, medidas u operaciones de inteligencia, registros o información derivados de las acciones previstas en la presente Ley, debe abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar que lleguen a tener publicidad".

Así, al hacer una interpretación armónica de dos preceptos, se desprende por un lado que, corresponde a las instancias representadas en el Consejo de Seguridad Nacional, entre las que se encuentra esta Procuraduría General de la República, la administración, protección, clasificación, desclasificación acceso de la información que genere o custodie, en los términos de leyes generales y específicas y, por otro lado, que tratándose de información en tema de seguridad nacional, las instancias que pertenecen al Consejo deben abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evita que lleguen a tener publicidad.

En el mismo sentido el artículo décimo séptimo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, prevén lo siguiente:

[...]

Como se puede observar, en el caso que los ocupa, la clasificación de estricta reserva de la información solicitada no obedece a un criterio arbitrario, sino que opera la reserva de la información por Ministerio de Ley, en razón de que existen disposiciones legales tanto generales como específicas, que expresamente mandatan su reserva.

Sobre ese aspecto, se estima que se debe tener en cuenta que aún en aquellos casos en que la información se solicite desagregada, ya sea de forma numérica o estadística, siempre está abierta la posibilidad de que su divulgación pueda comprometer la seguridad nacional. De ahí que es necesario que en cada caso se analice no sólo el tipo de información, sino el impacto que su divulgación podría ocasionar.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En ese orden de ideas, tratándose de información potencialmente afectada por una reserva, especialmente cuando ésta verse sobre un tema vinculado a la seguridad nacional y a la seguridad pública, es imprescindible que no sólo se descarte que no se trate de un tipo de información reservada en términos de los artículos 37, 42, 47 y 48 de la Ley de Seguridad Nacional, sino la posibilidad de que aún fragmentada, ésta pueda en conjunto ser sensible para la seguridad nacional y pública.

Para realizar dicho análisis se debe acudir al derecho comparado, concretamente a criterios doctrinales que se han desarrollado en la intersección de la seguridad nacional con el derecho a la información pública y sobre este punto, tenemos la denomina la "teoría del mosaico".

Esta teoría sostiene que en materia de seguridad nacional para determinar una reserva no debe analizarse de manera aislada la información que se solicita, puesto que una información aparentemente inofensiva puede afectar la seguridad nacional cuando se correlaciona con otras piezas que permitan tener una visión de conjunto del "mosaico".

De esta manera, es posible en algunos no entregar una información solicitada que, si bien sea inocua en sí misma, resulte, como se mencionó, sensible para la seguridad nacional una vez que es puesta conjuntamente con otra información.

[...]

En relación con la solicitud que identifica bajo el numeral 5, me permito comunicarle que la Procuraduría General de la República, para enfrentar de mejor manera el fenómeno delincencial y combatir con mejores herramientas técnicas a las organizaciones criminales, con base en las disposiciones de la Ley de Seguridad Nacional y de la Ley Federal contra la Delincuencia Organizada, ha adquirido sistemas informáticos para combatir dicho fenómeno y actividad delincencial citada.

Asimismo, respecto de la solicitud enumerada con el numeral 5, le comunico que mediante Acuerdo A/018/15 del Procurador General de la República, publicado en el Diario Oficial de la Federación el 23 de febrero de 2015, el Titular de esta Institución, delegó en los servidores públicos que en dicho instrumento jurídico se indican, diversas facultades previstas en el Código Nacional de Procedimientos Penales, concretamente, en su fracción V, del artículo Segundo la facultad de intervenir comunicaciones privadas, de conformidad con lo dispuesto en el artículo 291 del citado Código; así como que mediante nota aclaratoria del citado Acuerdo, publicada en el Diario Oficial de la Federación el 20 de marzo de 2015, se reiteró el contenido de dicha fracción y numeral del Acuerdo citado.

Es importante destacar que los servidores públicos en quienes se delegó la citada facultad, en el ejercicio de la misma, actúan con estricto apego a los derechos humanos y principios



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

reconocidos por la Constitución Política de los Estados Unidos Mexicanos y demás instrumentos jurídicos aplicables, en el caso concreto, los que enumera el párrafo segundo del artículo 1 de la Ley Orgánica de la Procuraduría General de la República.

Respecto a lo solicitado en los numerales 2, 3, 4, 6, 7, 8 y 9, en los términos expuestos relativos a la teoría del mosaico, es decir que no puede entregarse información reservada, aún en el caso de que ésta sea, ya que su divulgación comprometería la seguridad nacional en término de lo dispuesto por los artículos 37, 42, 47 y 48 de la Ley de Seguridad Nacional y estricta reserva de la información a que alude el artículo 218 del Código Nacional de Procedimientos Penales.

No se omite señalar también que, de entregarse información sobre las herramientas de inteligencia que se tienen, se puede poner en peligro la seguridad física de los servidores públicos que las operan, o afectar la investigación a su cargo. Asimismo, proporcionar dato alguno puede llevar a descubrir cómo funciona la técnica de investigación, inferir el tipo de equipo o de software utilizado u otras de sus características, todo lo cual, llevaría a encontrar la manera de neutralizarlas o inutilizarlas. Es por estas razones que nuestra Constitución y la Ley contemplan las reservas para las actividades de seguridad pública y nacional: no es conveniente para la seguridad del Estado, que es responsable de tutelar los derechos humanos de toda población, entregar información a persona o institución alguna que no esté expresamente contemplado en el marco jurídico.

Finalmente, respecto de la manifestación que solicita realice en relación con el acuerdo de treinta de junio de dos mil diecisiete, le comunico que sobre el particular se deberá estar a las consideraciones hechas en el presente documento, respecto de la estricta reserva de la información que integran las investigaciones del estado procesal y la teoría del mosaico a que he hecho referencia.

[...]

44. El doce de septiembre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **DGAJ/10815/2017** de la misma fecha, emitido y signado por el director general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/2120/17** descrito en el **antecedente 40**, indicando lo siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

*Con fundamento en los artículos 7, 10, fracción VI, de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso fracción II, y 49, fracción V, de su Reglamento, así como en el artículo Primero fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos concentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Director General de Asuntos Jurídicos me refiero a su diverso **INAI/SPDP/DGIV/2120/17**, relativo al expediente **INAI.3S.08.03-003/2017** por el que solicita se proporcione diversa información:*

Sobre el particular, me permito reiterarle que no es posible obsequiar favorablemente su solicitud, en atención a las siguientes consideraciones:

[...]

*Derivado del texto constitucional invocado, se advierte que el legislador, estableció un régimen especial al calificar como **estrictamente reservados** los registros de la investigación, es decir, en lo atinente al contenido del artículo 218, este dispositivo se expidió atendiendo los principios que se refieren en el párrafo primero del artículo 20 de la Constitución Política de los Estados Unidos Mexicanos, es decir, de publicidad, contradicción, concentración, continuidad e inmediación que rigen para el proceso penal.*

[...]

De lo anterior se sigue que el proceso penal, en su fase de investigación, no puede vincularse o equipararse a la garantía de acceso a la información, pues ésta se trata de un derecho guarda relación de forma directa con el principio administrativo de transparencia de la información pública gubernamental.

*Lo anterior, evidencia que, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y la Procuraduría General de la República, se ubican en ramas opuestas del derecho, es decir, mientras que ese Instituto actúa con base en normas de derecho administrativo, la investigación que realiza esta Procuraduría se circunscribe en el ámbito del derecho penal de ahí que, ante el conflicto que se presenta entre las funciones que constitucionalmente tiene conferidas ese Instituto y esta Procuraduría, priva el principio de especialidad de la norma, es decir, en el caso, prevalece la disposición de **reserva estricta** a que hace referencia el artículo 218 del Código Nacional de Procedimientos Penales.*

[...]

No se omite señalar también que, de entregarse información sobre las herramientas de inteligencia que se tienen, se puede poner en peligro la seguridad física de los servidores



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

públicos que las operan, o afectar la investigación a su cargo. Asimismo, proporcionar dato alguno puede llevar a descubrir cómo funciona la técnica de investigación, inferir el tipo de equipo o de software utilizado u otras de sus características, todo lo cual, llevaría a encontrar la manera de neutralizarlas o inutilizarlas. Es por estas razones que nuestra Constitución y la Ley contemplan las reservas para las actividades de seguridad pública y nacional: no es conveniente para la seguridad del Estado. que es responsable de tutelar los derechos humanos de toda población, entregar información a persona o institución alguna que no esté expresamente contemplado en el marco jurídico.

Finalmente, respecto de la manifestación que solicita realice en relación con el acuerdo de treinta de junio de dos mil diecisiete, le comunico que sobre el particular se deberá estar a las consideraciones hechas en el presente documento, respecto de la estricta reserva de la información que integran las investigaciones del estado procesal y la teoría del mosaico a que he hecho referencia.

[...]

45. Mediante el oficio número **INAI/SPDP/DGIV/2334/17** del diecinueve de septiembre de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó a la directora general de atención al pleno de este Instituto, lo siguiente:

[...]

Hago referencia al oficio INAI/STP/DGAP/1180/2017 del veinticuatro de agosto de dos mil diecisiete, a través del cual se desahogó el requerimiento que le fue formulado por medio del diverso INAI/SPDP/DGIV/1905/17.

En ese sentido, en el oficio de referencia se informó que, el recurso de revisión RRA 4265/17 fue resuelto por el Pleno de este Instituto el nueve de agosto de dos mil diecisiete, confirmando la respuesta del sujeto obligado. Asimismo, hizo del conocimiento que, de la búsqueda efectuada dentro de la búsqueda de datos relativa a la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público, se localizaran los siguientes recursos de revisión referentes al uso del software (malware) identificado como "Pegasus", a saber:

Expediente, Autoridad Comisionado	Solicitud	Ingreso	Fecha de sesión en que se resolvió	Sentido
--------------------------------------------------	------------------	----------------	---------------------------------------------------	----------------

[Handwritten signature]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

<p>RRA 4744/17 SECRETARÍA DE GOBERNACIÓN (SEGOB) Rosendoevgueni Monterrey Chepov</p>	<p><i>¿Con que objeto se contrató el programa Pegasus y cuanto costo? asimismo se solicita copia escaneada de los contratos relacionados con dicho programa. ¿Por que se espía a periodistas y a luchadores sociales con dicho programa?</i></p>	<p>12/07/2017</p>	<p>En sustanciación</p>	<p>En sustanciación</p>
<p>RRA 5259/17 CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL Areli Cano Guadiana</p>	<p><i>Contratos y Convenios adquiridos para el Sistema de Inteligencia Nacional Contratos y Convenios adquiridos para el Sistema de Inteligencia Nacional con empresas que venden Software para el espionaje especialmente del malware Pegasus por parte de las Secretaría de la Defensa Nacional, Secretaría de Gobernación y el Centro de Investigación y Seguridad.</i></p>	<p>09/08/2017</p>	<p>En sustanciación</p>	<p>En sustanciación</p>



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

	<i>Nacional y cómo se utilizan estos software para espiar a la población mexicana</i>			
--	---------------------------------------------------------------------------------------	--	--	--

Por tal motivo, con fundamento en los artículos [...]; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- 1. Indique cuál es el estado procesal actual del recurso de revisión RRA 4744/17, interpuesto en contra de la Secretaría de Gobernación.*
- 2. Señale cuál es el estado procesal actual del recurso de revisión RRA 5259/17, interpuesto en contra del Centro de Investigación y Seguridad Nacional.*
- 3. Señale si a la fecha del presente, el Pleno de este Instituto ha emitido resolución respecto de los recursos de revisión RRA 4744/17 y RRA 5259/17, sirviéndose remitir copia simple de las mismas, en su caso.*
- 4. Mencione, si tiene conocimiento de algún otro recurso de revisión en materia de acceso a la información y/o protección de datos personales, que se encuentre vinculado con información referente al uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente, el nombre del sujeto obligado en contra de quien se tramitó el asunto, así como su estado procesal, sirviéndose remitir copia de la resolución que, en su caso, haya recaído al mismo.*

*Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo, indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el veintisiete de septiembre de dos mil diecisiete.

46. El dos de octubre de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/2334/17**, descrito en el **antecedente 45**.

47. Mediante el oficio número **INAI/SPDP/DGIV/2438/17** del dos de octubre de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de gobierno abierto y transparencia de este Instituto, lo siguiente:

[...]

Hago referencia a la reunión que se celebró el 15 de septiembre del año en curso, en las instalaciones de este Instituto con integrantes del Núcleo de la Sociedad coordinada por el Comisionado Joel Salas Suárez en la cual, entre otros temas se invitó a las Organizaciones de la sociedad civil para que coadyuvaran en las investigaciones fomentando que los titulares afectados se acerquen a este Instituto para presentar las denuncias respectivas, o bien las presenten como propias Organizaciones que conforman el Núcleo referido.

Derivado de lo anterior, es que le solicito tenga a bien hacer del conocimiento de esta Dirección General si el Núcleo referido o los Titulares de los Datos Personales que presuntamente se vieron afectados por la utilización del malware "Pegasus", le han comunicado la decisión que tomaron sobre el tema referido.

[...]

Le agradeceré haga del conocimiento lo referido con anterioridad, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Gobierno Abierto y Transparencia, el tres de octubre de dos mil diecisiete.

48. El cinco de octubre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP/DGAP/1365/2017** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/2334/17** descrito en el **antecedente 45**, indicando lo siguiente:

[...]

Al respecto, me permito hacer de su conocimiento lo siguiente, por cada punto requerido:

[...]

Respecto del requerimiento 1 y 3 antes citado, esta Dirección General localizó que el recurso de revisión derivado de la respuesta a la solicitud 0000400189617, se interpuso el 12 de julio del 2017, mismo que fue turnado con el número de expediente RRA 4744/17 al Comisionado Rosendoevgueni Monterrey Chepov mismo que fue resuelto por el Pleno de este Instituto el pasado 13 de septiembre del año en curso, en el que se confirmó la respuesta del sujeto obligado y cuya resolución se anexa al presente en copia simple.

En cuanto al requerimiento 2 antes citado, esta Dirección General localizó que el recurso de revisión derivado de la respuesta a la solicitud 0410000018517, se interpuso el 09 de agosto del 2017, mismo que fue turnado con el número expediente RRA 5259/17 a la Comisionada Areli Cano Guadiana, el cual se encuentra en sustanciación.

Ahora bien, en cuanto al requerimiento identificado con el número 4, me permito informarle que esta Dirección General advierte que el único documento por medio del cual puede identificar asuntos dentro de su competencia que se relacionen con el uso del software (malware) identificado como Pegasus", es la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público.

Además, respecto de los medios de impugnación en materia de protección de datos personales, esta Dirección General no concentra el contenido de las solicitudes interpuestas por los particulares, sino únicamente almacena los datos de identificación de los expedientes que son turnados a las Ponencias de este Instituto.

*Así las cosas, se realizó una búsqueda dentro de la base de datos referida previamente, en la que se localizaron hasta la fecha de presentación de su oficio, además de los ya informados en los oficios INAI/STP/DGAP/972/2017, INAI/STP/DGAP/973/2017, INAI/STP/DGAP/1179/2017 y INAI/STP/DGAP/1180/2017, los siguientes recursos de revisión en materia de acceso a la información vinculados con información referente **al uso del software (malware) identificado como "Pegasus"**:*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Expediente, Autoridad y Comisionado	Solicitud	Ingreso o	Fecha de sesión en que se resolvió	Sentido
RRA 5858/17 CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL XPM	<i>Solicito la información en el formato en que se encuentre en las distintas áreas del CISEN que dé respuesta a la siguiente petición que es de interés público: Cantidad de Intervenciones de comunicaciones privadas autorizadas por los jueces competentes, realizadas con la tecnología o software PEGASUS, NSO PEGASUS o PEGASUS 500. Fechas en que se utilizó dicha tecnología para la intervención de comunicaciones privadas autorizadas por un juez. Duración de cada una de las intervenciones de las comunicaciones privadas autorizadas por los jueces, Áreas del CISEN que solicitaron la intervención de las comunicaciones privadas a un juez, Motivación y</i>	<i>01/09/2017</i>	<i>En sustanciación</i>	<i>En sustanciación</i>



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

	<p><i>fundamentación de sus solicitudes de intervención de comunicaciones privadas, Áreas y personal responsable que opero el software PEGASUS, NSO PEGASUS O PEGASUS 500 para las intervenciones autorizadas por un juez, Número de objetivos del Software PEGASUS NSO PEGASUS O PEGASUS 500 utilizados en cada una de las intervenciones de comunicaciones privadas autorizadas por los jueces. ¿Cuántos objetivos o intervenciones de comunicaciones privadas del software PEGASUS, NSO PEGASUS O PEGASUS 500 al 4 de julio de 2017 quedaban sin utilizar? ¿Áreas y personal que ha administrado y operado el software NSO PEGASUS O PEGASUS 500? En el caso de que el software NSO PEGASUS O</i></p>		
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

	<p><i>PEGASUS 500, se utilizará para una o varias intervenciones de comunicaciones privadas NO autorizadas por un juez, señalar el motivo y justificación de su uso, así como las áreas, o personal del CISEN que solicitaron su manejo y quiénes lo operaron. La información la solicito bajo el conocimiento que habrá datos personales o sensibles para las investigaciones que deberán resguardarse, no obstante considero que el interés público que existe sobre la utilización de este software PEGASUS, NSO PEGASUS O PEGASUS 500, compromete y obliga al CISEN PGR a transparentar la información y realizar una versión pública que de respuesta a la presente solicitud de información.</i></p>			
<p>RRA 5889/17 CENTRO DE INVESTIGACIÓN</p>	<p><i>requiero cualquier documento (contrato, convenio, oficio, memorándum, correo</i></p>	<p><i>01/09/ 2017</i></p>	<p><i>08/09/2017</i></p>	<p><i>Desecha</i></p>



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Y SEGURIDAD NACIONAL ACG	<i>electrónico, entre otros) que de cuenta de la adquisición del malware Pegasus, mediante el cual se esta realizando espionaje</i>			
RRA 5890/17 SECRETARÍA DE MARINA OMGF	<i>requiero cualquier documento (contrato, convenio, oficio, memorándum, correo electrónico, entre otros) que de cuenta de la adquisición del malware Pegasus, mediante el cual se esta realizando espionaje</i>		08/09/2017	Desecha
RRA 5891/17 OFICINA DE LA PRESIDENCIA DE LA REPÚBLICA MPKV	<i>requiero cualquier documento (contrato, convenio, oficio, memorándum, correo electrónico, entre otros) que de cuenta de la adquisición del malware Pegasus, mediante el cual se esta realizando espionaje</i>	01/09/2017	En sustanciación	En sustanciación
RRA 5895/17 SECRETARÍA DE LA DEFENSA NACIONAL (SEDENA)	<i>requiero cualquier documento (contrato, convenio, oficio, memorándum, correo electrónico, entre otros) que de cuenta de la adquisición del malware Pegasus, mediante el cual se esta realizando espionaje</i>	01/09/2017	En sustanciación	En sustanciación



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

RRA 6309/17 PROCURADURÍA A GENERAL DE LA REPÚBLICA (PGR) ACG	<i>"del sistema Pegasus y de los equipos que actualmente operan para intervenir teléfonos, se solicita la fecha, el número de oficio, número de carpeta de investigación, hora, jueces que autorizaron la intervención de teléfonos por número consecutivo máxima publicidad / contrato de los nuevos equipos y plataformas que están usando para intervención de teléfonos, solicitudes a las empresas de telefonía celular con los mismos datos y máxima publicidad solicitada con todos los datos solicitados, de todos los teléfonos intervenidos, se solicita los casos concretos donde se aprendió al delincuente que deberá de informar sin reserva alguna los casos que causaron estado, se rescató a una secuestrado, [...] se solicita versión pública de los nuevos contratos y</i>	<i>18/09/ 2017</i>	<i>En sustanciación</i>	<i>En sustanciación</i>
-----------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------	-----------------------------	-------------------------



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

	<i>plataformas que emplea la PGR, número de trabajadores salario, prestaciones que tienen los que se desempeñan en estas actividades y que áreas delincuenciales.se opera la intervención, de teléfonos, ejemplo secuestros, lavado de dinero, fraude, extorsión, ETC</i>			
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Resulta necesario recalcar que, dentro de las actividades competencia de esta Dirección General, no se encuentra la de llevar a cabo análisis normativo o de cualquier otro tipo del cuerpo de las resoluciones emitidas por el Pleno de este Instituto, de tal manera que la única fuente de información con la que cuenta esta Unidad Administrativa; para efectos de la atención a su requerimiento, es la base de datos previamente indicada.

Aunado a lo anterior, esta Unidad Administrativa informa que los documentos del carácter público tales como solicitudes, estudios, resoluciones, entre otros, que pudiesen ser de su interés pueden ser localizados y consultados en el Buscador de Solicitudes de Información y Recursos de Revisión.

A través de ese buscador, es posible ubicar aquellos documentos relacionados adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus".

[...]

a) Adjunto, se remitieron las siguientes resoluciones y acuerdos:

- Resolución al recurso de revisión **RRA 4744/17**, en la que se determinó **confirmar** la respuesta de la Secretaría de Gobernación, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el trece de septiembre de dos mil diecisiete.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Acuerdo dictado en el **RRA 5889/17** en el que se determinó **desechar** por improcedente el recurso de revisión interpuesto en contra del Centro de Investigación y Seguridad Nacional, el ocho de septiembre de dos mil diecisiete.
- Acuerdo dictado en el **RRA 5890/17** en el que se determinó **desechar** por extemporáneo el recurso de revisión interpuesto en contra de la Secretaría de Marina, el ocho de septiembre de dos mil diecisiete.

49. El nueve de octubre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/SAI/DGGAT/00207/17** de la misma fecha, emitido y signado por el director general de gobierno abierto y transparencia de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/2438/17** descrito en el **antecedente 47**, indicando lo siguiente:

[...]

Me refiero a su oficio INAI/SPDP/DGIV/2438/17, correspondiente al expediente INAI.3S.08.03-003/2017; mediante el cual hace alusión a la reunión celebrada el 15 de septiembre de 2017, coordinada por el Comisionado Joel Salas Suárez, en la que estuvieron presentes servidores públicos adscritos a las áreas técnicas en las materias de acceso a la información y protección de datos personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y algunos de los representantes del Núcleo de Organizaciones de la Sociedad Civil que han participado de los trabajos de la Alianza para el Gobierno Abierto en México.

En relación con dicha reunión, su oficio resalta lo siguiente:

- 1. La recomendación que la Secretaría de Protección de Datos Personales realizó a los representantes del núcleo de Organizaciones de la Sociedad Civil (OSC) para que coadyuvaran en las investigaciones que está llevando a cabo la Dirección General de Investigación y Verificación, y con ello fomentar que los titulares afectados se acerquen al INAI para presentar las denuncias respectivas, o bien, que éstas se presenten por las OSC que integran el núcleo.*
- 2. La alusión al acuerdo alcanzado con el Núcleo de las OSC para que mantengan informado a este Instituto respecto de la posibilidad que los titulares de los datos*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

personales que se sientan afectados, o el propio Núcleo, presenten sus respectivas denuncias.

3. *La solicitud a esta Dirección General de Gobierno Abierto y Transparencia de informar si el Núcleo de OSC o los titulares de los datos personales que presuntamente se vieron afectados por la utilización del malware "Pegasus" han comunicado la decisión de presentar o no denuncias sobre el caso en comento ante este Instituto.*

Al respecto, me permito emitir las siguientes manifestaciones:

1. *Si bien esta Dirección General asistió a la reunión y se encontraba presente al momento de la definición del acuerdo al que hace alusión, se considera que para aseverar la celebración del acuerdo y tener un soporte que acredite la manifestación de las ideas vertidas durante su desarrollo, es necesario que la minuta de la reunión sea firmada por todas las personas que estuvieron presentes.*
2. *Si bien, a la fecha el Núcleo de las OSC no ha hecho del conocimiento de esta Dirección General la decisión tomada al respecto de presentar o no una denuncia ante este Instituto; se considera fundamental puntualizar lo siguiente:*
 - a. *Como se establece en el proyecto de minuta de la reunión del pasado 15 de septiembre, se acordó que se abrirían dos mesas de trabajo para atender las inquietudes del Núcleo de las OSC en materia de transparencia y acceso a la información y protección de Datos Personales, mismas que serían coordinadas por las Secretarías de Acceso a la Información y de Protección de Datos Personales, respectivamente.*
 - b. *Al desconocer los alcances que tendrá esta respuesta -respecto del desconocimiento de la decisión de los afectados o del Núcleo de las OSC de presentar o no una denuncia ante este Instituto-; esta Dirección General sugiere que se solicite formalmente y de manera directa a los afectados o, en su caso, a los representantes que tengan la capacidad jurídica para actuar a nombre y por cuenta de éstos, que manifiesten la decisión de presentar o no la denuncia.*
 - c. *La redacción del acuerdo que se encuentra en el proyecto de minuta de la reunión celebrada el pasado 15 de septiembre, a la letra dice:*

"El Núcleo del OSC valorarían la posibilidad de presentar las denuncias correspondientes dentro de los procedimientos de investigación que se tramitan referentes al malware "Pegasus", así como analizarían la viabilidad de que los



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

*Titulares de datos personales acudieran a interponer también sus denuncias.”
(Sic)*

Al respecto, salta a la vista -para efectos de la interpretación que se pueda desprender del silencio del Núcleo de las OSC- que no se estableció una fecha compromiso para informar a este Instituto la decisión de presentar o no una denuncia.

- d. *Como se indica en el texto del proyecto de minuta, el Núcleo de las OSC solicitó se les informara qué se necesita para iniciar un procedimiento de verificación, con el objetivo de determinar si éste es conveniente para los titulares de los datos personales en los procedimientos de investigación que actualmente tramita el INAI. Asimismo, indicaron que desde su perspectiva existen los indicios suficientes para iniciar el procedimiento de verificación de manera oficiosa y que por lo tanto han recomendado a los afectados no presentar denuncia alguna, hasta que se definan estándares de prueba. Así, como lo refiere el proyecto de minuta, uno de los temas centrales de la reunión fue el cuestionamiento a la sugerencia del INAI de involucrar en el procedimiento de verificación a los titulares de los datos personales, toda vez que el Núcleo de las OSC actualmente lo considera innecesario.*

Es así que, en el marco de las actuaciones que realiza esta Dirección General en las materias de Gobierno y Transparencia Proactiva, con base en el artículo 40 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, se sugiere que previo a la eventual apertura -o en el marco- de un procedimiento de verificación, se difunda de manera proactiva información pública útil y de calidad al Núcleo de las OSC, que les permita disminuir las asimetrías de información que actualmente se observan en el conocimiento de las distintas hipótesis para iniciar un procedimiento de verificación, sus alcances, el nivel acceso a la información a los expedientes en cada caso, entre otra que se considere necesaria para que cuenten con los elementos suficientes para tomar una decisión sobre presentar o no una denuncia.

Dicho ejercicio de construcción de conocimiento útil, será determinante, certeza que se dé a la sociedad sobre el desarrollo de las actuaciones del INAI en el presunto caso de espionaje; considerando que éstas no sólo tendrán un impacto directo en los afectados, sino en la colectividad. Asimismo, esto abonaría al cumplimiento de la misión de este Instituto de garantizar la protección de datos personales y promover una cultura de debido tratamiento de dichos datos para el fortalecimiento de una sociedad incluyente y participativa.

Es así que, la apertura y las acciones de construcción de conocimiento útil antes referidas son consideradas por esta Dirección General, de mayor trascendencia en el marco del caso en



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

comento y para el desarrollo de las actuaciones de investigación y verificación que se lleven a cabo, dado que brindarán certeza a los afectados y a la colectividad no sólo en materia de legalidad, sino de los esfuerzos que este instituto lleva a cabo para impulsar acciones con un enfoque de derechos humanos en su labor cotidiana.

[...]

50. El once de octubre de dos mil diecisiete, el entonces director general de investigación y verificación, emitió un acuerdo en el que se determinó que dado que no se recibió denuncia formal de titular y/o titulares de datos personales presuntamente afectados por la operación del *software*, debía **emitirse el edicto** correspondiente, a efecto de notificar a los titulares de los datos personales que tuvieron una presunta afectación en el caso concreto, con la finalidad de que comparezcan en el domicilio de este Instituto para presentar formalmente su denuncia cumpliendo los requisitos mínimos establecidos por la normatividad aplicable, manifestar lo que a su derecho convenga, aportar pruebas y señalar un domicilio cierto y determinado para recibir notificaciones.

51. Mediante el oficio número **INAI/SPDP/DGIV/2569/17** del once de octubre de dos mil diecisiete, con el objeto solicitar su colaboración, la entonces Dirección General de Investigación y Verificación requirió al director general de asuntos jurídicos de este Instituto, lo siguiente:

[...]

*Me permito hacer de su conocimiento que, la Dirección General de Investigación y Verificación a mi cargo, se encuentra en trámite el procedimiento de investigación con número de expediente INAI.3S.08.03-003/2017, mismo que fue iniciado de forma oficiosa y en el cual se advierte la supuesta existencia de personas físicas que posiblemente podrían estar involucradas en alguna probable afectación debido, a la utilización del *software* (malware) identificado como "Pegasus".*

Sin embargo, este organismo constitucional autónomo no ha recibido formalmente documento alguno por parte de algún titular que haya denunciado algún presunto incumplimiento en materia de protección de datos personales, por lo que se desconoce el nombre y domicilio de las referidas personas físicas.

*Ante la imposibilidad de notificar personalmente a los titulares de los datos personales que pudieran resultar presuntamente afectadas por la utilización del *software* (malware)*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

denominado "Pegasus", con fundamento en los artículos [...], se determinó procedente realizar la notificación correspondiente mediante edicto, con la finalidad de que comparezcan en el domicilio del Instituto para que presenten formalmente su denuncia cumpliendo los requisitos mínimos establecidos por la normatividad aplicable, manifiesten lo que a su derecho convenga, aporten pruebas y señalen un domicilio cierto y determinado en esta Ciudad de México para recibir notificaciones, en el procedimiento de investigación INAI.3S.08.03-003/2017.

Por lo anterior, solicito su apoyo para llevar a cabo los trámites necesarios para la publicación del edicto, sugiriendo que lo anterior pudiera realizarse a partir del trece de marzo de dos mil diecisiete, se adjunta al presente la impresión que contiene el texto del edicto que se requiere publicar.

[...]

La solicitud se notificó a la Dirección General de Asuntos Jurídicos, el once de octubre de dos mil diecisiete.

a) Adjunto a la solicitud, se remitió la propuesta de edicto a publicar:

[...]

EDICTO

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Titulares de datos personales que tuvieron una presunta afectación derivada de la operación del software (malware) denominado "Pegasus".

En los autos del expediente de investigación INAI.3S.08.03-003/2017, tramitado en la Dirección General de Investigación y Verificación, de la Secretaría de Protección de Datos Personales Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el doce de octubre de dos mil diecisiete, se dictó un acuerdo, cuyo numeral Tercero a la letra dice:

"... TERCERO.- En virtud de que en la Dirección General de Investigación y Verificación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, no existe registro alguno de haberse recibido denuncia formal de Titular y/o Titulares de datos personales presuntamente afectados por la operación del software



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

(malware) denominado "Pegasus", y, en consecuencia, tampoco se cuenta con domicilio alguno en el cual realizar actuaciones, SE ORDENA NOTIFICAR a los titulares de datos personales que tuvieron una presunta afectación derivada de la operación del software (malware) identificado como Pegasus", en el caso concreto, por medio de edicto publicado en el Diario Oficial de la Federación y en un periódico de circulación nacional por tres días consecutivos, a efecto de que en el término de TREINTA DÍAS hábiles, contados a partir del día siguiente a la última publicación, comparezcan en el domicilio del Instituto para que presenten formalmente su denuncia cumpliendo los requisitos mínimos establecidos por la normatividad aplicable, manifiesten lo que a su derecho convenga, aporten pruebas y señalen un domicilio cierto y determinado en esta Ciudad de México para recibir notificaciones, en el procedimiento de investigación con número de expediente INAI.3S.08.03.003/2017. Asimismo, se hace de su conocimiento que transcurrido el plazo otorgado sin que se presente denuncia alguna, esta autoridad procederá emitir la Resolución que en derecho corresponda.

En ese sentido, con fundamento en los artículos 9, párrafo primero, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 5, párrafo segundo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 32, 35, fracción III, 37 y 38, tercer párrafo, de la Ley Federal de Procedimiento Administrativo; y 315 del Código Federal de Procedimientos Civiles, ambos ordenamientos de aplicación supletoria a las leyes de la materia; 5, fracción X, letra p., 29, fracciones XXX y XXXVIII, y 41, fracciones I, VI y IX, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; 8, fracción IV, de los Lineamientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones; se ordena notificar a los titulares de los datos personales que tuvieron una presunta afectación en el caso concreto, por medio de edicto publicado en el Diario Oficial de la Federación y en un periódico de circulación nacional por tres días consecutivos. a efecto de que, en el término de TREINTA DÍAS hábiles, contados a partir del día siguiente a la última publicación, comparezca en Avenida Insurgentes Sur número 3211, Colonia Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, Ciudad de México, y presenten formalmente su denuncia cumpliendo los requisitos mínimos establecidos por la normatividad aplicable, manifiesten lo que a su derecho convenga, aporten pruebas y señalen un domicilio cierto y determinado, en esta Ciudad de México para recibir notificaciones. en el procedimiento de investigación con número de expediente INAI.3S.08.03-003/2017; asimismo, se hace de su conocimiento que transcurrido el plazo otorgado sin que se presente denuncia alguna, esta autoridad procederá a emitir la Resolución que en derecho corresponda.

[...]

Al respecto, resulta importante mencionar que en el expediente obran las copias de los edictos publicados en el Diario Oficial de la Federación el diecisiete, dieciocho y



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

diecinueve de octubre de dos mil diecisiete; así como, los publicados en los diarios de circulación nacional el diecisiete, diecinueve y veinte de octubre de dos mil diecisiete.

52. El dieciséis de octubre de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/2569/17**, descrito en el **antecedente 51**.

53. El cuatro de diciembre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el escrito presentado por la Red en Defensa de los Derechos Digitales A.C., en el que manifestó:

[...]

Que, por medio del presente escrito, de conformidad con lo que señala el artículo 147, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante "LGDPPSO"), se presenta DENUNCIA de hechos violatorios de diversas disposiciones de la LGDPPSO y de otras leyes aplicables en la materia.

A efectos de cumplir con los requisitos formales que establece el artículo 148 de la LGDPPSO se señala lo siguiente:

I.- NOMBRE DE LAS DENUNCIANTES:

[...]

II.- DOMICILIO O MEDIO PARA RECIBIR NOTIFICACIONES:

[...]

III.- AUTORIDADES RESPONSABLES DENUNCIADAS:

- *La AGENCIA DE INVESTIGACIÓN CRIMINAL de la PROCURADURÍA GENERAL DE LA REPÚBLICA y los funcionarios adscritos a estas y otras dependencias federales encargados de operar el sistema para la intervención de comunicaciones privadas denominado "PEGASUS" así como aquellas encargadas de hacer tratamiento de los datos personales obtenidos mediante la operación de dicho sistema.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Las demás autoridades federales que resulten responsables.*

IV.- HECHOS DENUNCIADOS

A. EL MALWARE PEGASUS

En agosto de 2016, el Citizen Lab de la Universidad de Toronto publicó un reporte en el que se documenta el uso del malware Pegasus en contra del activista Ahmed Mansoor en los Emiratos Árabes Unidos.

En términos generales, el modus operandi de la infección consiste en el envío de un SMS al objetivo, con un mensaje que busca engañarlo para hacer clic en un enlace adjunto. Al hacer clic en el enlace, el navegador se abre y redirige al objetivo a uno de los sitios web de la infraestructura de NSO Group, dándole la oportunidad al malware de instalarse en el dispositivo gracias a una vulnerabilidad en el sistema operativo. De este modo, el atacante gana acceso a los archivos guardados en el equipo, así como a los contactos, mensajes y correos electrónicos.

Mansoor había recibido mensajes de texto que supuestamente contenían "secretos" sobre los detenidos torturados en las cárceles de EAU. Dicha información podía ser consultada al hacer clic en un enlace. En lugar de acceder a la liga, Mansoor envió los mensajes de texto al Citizen Lab. Los investigadores reconocieron que los enlaces estaban relacionados con la infraestructura de NSO Group, una empresa de software de espionaje que comercializa Pegasus, un spyware de "intercepción legal" para gobiernos.

Los investigadores del Citizen Lab sospecharon que la infección se daba al hacer clic en el enlace enviado al objetivo, en cual dirigía hacia uno de los dominios de la infraestructura de NSO Group. Para comprobar esta hipótesis, los investigadores utilizaron un iPhone 5 nuevo con la misma versión de sistema operativo que el celular de Mansoor (iOS 9.3.3). Ingresaron manualmente la dirección URL proporcionada a Mansoor en el SMS en el navegador Safari. Al acceder el enlace, apareció una página en blanco y, posteriormente, el navegador se cerró. Mientras tanto, descubrieron que un software desconocido fue implantado en el dispositivo.

El Citizen Lab descubrió que Pegasus explotaba una vulnerabilidad de seguridad inédita (zero-day exploit) en el sistema operativo iOS, bautizada como Trident. A través de esta infección, se hacía jailbreak al dispositivo y se instalaba un sofisticado software que habría permitido al atacante tomar control de diferentes funciones y acceder a los contenidos del aparato. Entre los permisos adquiridos, se encuentran:

- *Acceso a la información guardada en el dispositivo como: archivos, datos del calendario, listas de contactos, contraseñas, entre otros.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

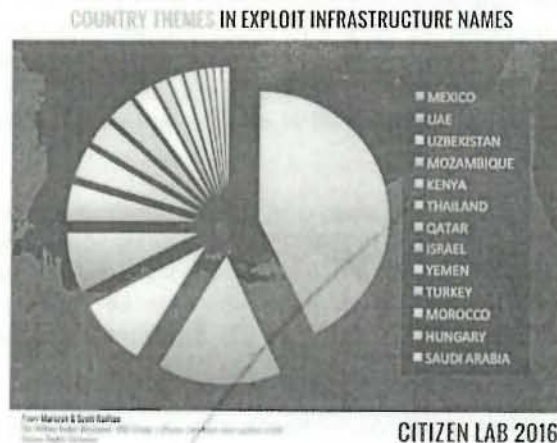
DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Acceso a mensajes de texto, así como datos de otras aplicaciones como Gmail, WhatsApp, Skype, Facebook, Telegram.
- Acceso a escuchar llamadas realizadas por teléfono, a través de WhatsApp o Viber.
- Permisos para grabar activa o pasivamente utilizando el micrófono y la cámara del dispositivo.

En dicha investigación, Citizen Lab logró identificar la infraestructura utilizada por Pegasus, incluyendo diversos dominios que buscaban suplantar la identidad de sitios web de telecomunicaciones, noticias, redes sociales, entre otros. El reporte descubrió que, por mucho, México era el país al que está dedicada mayor parte de su infraestructura:

Gráfico 1 Proporción de dominios asociados a la infraestructura de Pegasus por país



Entre los dominios identificados, se encuentran:

- *Unonoticias.net*
- *Univision.clic*
- *lusacell-movil.com.mx*
- *YOutube.com.mx*
- *Fb-accounts.com*
- *Googleplay-store.com*
- *Whatsapp-app.com*
- *smsmensaje.mx*

B. ATAQUES CON PEGASUS EN MÉXICO



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Diversas investigaciones realizadas por Citizen Lab, R3D, ARTICLE 19 y SocialTIC han documentado ataques con el malware Pegasus en México. En atención al principio de economía procesal, se comparten los enlaces electrónicos de dichas publicaciones, las cuales deben tenerse por reproducidas como si a la letra se insertasen:

Publicaciones de Citizen Lab:

- *Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links (Febrero 11, 2017: <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware>)*
- *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware (Junio 19, 2017: <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>)*
- *Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware (Junio 29, 2017: <https://citizenlab.ca/2017/06/more-mexican-nso-targets/>)*
- *Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware (Julio 10, 2017: <https://citizenlab.ca/2017/07/mexico-disappearances-nso/>)*
- *Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware (Agosto 2, 2017: <https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/>)*
- *Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware (Agosto 30, 2017: <https://citizenlab.ca/2017/98/nso-spyware-mexico-corruption/>)*

Publicaciones de R3D, ARTICLE 19 y/o SocialTIC:

- *Destapa la Vigilancia: promotores del impuesto al refresco espiados con malware gubernamental (Febrero 11, 2017 <https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/>)*
- *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México (Junio 19, 2017 <https://r3d.mx/gobiernoespia>)*
- *Confirman que GIEI también fue objetivo del #GobiernoEspía (Julio 10, 2017 <https://r3d.mx/2017/07/10/giei-gobierno-espia/>)*

Los casos documentados en las publicaciones mencionadas son producto de un proceso de investigación conjunta entre R3D, ARTICLE 19, SocialTIC y Citizen Lab consistente, manera esencial, en la identificación y recolección de mensajes de texto SMS sospechosos y el análisis realizado por Citizen Lab de los enlaces contenidos en los mismos. Producto de dicho análisis, Citizen Lab ha concluido que dichos mensajes constituyen ataques para infectar dispositivos de comunicación móvil con el malware Pegasus.

(...)



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Finalmente, cabe señalar que, según todas las fuentes de información disponibles, incluyendo comunicados públicos de la empresa NSO Group "dicha empresa únicamente comercializa sus productos a gobiernos "exclusivamente para prevenir e investigar el terrorismo y el crimen". Inclusive, un ejecutivo de NSO Group, en entrevista para el diario israelí Haaretz, confesó que de haber sabido que el gobierno mexicano iba a abusar de su producto para espiar a periodistas y defensores de derechos humanos no se lo habrían vendido.

De todo lo anterior resulta claro que agencias del gobierno mexicano, en particular la AIC, adquirieron y utilizaron el sistema Pegasus para adquirir y tratar datos personales mediante la intervención de comunicaciones privadas. A su vez resulta claro que alguna de esas agencias realizó ataques en contra de periodistas, defensores de derechos humanos, activistas y un número indeterminado de personas, respecto de las cuales potencialmente realizó el tratamiento de sus datos personales de manera continua.

D. CONSIDERACIONES JURÍDICAS

Los hechos descritos en la denuncia en particular la adquisición y utilización regular del malware Pegasus, así como el subsecuente y continuo tratamiento de datos personales representan claros indicios de incumplimiento de las disposiciones de la LGPDPPSO por parte de autoridades federales, en especial la AIC de la PGR. En concreto, se advierte la probable violación de los artículos 16, 17, 18, 19, 25, 80, 81 y 82 de la LGPDPPSO.

Para dimensionar las probables violaciones es preciso hacer referencia al contexto normativo que regula el tratamiento de datos personales mediante la intervención de comunicaciones. En particular, es necesario hacer referencia al marco jurídico nacional e internacional en materia de derechos humanos relacionado con las interferencias encubiertas en el derecho a la privacidad.

(...)

Aplicación de los principios a los hechos denunciados

A la luz de las normas de derechos humanos y el marco jurídico que regula la vigilancia gubernamental en México, la utilización del malware Pegasus, en particular, los casos de espionaje a periodistas, defensores de derechos humanos y activistas anticorrupción son absolutamente insostenibles jurídicamente y, por el contrario, apuntan a la comisión de graves delitos y violaciones a derechos humanos.

a. La utilización del malware de espionaje Pegasus no cumple con el principio de legalidad



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Como fue mencionado anteriormente, por las características de alta invasividad y secrecía, las facultades de vigilancia gubernamental deben estar estricta y detalladamente reguladas en una ley formal y material. En este sentido, no puede considerarse que las normas que contemplan la "intervención de comunicaciones privadas" constituyen base legal suficiente para la utilización de herramientas tan poderosas e invasivas como los ataques con malware de espionaje. Por lo tanto, la utilización de estas herramientas, sin una norma legal que las regule específicamente debe considerarse violatoria de los derechos humanos.

b. El espionaje difícilmente contó con autorización judicial federal

Aun si los ataques con malware de espionaje con las características de Pegasus fueran considerados como una forma más de "intervención de comunicaciones privadas", resulta altamente improbable que una autoridad judicial federal hubiera autorizado este tipo de invasiones a la privacidad de periodistas, defensores de derechos humanos y activistas anticorrupción. La ausencia del control judicial previo sería una grave violación a la ley y a los derechos de las personas afectadas. Al día de hoy, ni la AIC, ni el Poder Judicial Federal han accedido a otorgar información respecto a sí el uso del malware Pegasus cuenta con un control judicial federal previo y permanente.

c. El espionaje no persigue un fin legítimo

Para que las personas atacadas con malware referenciadas en este informe pudieran considerarse como objetivos legítimos de medidas de vigilancia legal, la autoridad tendría que demostrar que todos los periodistas, defensores de derechos humanos y activistas anticorrupción se encontraban bajo investigación criminal. existan indicios suficientes para acreditar que se encontraban organizando la comisión de delitos o que, de alguna manera, todos los objetivos constituyen una amenaza inminente a la seguridad nacional.

Claramente, ninguna de las circunstancias descritas se actualiza respecto de los objetivos del espionaje gubernamental. Por el contrario, existen indicios de que la labor de interés público que realizan y que han afectado intereses particulares y de algunos funcionarios del gobierno federal habrían motivado los ataques con el malware de espionaje. Lo anterior no constituye un fin legítimo para la vigilancia de persona alguna.

d. El espionaje mediante el malware Pegasus no es una medida necesaria ni proporcional

Aun en el remoto caso de que- existiera una finalidad legítima para vigilar a todas las personas objeto de este informe, es claro que la utilización de una herramienta tan invasiva y poderosa como el malware Pegasus no podría ser considerada una medida necesaria o proporcional.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Como fue señalado anteriormente, el cumplimiento de los principios de necesidad y proporcionalidad requiere que únicamente sea utilizada la medida que constituya la medida menos lesiva disponible para conseguir el objetivo legítimo. En este caso, es claro que el perfil de las personas que fueron atacadas con intentos de infección con el malware Pegasus no justifica la utilización de esta herramienta. Resulta inexplicable por qué, en todo caso, no serían suficientes otras técnicas de investigación menos invasivas, costosas y respecto de las cuales es necesaria la colaboración de empresas de telecomunicaciones, como la intervención de comunicaciones privadas tradicional.

Lo anterior sugiere que la elección de la herramienta de espionaje no guarda relación con la peligrosidad o capacidades de elusión de los objetivos sino con el intento deliberado de ocultar los intentos de espionaje dada su ilegalidad.

e. Los atacantes cometieron delitos graves

En caso de que, en efecto, como toda la evidencia sugiere, los intentos de infección de los dispositivos de periodistas, defensores de derechos humanos y activistas anticorrupción con el malware de espionaje Pegasus, comercializado exclusivamente a gobiernos por la empresa NSO, fueron llevados a cabo de manera ilegal, sin autorización judicial y para fines ilegítimos, es claro que se acreditaría la comisión de diversos delitos.

De manera destacada, podría haberse cometido el delito de intervención ilegal de comunicaciones privadas, contemplado en el artículo 177 del Código Penal y considerado un delito grave, por el cual resulta aplicable una pena de 6 a 12 años de prisión.

Igualmente, se habría cometido el delito de acceso ilícito a sistemas y equipos de informática, contemplado en el artículo 211 Bis 1 del Código Penal Federal, por el cual puede imponerse una pena de hasta dos años. Lo anterior, sin perjuicio de otros delitos que podrían haberse cometido en paralelo.

f. Violaciones a la LGPDPPSO

Existen indicios suficientes para considerar, de manera fundada y motivada, la probable comisión de violaciones a la LGPDPPSO. En concreto se advierten las probables violaciones siguientes:

- El responsable no habría observado los principios de licitud, finalidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales mediante la utilización del malware Pegasus y el subsecuente tratamiento de los datos obtenidos mediante dicho sistema en violación del artículo 16 de la LGPDPPSO.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *El tratamiento de datos personales por parte del responsable no se habría sujetado a las facultades y atribuciones que la normatividad le confiere en violación del artículo 17 de la LGPDPPSO.*
- *El tratamiento de datos personales no se encontraría justificado por finalidades concretas, lícitas, explícitas y legítimas ni relacionadas con las atribuciones que la normatividad aplicable les confiere en violación del artículo 18, 80 y 81 de la LGPDPPSO.*
- *El responsable obtiene datos personales a través de medios engañosos y fraudulentos, como lo es el modus operandi del sistema Pegasus en violación del artículo 19 de la LGPDPPSO.*
- *El responsable utiliza herramientas para la obtención, tratamiento de datos personales que no cumplen con los criterios de adecuación, relevancia y estricta necesidad para la finalidad que justifica su tratamiento en violación del artículo 25 de la LGPDPPSO.*
- *La obtención y tratamiento de datos personales mediante el sistema Pegasus por parte de una instancia de procuración de justicia como lo es la AIC de la PGR, no cumple con los principios de necesidad y proporcionalidad a los que se refiere el artículo 80 de la LGPDPPSO.*
- *El responsable no habría establecido medidas de seguridad para evitar un tratamiento no autorizado de datos personales mediante la utilización del sistema Pegasus, en violación del artículo 82 de la GPDPPSO.*

Sobre la procedencia del inicio del procedimiento de verificación

De conformidad con lo que señala el artículo 146 de la LGPDPPSO, este Instituto tiene la atribución de "vigilar y verificar el cumplimiento de las disposiciones contenidas" en la LGPDPPSO.

En este sentido, el artículo 147 de la LGPDPPSO dispone que este Instituto puede iniciar el procedimiento de verificación cuando cuente con "indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes" o cuando cualquier persona interponga denuncia en casos en que "tenga conocimiento de presuntos incumplimientos a las obligaciones previstas" en la LGPDPPSO.

De los hechos denunciados se desprende la actualización del supuesto para que este Instituto puede iniciar de manera oficiosa el procedimiento de verificación en tanto existen indicios que hacen presumir, de manera fundada y motivada, la existencia de violación a la LGPDPPSO.

Asimismo, mediante este escrito de denuncia se encuentra satisfecho un supuesto alternativo para la apertura del procedimiento de verificación, en tanto que, como lo señala la Ley, basta con la presentación de denuncia en la que el denunciante exprese su conocimiento de presuntos incumplimientos a las obligaciones previstas.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Cabe resaltar que la legislación no exige que los incumplimientos se encuentren probados de manera fehaciente, sino que existan indicios que hagan presumir que esos incumplimientos podrían haberse dado. En este sentido, el estándar de presunción prima facie para la apertura del procedimiento de verificación se encuentra más que acreditado. Será el propio Instituto, mediante las amplias facultades de investigación que posee, la que podrá allegarse de más indicios y pruebas, inaccesibles para esta parte denunciante, que podrán confirmar o descartar las violaciones alegadas.

Sobre la competencia temporal del Instituto

Resulta pertinente resaltar que, en consideración de esta parte denunciante, este Instituto no posee limitaciones temporales para investigar, a través del procedimiento de verificación, las violaciones a la LGPDPPSO; relacionadas con la utilización del malware Pegasus denunciadas en este escrito.

Si bien, la LGPDPPSO entró en vigor el 29 de enero de 2017, el procedimiento de verificación debería, en cumplimiento de sus obligaciones y de la esencial función de protección de derechos humano que desempeña, analizar los hechos denunciados de manera integral en tanto:

- 1) *El procedimiento de verificación tiene como objeto la investigación y verificación del cumplimiento de la LGPDPPSO, con independencia de la identificación de víctimas específicas de dichos incumplimientos. En este sentido, si bien la utilización del malware Pegasus y algunos tratamientos de datos personales, presuntamente violatorios de la LGPDPPSO habrían iniciado con anterioridad a la entrada en vigencia de la LGPDPPSO, no existe indicio alguno de que la utilización de dicho sistema habría cesado antes del 29 de enero de 2017, sino que se presume que dicho sistema continua siendo utilizado por la AIC de la PGR.*
- 2) *Aun cuando el inicio del ilegal tratamiento de datos personales, en algunos casos específicos, habría iniciado con anterioridad a la vigencia de la LGPDPPSO, es razonable presumir que el tratamiento de la información obtenida mediante el sistema Pegasus fue permanente y continuo, inclusive hasta el día de hoy. Por lo tanto, es claro que la naturaleza continuada y compleja de la conducta violatoria faculta a este Instituto a analizar de manera integral las violaciones.*

En este sentido, es claro que el Instituto posee competencia temporal para verificar si la AIC y otras autoridades federales ha cumplido con sus obligaciones en materia de protección de datos personales al llevar a cabo medidas de vigilancia e intervención de comunicaciones privadas, en particular mediante la utilización del malware Pegasus.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En su caso, si de la investigación del Instituto se desprende la improbable circunstancia de que el sistema Pegasus dejó de ser utilizado antes de la entrada en vigor de la LGPDPPSO o que los datos obtenidos con anterioridad dejaron de ser sujetos de tratamiento, el Instituto estaría en posibilidad de determinar lo conducente. De manera contraria, la no apertura del procedimiento de verificación respecto de los hechos denunciados de manera integral, impediría de manera irremediable el cumplimiento de las obligaciones de vigilancia y verificación del Instituto, incumpliendo así el efecto útil de la LGPDPPSO.

Por lo expuesto y fundado.

A ESE H. INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

PRIMERO.- Tener por presentado el presente escrito, autorizando en sus términos a las personas que al inicio del mismo se indican.

SEGUNDO.- Acordar el inicio del procedimiento de verificación correspondiente y llevar a cabo los actos de verificación y vigilancia necesarios en el presente caso.

TERCERO.- Una vez copiado y cotejado el documento original con el que se acredita la personalidad, sea acordada su devolución a esta parte denunciante.

[...] (sic)

- a) Adjunto a su escrito, con el objeto de acreditar su personalidad, la denunciante remitió el instrumento notarial 17, 413 emitido por el notario público número 95, en el Estado de México.

54. El seis de diciembre de dos mil diecisiete, el entonces director general de investigación y verificación, emitió un acuerdo a través del cual tuvo por presentado el escrito descrito en el **antecedente 53** y se hizo constar que feneció el plazo de 30 días hábiles otorgados a los titulares de datos personales que tuvieran una presunta afectación debido a la utilización del *software (malware)* identificado como "Pegasus", para comparecer ante este Instituto a presentar formalmente su denuncia.

55. Mediante el oficio número **INAI/SPDP/DGIV/3238/17** del siete de diciembre de dos mil diecisiete, con el objeto de estar en condiciones de esclarecer los hechos motivo de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

la investigación, la entonces Dirección General de Investigación y Verificación solicitó a la directora general de atención al pleno de este Instituto, lo siguiente:

[...]

En ese sentido, en el oficio de referencia se informó que el recurso de revisión 4744/17, interpuesto en contra de la Secretaría de Gobernación, fue resuelto el trece de septiembre de dos mil diecisiete, confirmando la respuesta del sujeto obligado; mientras que el diverso RRA 5259/17, presentado en contra del Centro de Investigación y Seguridad Nacional, se encontraba en sustanciación a cargo de la ponencia de la Comisionada Areli Cano Guadiana. Asimismo, refirió la existencia de otros seis recursos de revisión vinculados con el software (malware) "Pegasus", a saber:

- *RRA 5858/17, en contra del Centro de Investigación y Seguridad Nacional, a cargo de la Comisionada Ximena Puente de la Mora.*
- *RRA 5889/17, en contra del Centro de Investigación y Seguridad Nacional; correspondiente a la Comisionada Areli Cano Guadiana.*
- *RRA 5890/17, en contra de la Secretaría de Marina, a cargo del Comisionado Oscar Mauricio Guerra Ford.*
- *RRA 5891/17, en contra de la Presidencia de la República, a cargo de la Comisionada María Patricia Kurczyn Villalobos.*
- *RRA 5895/17, en contra de la Secretaría de la Defensa Nacional, a cargo del Comisionado Presidente Francisco Javier Acuña Llamas*
- *RRA 6309/17, en contra de la Procuraduría General de la República, a cargo de la Comisionada Areli Cano Guadiana.*

Por tal motivo, con fundamento en los artículos [...]; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique cuál es el estado procesal actual de los recursos de revisión que a continuación se indican:*
 - *RRA 5858/17, en contra del Centro de Investigación y Seguridad Nacional, a cargo de la Comisionada Ximena Puente de la Mora*
 - *RRA 5889/17, en contra del Centro de Investigación y Seguridad Nacional; correspondiente a la Comisionada Areli Cano Guadiana*
 - *RRA 5890/17, en contra de la Secretaría de Marina, a cargo del Comisionado Oscar Mauricio Guerra Ford*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *RRA 5891/17, en contra de la Presidencia de la República, a cargo de la Comisionada María Patricia Kurczyn Villalobos*
 - *RRA 5895/17, en contra de la Secretaría de la Defensa Nacional, a cargo del Comisionado Presidente Francisco Javier Acuña Llamas*
 - *RRA 6309/17, en contra de la Procuraduría General de la República, a cargo de la Comisionada Areli Cano Guadiana.*
2. *Señale si a la fecha de la presente, el Pleno de este Instituto ha emitido resolución respecto de los recursos de revisión RRA 5858/17, RRA 5889/17, RRA 5890/17, RRA 5891/17, RRA 5895/17 y RRA 6309/17, sirviéndose remitir copia simple de las mismas, en su caso.*
3. *Mencione si tiene conocimiento de algún otro recurso de revisión en materia de acceso a la información y/o protección de datos personales, que se encuentre vinculado con información referente al uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente, el nombre del sujeto obligado en contra de quien se tramitó el asunto; así como su estado procesal, sirviéndose remitir copia de la resolución que, en su caso, haya recaído al mismo.*

Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, en un término máximo de cinco días hábiles contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el once de diciembre de dos mil diecisiete.

56. El quince de diciembre de dos mil diecisiete, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP/DGAP/1679/2017** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/3238/17** descrito en el **antecedente 55**, indicando lo siguiente:

[...]

Al respecto, me permito hacer de su conocimiento lo siguiente, por cada punto requerido:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Respecto de los requerimientos 1 y 2 antes citados, esta Dirección General informa que los recursos revisión RRA 5858/17, RRA 5891/17 y 5895/17, se encuentran resueltos por el Pleno de este Instituto, como se muestran en la siguiente tabla:

Expediente	Autoridad	Comisionado	Ingreso	Fecha de sesión en que se resolvió	Sentido
RRA 5858/17	CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL	XPM	01/09/2017	01/11/2017	Modifica
RRA 5891/17	OFICINA DE LA PRESIDENCIA DE LA REPÚBLICA	MPKV	01/09/2017	18/10/2017	Confirma
RRA 5895/17	SECRETARÍA DE LA DEFENSA NACIONAL (SEDENA)	FJAL	01/09/2017	22/11/2017	Sobresee

Por otro lado, derivado de los recursos de revisión RRA 5889/17 y RRA 5890/17, se informa que, fueron desechados por acuerdo de ponencia respectivamente, como se muestran en la siguiente tabla:

Expediente	Autoridad	Comisionado	Ingreso	Fecha de sesión en que se resolvió	Sentido
RRA 5889/17	CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL	ACG	01/09/2017	08/09/2017	Desecha
RRA 5891/17	SECRETARÍA DE MARINA	OMGF	01/09/2017	08/09/2017	Sobresee



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora bien, es de mencionar que el recurso de revisión RRA 6309/17, interpuesto ante la Procuraduría General de la República, turnado a la ponencia de la Comisionada Areli Cano Guadiana, se encuentra en sustanciación.

Ahora bien, en cuanto al requerimiento identificado con el número 3, me permito informarle que esta Dirección General tiene conocimiento de un nuevo recurso de revisión vinculado al referente uso del software (malware) "Pegasus", identificado con el número RRA 7477/17 interpuesto ante la Secretaría de Gobernación, mismo que fue turnado a la ponencia del Comisionado Presidente y que al momento, se encuentra en sustanciación.

Aunado a lo anterior, esta Unidad Administrativa informa que los documentos de carácter público tales como solicitudes, estudios, resoluciones, entre otros, que pudiesen ser de su interés pueden ser localizados y consultados en el Zoom, Buscador de Solicitudes de Información y Recursos de Revisión.

A través de ese buscador, es posible ubicar aquellos documentos relacionados adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus".

Para acceder al Zoom, Buscador de Solicitudes de Información y Recursos de Revisión, debe seleccionarse el apartado Acceso a Información Pública, el cual despliega un menú en el que se encuentra la opción denominada Instrumentos, en el cual se muestra el icono del Zoom.

[...]

a) Adjunto, se remitieron las siguientes resoluciones y acuerdos:

- Resolución al recurso de revisión **RRA 5858/17**, en la que se determinó **modificar** la respuesta del Centro de Investigación y Seguridad Nacional, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el uno de noviembre de dos mil diecisiete.
- Resolución al recurso de revisión **RRA 5891/17**, en la que se determinó **confirma** la respuesta de la Oficina de la Presidencia de la República, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el dieciocho de octubre de dos mil diecisiete.
- Resolución al recurso de revisión **RRA 5895/17**, en la que se determinó **sobreseer** el recurso interpuesto en contra de la respuesta de la Secretaría



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

de la Defensa Nacional, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el veintidós de noviembre de dos mil diecisiete.

- Acuerdo dictado en el **RRA 5889/17** en el que se determinó **desechar** por improcedente el recurso de revisión interpuesto en contra del Centro de Investigación y Seguridad Nacional, el ocho de septiembre de dos mil diecisiete.
- Acuerdo dictado en el **RRA 5890/17** en el que se determinó **desechar** por extemporáneo el recurso de revisión interpuesto en contra de la Secretaría de Marina, el ocho de septiembre de dos mil diecisiete.

57. Mediante el oficio número **INAI/SPDP/DGIV/0021/18** del ocho de enero de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al titular del área jurídica del Centro de Investigación y Seguridad Nacional, lo siguiente:

[...]

De tal forma, con fundamento en los artículos [...], me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique si el Centro de Investigación y Seguridad Nacional ha adquirido, comprado, arrendado o se encuentra en posesión, bajo cualquier figura jurídica, del software (malware) identificado como "Pegasus".*
2. *Precise el nombre, denominación y la razón social de la persona física y/o moral de quien, haya adquirido el software (malware) identificado como "Pegasus".*
3. *Describa en qué consiste y cómo opera el software (malware) identificado como "Pegasus".*
4. *Indique de forma detallada las acciones que pueden llevarse a cabo con el software (malware) identificado como "Pegasus", y describa puntualmente cuál es la información y datos personales a los que se puede tener acceso.*
5. *Señale quienes son los servidores públicos y/o personal, perteneciente o no al Centro de Investigación y Seguridad Nacional, autorizado para la utilización del software (malware) identificado como "Pegasus".*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

6. *Describa los procedimientos técnicos, informáticos y, en su caso, legales seguidos para la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".*
7. *Proporcione copia simple de los convenios, contratos, fallo de licitaciones o cualquier documento físico y/o electrónico, con independencia de su denominación, relacionado con la adquisición, instalación, operación y utilización del software (malware) identificado como "Pegasus".*
8. *Señale si el Centro de Investigación y Seguridad Nacional ha utilizado el software (malware) identificado como "Pegasus", y precise cuál es la información y datos personales que ha recabado.*
9. *De ser el caso, explique en qué situaciones o circunstancias, para qué finalidades y respecto de que titulares ha utilizado el software (malware) Identificado como "Pegasus", y precise si ha llevado a cabo el tratamiento (obtención, uso, registro, reproducción, conservación, organización, modificación, transmisión y/o cancelación) de datos personales a partir del mismo.*
10. *Manifieste si el Centro de Investigación y Seguridad Nacional ha tenido conocimiento de los hechos referidos en el acuerdo del treinta de junio de dos mil diecisiete, así como de alguna queja, denuncia o inconformidad relacionada con los mismos y, en su caso describa las acciones que ha llevado a cabo al respecto.*

*Le agradeceré haga del conocimiento de este Instituto lo referida con anterioridad, en el domicilio abajo indicado, **en un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente. de conformidad con los 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Centro de Investigación y Seguridad Nacional, el nueve de enero de dos mil dieciocho.

58. El quince de enero de dos mil dieciocho, la entonces Dirección General de Investigación y Verificación remitió vía correo electrónico al secretario de protección de datos personales de este Instituto, copia de conocimiento del oficio número **INAI/SPDP/DGIV/0021/18**, descrito en el **antecedente 57**.

59. El diecisiete de enero de dos mil dieciocho, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **SG/AJ/009/18** de la misma fecha, emitido y signado por el titular del área jurídica del Centro de Investigación y Seguridad



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Nacional, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/0021/18** descrito en el **antecedente 57**, indicando lo siguiente:

[...]

Al respecto, y en atención a su petición, se realizó nuevamente una búsqueda exhaustiva de la información solicitada al interior de las áreas competentes de este órgano desconcentrado, dando como resultado la INEXISTENCIA de información relacionada con el presente requerimiento.

No pasa desapercibida para este sujeto obligado, que la investigación preliminar motivo del presente requerimiento, se desprende fundamentalmente de hechos referidos en diversas notas periodísticas y en ese sentido, es importante precisar que estas no hacen prueba plena para acreditar los hechos que refieren y únicamente reflejan el punto de vista del autor. Al caso, resultan aplicables, los siguientes criterios emitidos por el Poder Judicial:

[...]

Por último, se solicita que las subsecuentes comunicaciones sean realizadas vía correo electrónico cisen@cisen.gob.mx.

[...]

60. Mediante el oficio número **INAI/SPDP/DGIV/0159/18** del veintidós de enero de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de cumplimientos y responsabilidades de este Instituto, lo siguiente:

[...]

En ese sentido, con fundamento en los artículos [...]; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y de no existir inconveniente alguno, haga llegar a esta Dirección General la siguiente información:

1. *Si derivado de algún asunto de su competencia ha tenido conocimiento de hechos o documentos vinculados con la adquisición posesión, uso u operación del software (malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

2. *El estado que guarda el cumplimiento de las resoluciones emitidas por el Pleno de este Instituto con motivo de los recursos de revisión en materia de acceso a la información y/o protección de datos personales que a continuación se indican, a saber:*
 - *RRA 3762/16, en contra de la Procuraduría General de la República.*
 - *RRA 5259/17, en contra del Centro de Investigación y Seguridad Nacional.*
 - *RRA 5858/17, en contra del Centro de Investigación y Seguridad Nacional.*
 - *RRA 5869/17, en contra del Centro de Investigación y Seguridad Nacional.*
 - *RRA 5895/17, en contra de la Secretaría de la Defensa Nacional.*
 - *RRA 6309/17, en contra de la Procuraduría General de la República.*
3. *Si con motivo del cumplimiento de algún recurso de revisión en materia de acceso a la información y/o protección de datos personales, resuelto por el Pleno de este Instituto (incluyendo los listados en el punto anterior), se cuenta con información y/o documentación vinculada con el uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente el nombre del sujeto obligado en contra de quien se tramitó el asunto y, sírvase remitir copia de la respuesta, acuerdo o resolución en que se advierta dicha circunstancia.*
4. *Copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación física y/o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión*

Le agradeceré haga del conocimiento de este instituto lo referido con anterioridad en el domicilio abajo indicado, en un término máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.

[...]

El requerimiento se notificó a la Dirección General de Cumplimientos y Responsabilidades, el veintitrés de enero de dos mil dieciocho.

61. Mediante el oficio número **INAI/SPDP/DGIV/0163/18** del veintidós de enero de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó al director general de normatividad y consulta de este Instituto, lo siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En ese sentido, se estima relevante hacer de su conocimiento que con el objeto de conocer la postura e información con que cuentan las unidades administrativas que pudieran estar relacionadas o, al menos, tener conocimiento de los hechos en cuestión a partir del ejercicio de sus atribuciones se formularon requerimientos de información a la Secretaría de Acceso a la Información, Direcciones Generales de Tecnologías de la Información, de Atención al Pleno, de Protección de Derechos y Sanción, de Prevención y Autorregulación, las cuales respondieron esencialmente lo siguiente:

- **Secretaría de Acceso a la Información:** *indicó esencialmente que de la búsqueda en el Sistema de Portales de Obligaciones de Transparencia (SIPOT) no se localizó información alguna en relación con contratos, convenios o instrumentos jurídicos celebrados por cualquier instancia del Gobierno Federal con cualquier empresa, sobre el software (malware) denominado "Pegasus", con excepción de un sistema de un contrato de "servicios para el aplicativo de gestión institucional electrónico Pegasus" a cargo de la Secretaría de Hacienda y Crédito Público.*
- **Dirección General de Tecnologías de la Información:** *señaló básicamente que "Pegasus" es un software de espionaje que contiene código malicioso, procesos y aplicaciones que se utilizan para espiar, recopilar datos e informar sobre lo que hace el usuario en su dispositivo móvil. Asimismo, sostuvo que, si es posible tener acceso, extraer y utilizar la información y/o los datos personales contenidos en los dispositivos comprometidos; sin embargo, precisó que no puede determinarse simplemente a partir de la utilización de este software. Finalmente, se adjuntó el documento titulado "Análisis técnico del Spyware de Pegasus", en inglés y su traducción respectiva.*
- **Dirección General de Prevención y Autorregulación:** *proporcionó un informe en el que se describe la operación del malware "Pegasus", del cual se puede advertir que a través del uso de esta herramienta se podría tener acceso, extraer y utilizar información y/o datos personales contenidos en los dispositivos comprometidos. Además, señaló que es factible el tratamiento a partir del acceso que se podría tener a datos personales contenidos en los dispositivos comprometidos por una herramienta tecnológica que opere como se dice que lo hace el software (malware) identificado como "Pegasus"; no obstante, en cuanto a quién es el responsable de tratamiento, dicha unidad administrativa, refirió que no cuenta con información suficiente para dar respuesta a dicho cuestionamiento.*
- **Dirección General de Atención al Pleno:** *comunicó que de la búsqueda a la base de datos consistente en la "Relación de Recursos de Revisión en materia de acceso a la información" identificó un recurso de revisión vinculado con información relativa al uso del software (malware) identificado como "Pegasus" a saber: RRA 3762/16 en contra de la Procuraduría General de la República.*
- **Dirección General de Protección de Derechos y Sanción:** *informó que no cuenta con información alguna al respecto.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Con base en las respuestas recibidas, se formularon requerimientos adicionales a las unidades administrativas del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, cuyas respuestas se describen brevemente a continuación:

- **Secretaría de Acceso a la Información:** informó que una vez que feneciera el plazo legal otorgado a los sujetos obligados, procedería a realizar una verificación diagnóstica sobre el cumplimiento de las obligaciones de transparencia, cuyo plazo de desarrollo es del cinco de mayo hasta el veinte de diciembre de dos mil diecisiete; motivo por el cual dicha verificación se encontraba en trámite, por lo que no era posible atender favorablemente el requerimiento formulado.
- **Dirección General de Asuntos Internacionales:** proporcionó la traducción al castellano respecto de los documentos remitidos por la Dirección General de Prevención y Autorregulación en idioma inglés.
- **Dirección General de Atención al Pleno:** comunicó la existencia de otro recurso de revisión vinculado con el software (malware) Pegasus a saber: RRA 5259/17 en contra del Centro de Investigación y Seguridad Nacional.

Ahora bien, a partir de los señalamientos realizados en notas periodísticas y comunicados realizados públicamente a través de Internet por instituciones gubernamentales formularon requerimientos de información a la Procuraduría General de la República y la Secretaría de la Defensa Nacional, obteniendo las siguientes respuestas:

- **La Procuraduría General de la República** en sus oficios de respuesta, recibidos el trece de julio y el doce de septiembre de dos mil diecisiete, argumentó fundamentalmente lo siguiente:
 - La materia de las investigaciones instauradas por este Instituto se contrapone con la facultad persecutora de delitos, a cargo del Ministerio Público.
 - Los hechos se encuentran en etapa de investigación por lo que todos los documentos relacionados y contenidas en ella, son reservados.
 - Las notas periodísticas en que se basó el inicio de las investigaciones instruidas por este Instituto no acreditan los hechos que en ellas se contienen.
 - Se manifestó la imposibilidad para proporcionar información sobre la denuncia presentada por la probable constitución de los delitos consistentes en la intervención de comunicaciones privadas, el acceso ilícito a sistemas y equipos de informática y los demás que resulten, derivado de la utilización del "software" identificado como "Pegasus", toda vez que los hechos se encuentran sujetos a investigación ministerial por lo que toda la información contenida en las carpetas de investigación son estrictamente reservados, en términos del artículo 218 del



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Código Nacional de Procedimientos Penales y 51, fracción I, de la Ley de Seguridad Nacional.

- *Por otro lado, se informó que la Procuraduría General de la República para enfrentar de mejor manera el fenómeno delincriminal y combatir con mejores herramientas técnicas a las organizaciones criminales, con base en las disposiciones de la Ley de Seguridad Nacional y de la Ley Federal contra la Delincuencia Organizada, ha adquirido sistemas informáticos para combatir dicho fenómeno y actividad delincriminal citada.*
- *Del mismo modo, mediante Acuerdo A/018/15 del Procurador General de la República, publicado en el Diario Oficial de la Federación el 23 de febrero de 2015, se delegó en los servidores públicos que en dicho instrumento jurídico se indican, diversas facultades para intervenir comunicaciones privadas, en términos de su artículo Segundo, fracción V, de conformidad con el diverso 291 del Código Nacional de Procedimientos Penales.*
- *En sus oficios de respuesta recibidos el cuatro de septiembre de dos mil diecisiete, la **Secretaría de la Defensa Nacional** argumentó esencialmente lo siguiente:*
 - *En los periodos de dos mil quince y dos mil dieciséis no adquirió, arrendó o tuvo en posesión el software identificado como "Pegasus", ya que en dicho periodo no se contaba con esa herramienta informática, por lo que no se localizó información respecto a que se haya recabado, obtenido, transmitido, manejado o se haya dado algún tratamiento a datos personales que se hayan obtenido a través del citado software de dos mil quince a la fecha.*
 - *En el requerimiento no se señaló cuáles fueron los datos personales desprotegidos, ni obra una denuncia o medios de prueba específicas, por lo que normativamente no existía materia de controversia o investigación.*

De igual forma, el cinco de octubre de dos mil diecisiete la Dirección General de Atención al Pleno de este Instituto comunicó la existencia de otros cuatro recursos de revisión vinculados con el software (malware) "Pegasus", a saber:

- *RRA 5858/17, en contra del Centro de Investigación y Seguridad Nacional.*
- *RRA 5889/17, en contra del Centro de Investigación y Seguridad Nacional.*
- *RRA 5895/17, en contra de la Secretaría de la Defensa Nacional.*
- *RRA 6309/17, en contra de la Procuraduría General de la República.*

*El nueve de octubre de dos mil diecisiete, la **Dirección General de Gobierno Abierto y Transparencia** respondió el requerimiento formulado informando que el Núcleo de las Organizaciones de la Sociedad Civil no había hecho del conocimiento la decisión tomada*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

respecto de presentar o no una denuncia ante este Instituto; resaltando que sugería que se solicitará formalmente y de manera directa a los presuntos afectados o en su caso, a las representantes legales que tengan la capacidad jurídica para actuar, que manifestaran la decisión de presentar o no la denuncia, considerando que no se estableció una fecha para informar dicha decisión.

*En tal virtud, los días diecisiete, dieciocho y diecinueve de octubre de dos mil diecisiete, en el Diario Oficial de la Federación, y el diecisiete, diecinueve y veinte del mismo mes y año, en el periódico "El Universal", se publicaron sendos **edictos** para notificar a los titulares de datos personales que tuvieran una presunta afectación derivada de la operación del software (malware) identificado como "Pegasus", a efecto de que, en el término de treinta días hábiles, el cual venció el cinco de diciembre de dos mil diecisiete, comparecieran en el domicilio del Instituto para que presentaran formalmente su denuncia cumpliendo los requisitos mínimos establecidos por la normatividad aplicable, manifestaran lo que a su derecho convenga, aportaran pruebas y señalen un domicilio cierto y determinado en esta Ciudad de México para recibir notificaciones.*

Por tal motivo, el cuatro de diciembre de dos mil diecisiete, se recibió una denuncia en la que se refirieron presuntos incumplimientos a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados por parte de la Agencia de Investigación Criminal de la Procuraduría General de la República y otras dependencias federales, en relación con el presunto tratamiento de datos personales derivado de la operación del sistema para la intervención de comunicaciones privadas denominado "Pegasus"; la cual se integró al expediente de mérito mediante acuerdo del seis de diciembre de dos mil diecisiete.

*Por otra parte, con base en la información recabada por este Instituto derivado de los recursos de revisión referidos, se formuló un requerimiento de información al **Centro de Investigación y Seguridad Nacional**, para que indicara diversas cuestiones sobre la adquisición, utilización y operación del software (malware) denominado "Pegasus", así como el probable tratamiento de datos personales como consecuencia de su actividad y las circunstancias en que se realiza, recibiendo la respuesta respectiva el diecisiete de enero de dos mil dieciocho, en la que se expresó esencialmente lo siguiente:*

- Se realizó una búsqueda exhaustiva de la información solicitada al interior de las áreas competentes de dicho órgano desconcentrado, dando como resultado la inexistencia de la información relacionada con el requerimiento.*
- Los hechos que motivaron la investigación preliminar motivo del requerimiento, se derivan de notas periodísticas, por lo que es importante precisar que éstas no hacían prueba plena para acreditar los hechos que refieren y únicamente reflejan el punto de vista del autor, conforme a los criterios emitidos por el Poder Judicial de la Federación.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Con base en lo expuesto hasta este punto, y con fundamento en los artículos [...]; me permito solicitarle su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y, de no existir inconveniente alguno, haga llegar a esta Dirección General la siguiente información:

- 1. Su opinión pormenorizada respecto de cuáles son los alcances e implicaciones en materia de protección de datos personales de la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus"; precisando si es posible determinar la existencia o no de algún tratamiento de datos personales por parte de algún sujeto obligado del sector público o privado.*
- 2. De ser el caso, de manera fundada y motivada, quién o quiénes revisten el carácter de responsables y/o encargados del tratamiento de los datos personales en el presente asunto.*
- 3. Los actos y/u omisiones que estime contrarias a la normatividad aplicable en materia de protección de datos personales y que, en su caso, pudieran actualizar alguna hipótesis de infracción a las leyes de la materia, por parte de los sujetos obligados de los sectores público y/o privado.*
- 4. Si a su consideración, en el presente asunto, se encuentra acreditado o se puede advertir la existencia de actos de tracto sucesivo con motivo de la adquisición, posesión, uso u operación del software (malware) identificado como "Pegasus", precisando, en su caso, a quién le son atribuibles, si los mismos podrían actualizar alguna hipótesis de infracción en materia de protección de datos personales, así como el marco normativo que resultada aplicable en esa hipótesis.*
- 5. Una explicación, de manera fundada y motivada, sobre cuál es el marco legal aplicable en materia de protección de datos personales en el presente asunto, así como el que debe aplicarse en caso de actualizarse alguna hipótesis de infracción; lo anterior, tomando en cuenta, entre otras circunstancias, la temporalidad en que ocurrieron o pudieron haber ocurrido los hechos materia de investigación, los sujetos obligados responsables y/o encargados de los sectores público y/o privado, así como las conductas que presumiblemente resulten violatorias de las leyes de la materia.*

Le agradeceré haga del conocimiento de esta Dirección General lo referido con anterioridad, a la brevedad posible, considerando que la opinión e interpretación solicitada, en relación con el marco normativo aplicable en el caso concreto, resulta ser un insumo indispensable para continuar con la sustanciación y trámite del expediente de investigación citado al rubro.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

El requerimiento se notificó a la Dirección General de Normatividad y Consulta, el veinticuatro de enero de dos mil dieciocho.

62. Mediante el oficio número **INAI/SPDP/DGIV/0171/18** del veintidós de enero de dos mil dieciocho¹⁵, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la entonces Dirección General de Investigación y Verificación solicitó a la directora general de atención al pleno de este Instituto, lo siguiente:

[...]

En ese sentido, en el oficio de referencia se informó el estado procesal de los recursos de revisión RRA 5858/17, RRA 5889/17, RRA 5890/17, RRA 5891/17, RRA 5895/17 como resueltos y respectivamente, puntualizando que el diverso RRA 6309/17, interpuesto en contra de la Procuraduría General de la República, se encontraba en sustanciación a cargo de la ponencia de la Comisionada Areli Cano Guadiana. Asimismo, refirió la existencia de otro recurso de revisión vinculados con el software (malware) "Pegasus", identificado con el número RRA 7477/17, interpuesto en contra de la Secretaría de Gobernación y turnado al Comisionado Presidente.

Por tal motivo, con fundamento en los artículos [...]; me permito solicitarle su colaboración, a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

1. *Indique cuál es el estado procesal actual de los recursos de revisión que a continuación se indican:*
 - *RRA 6309/17, interpuesto en contra de la Procuraduría General de la República, correspondiente a la Comisionada Areli Cano Guadiana.*
 - *RRA 7477/17, interpuesto en contra de la Secretaría de Gobernación, correspondiente al Comisionado Presidente, Francisco Javier Acuña Llamas.*
2. *Señale si a la fecha del presente, el Pleno de este Instituto ha emitido resolución respecto de los recursos de revisión RRA 6309/17 y RRA 7477/17, sirviéndose remitir copia simple de las mismas, en su caso.*

¹⁵ Si bien por un error el oficio número **INAI/SPDP/DGIV/0171/18** tiene fecha del siete de diciembre de dos mil diecisiete, la fecha correcta en la que se emitió el oficio es el veintidós de enero de dos mil dieciocho.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Mencione si tiene conocimiento de algún otro recurso de revisión en materia de acceso a la información y/o protección de datos personales, que se encuentre vinculado con información referente al uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente, el nombre del sujeto obligado en contra de quien se tramitó el asunto, así como su estado procesal, sirviéndose remitir copia de la resolución que, en su caso, haya recaído al mismo.*

*Le agradeceré haga del conocimiento de este Instituto lo referido con anterioridad, en el domicilio abajo indicado, en **un término máximo de cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a las leyes de la materia.*

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el veinticuatro de enero de dos mil dieciocho.

63. El treinta de enero de dos mil dieciocho, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP-DGCR/039/2018** del veintinueve de enero de dos mil dieciocho, emitido y signado por el director general de cumplimientos y responsabilidades de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGIV/0159/18** descrito en el **antecedente 60**, indicando lo siguiente:

[...]

En atención al oficio INAI/SPDP/DGIV/0158/19, primeramente, resulta pertinente destacar que de conformidad con lo dispuesto en el artículo 36, fracción II, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, esta Dirección General a mi cargo, es la encargada de verificar el cumplimiento que los sujetos obligados den a las resoluciones de los medios de impugnación emitidas por el Pleno de este Instituto con instrucción, por lo cual, el requerimiento efectuado se atenderá con base en la información que en atención a su competencia resguarda esta Dirección General.

En tal virtud, me permito informar sobre lo solicitado en los siguientes términos:

1. *Si derivado de algún asunto de su competencia ha tenido conocimiento de hechos o documentos vinculados con la adquisición, posesión, uso u operación del software*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

(malware) identificado como "Pegasus", por parte de algún sujeto obligado del sector público o privado.

R= Esta Dirección General ha dado seguimiento al cumplimiento de dos resoluciones emitidas por el Pleno de este Instituto, a saber: RRA 5259/17 y RRA 5858/17.

Cabe señalar que ambos recursos se encuentran relacionados con solicitudes de información, en los cuales los particulares interesados plantearon el acceso a información relacionada con el software conocido como "Pegasus"; asimismo, que en ambos casos el sujeto obligado del sector público es el Centro de Investigación y Seguridad Nacional; aclarando que esta Dirección General no tiene competencia sobre sujetos obligados del sector privado.

Ahora bien, del seguimiento al cumplimiento de tales resoluciones, esta Dirección General sólo cuenta con los documentos proporcionados por el sujeto obligado en atención a lo instruido, sin tener ningún otro conocimiento sobre otros hechos o documentos.

2. *El estado que guarda el cumplimiento de las resoluciones emitidas por el Pleno de este Instituto con motivo de los recursos de revisión en materia de acceso a la información y/o protección de datos personales que a continuación se en listan, a saber:*

- RRA 3762/16, en contra de la Procuraduría General de la República.*
- RRA 5259/17, en contra del Centro de Investigación y Seguridad Nacional.*
- RRA 5858/17, en contra del Centro de Investigación y Seguridad Nacional.*
- RRA 5889/17, en contra del Centro de Investigación y Seguridad Nacional.*
- RRA 5895/17, en contra de la Secretaría de la Defensa Nacional.*
- RRA 6309/17, en contra de la Procuraduría General de la República*

R= De acuerdo con la información con que cuenta esta Dirección General de acuerdo con su competencia en los términos precisados anteriormente, se informa que por cuanto hace a los recursos RRA 5259/17 y RRA 5858/17, a la fecha los mismos se encuentran cumplidos.

Por otra parte, en relación con los demás expedientes precisados en su requerimiento, le informo que esta Dirección General no ha conocido de los mismos toda vez que no han sido turnados por el área competente para el seguimiento del cumplimiento de alguna resolución con instrucción dictada por el Pleno relacionada con éstos. Sin embargo, privilegiando el principio de exhaustividad y en plena colaboración con esa Dirección General, se procedió a verificar en el Sistema Institucional denominado "Herramienta de Comunicación", del cual se advirtió lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Por cuanto hace a los RRA 3762/16 y RRA 5895/17, el Pleno emitió sendas resoluciones en las cuales, respecto del RRA 3762/17 confirmó la respuesta del sujeto obligado y con relación al RRA 5895/17 sobreseyó el recurso, por lo cual, esta Dirección General no cuenta con información alguna relacionada con tales recursos, al no haberse emitido resoluciones con instrucción para su seguimiento; en tal virtud, se sugiere que se consulte a la Dirección General de Atención Pleno para que proporcione la información con que cuente sobre su requerimiento respecto de los recursos de revisión precisados, al ser ésta el área competente.*
 - *Con relación a los RRA 5889/17 y RRA 6309/17, se advierte del aludido sistema que aparecen aún en trámite en la ponencia a la cual fueron turnados, por lo cual, igualmente, se sugiere que se consulte a la Dirección General de Atención Pleno para que proporcione la información con que cuente sobre su requerimiento respecto de los recursos de revisión precisados, al ser ésta el área competente.*
3. *Si con motivo del cumplimiento de algún recurso de revisión en materia de acceso a la información y/o protección de datos personales, resuelto por el Pleno de este Instituto (incluyendo los listados en el punto anterior), se cuenta con información y/o documentación vinculada con el uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente y el nombre del sujeto obligado en contra de quien se tramitó el asunto y sírvase remitir copia de la respuesta, acuerdo o resolución en que se advierta dicha circunstancia.*

R= Después de una consulta a los responsables del seguimiento de las resoluciones turnadas a esta Dirección General, así como a las bases de datos con que se cuenta se informa que no se advirtió ninguna otra resolución en seguimiento a cargo de esta Dirección, de la que se desprenda que lo solicitado por el particular interesado o de lo instruido por el Pleno, esté claramente vinculada con el software denominado "Pegasus"; pues solamente se localizaron las correspondientes al RRA 5259/17 y la RRA 5858/17, en los términos informados anteriormente.

4. *Copia simple de los documentos que acrediten la información que precede, así como cualquier otra información y documentación (física o electrónica) que pudiera coadyuvar a dilucidar los hechos en cuestión.*

R= Se remite copia certificada de los expedientes de cumplimiento relacionados con los recursos RRA 5259/17 y RRA 5858/17, para los efectos a que haya lugar, sin que esta Dirección General a la fecha, cuente con ningún otro documento o información adicional, física o electrónica, que se advierta en forma manifiesta que esté relacionada con los hechos que menciona en su requerimiento.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

a) Adjunto, se remitió:

- Resolución al recurso de revisión **RRA 5858/17**, en la que se determinó **modificar** la respuesta del Centro de Investigación y Seguridad Nacional, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el uno de noviembre de dos mil diecisiete.
- Correo electrónico remitido el veintidós de noviembre de dos mil diecisiete a la dirección señalada por la recurrente como medio para recibir notificaciones, a través del cual el Centro de Investigación y Seguridad Nacional informó el cumplimiento dado a la resolución del recurso de revisión **RRA 5858/17**.
- Correo electrónico remitido el veintitrés de noviembre de dos mil diecisiete a la dirección señalada por la recurrente como medio para recibir notificaciones, a través del cual la jefa de departamento de verificación de cumplimientos de este Instituto, le solicitó manifestar lo que a su derecho convenga respecto del cumplimiento dado por el Centro de Investigación y Seguridad Nacional a la resolución del recurso de revisión **RRA 5858/17**.
- Correo electrónico del cinco de diciembre de dos mil diecisiete, dirigido a la Dirección General de Cumplimientos y Responsabilidades de este Instituto, a través del cual el Centro de Investigación y Seguridad Nacional remitió la resolución CT/180/17 emitida por su Comité de Transparencia en atención a la resolución del recurso de revisión **RRA 5858/17**.
- Acuerdo del cinco de diciembre de dos mil diecisiete, emitido por el director general de cumplimientos y responsabilidades de este Instituto, por el que tuvo por cumplida por parte del Centro de Investigación y Seguridad Nacional, la resolución del recurso de revisión **RRA 5858/17**.
- Correo electrónico remitido el ocho de diciembre de dos mil diecisiete a la dirección señalada por la recurrente como medio para recibir notificaciones, a través del cual la jefa de departamento de verificación de cumplimientos de este Instituto, le notificó el acuerdo dictado el cinco de diciembre de dos mil diecisiete.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Notificación a través de la Herramienta de Comunicación al Centro de Investigación y Seguridad Nacional, del acuerdo del cinco de diciembre de dos mil diecisiete.
- Resolución al recurso de revisión **RRA 5259/17**, en la que se determinó **modificar** la respuesta del Centro de Investigación y Seguridad Nacional, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el veinticinco de octubre de dos mil diecisiete.
- Correo electrónico remitido el catorce de noviembre de dos mil diecisiete a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual el Centro de Investigación y Seguridad Nacional informó el cumplimiento dado a la resolución del recurso de revisión **RRA 5259/17**.
- Correo electrónico remitido el catorce de noviembre de dos mil diecisiete a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual la jefa de departamento de cumplimientos B de este Instituto, le solicitó manifestar lo que a su derecho convenga respecto del cumplimiento dado por el Centro de Investigación y Seguridad Nacional a la resolución del recurso de revisión **RRA 5259/17**.
- Acuerdo del veintinueve de enero de dos mil dieciocho, emitido por el director general de cumplimientos y responsabilidades de este Instituto, por el que tuvo por cumplida por parte del Centro de Investigación y Seguridad Nacional, la resolución del recurso de revisión **RRA 5259/17**.
- Correo electrónico remitido el treinta de enero de dos mil dieciocho a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual la jefa de departamento de cumplimientos B de este Instituto, le notificó el acuerdo dictado el veintinueve de enero de dos mil dieciocho.
- Notificación a través de la Herramienta de Comunicación al Centro de Investigación y Seguridad Nacional, del acuerdo del veintinueve de enero de dos mil dieciocho.

64. El treinta de enero de dos mil dieciocho, se recibió en la entonces Dirección General Investigación y Verificación el oficio número **INAI/STP/DGAP/105/2018** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

mediante el cual remitió el desahogo al requerimiento formulado a través del oficio INAI/SPDP/DGIV/0171/18 descrito en el antecedente 62, indicando lo siguiente:

[...]

Respecto de los requerimientos 1 y 2 antes citados, esta Dirección General informa que el recurso de revisión RRA 7477/17, se encuentra resuelto por el Pleno de este Instituto, como se muestran en la siguiente tabla:

<i>Expediente</i>	<i>Autoridad</i>	<i>Comisionado</i>	<i>Ingreso</i>	<i>Fecha de sesión en que se resolvió</i>	<i>Sentido</i>
RRA 7477/17	SECRETARÍA DE GOBERNACIÓN (SEGOB)	FJALL	01/11/2017	19/12/2017	Confirma

Por otro lado, es de mencionar que el recurso de revisión RRA 6309/17, interpuesto ante la Procuraduría General de la República, turnado a la ponencia de la Comisionada Areli Cano Guadiana, hasta la fecha de recepción del oficio INAI/SDPD/DGIV/0170/18, se encuentra en sustanciación.

Ahora bien, en cuanto al requerimiento identificado con el número 3, me permito informarle que esta Dirección General no localizó algún recurso de revisión diverso a los indicados en oficios previos, vinculado con información referente al uso del software (malware) "Pegasus".

Aunado a lo anterior, esta Unidad Administrativa informa que los documentos de carácter público tales como solicitudes, estudios, resolución de otros, que pudiesen ser de su interés pueden ser localizados y consultados en el Zoom, Buscador de Solicitudes de Información y Recursos de Revisión.

[...]

a) Adjunto, se remitieron las siguientes resoluciones:

- Resolución al recurso de revisión **RRA 7477/17**, en la que se determinó **confirmar** la respuesta de la Secretaría de Gobernación, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Información y Protección de Datos Personales el diecinueve de diciembre de dos mil diecisiete.

65. El trece de febrero de dos mil dieciocho, la Dirección General de Investigación y Verificación del Sector Privado visto el acuerdo mediante el cual se aprueban las modificaciones de la estructura orgánica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a través del cual se modifica la denominación de la Dirección General de Investigación y Verificación por la de Dirección General de Investigación y Verificación del Sector Privado y se crea la Dirección General de Evaluación, Investigación y Verificación del Sector Público, **acordó** remitir el original del expediente **INAI.3S.08.03-003/2017** a la Dirección General de Evaluación, Investigación y Verificación del Sector Público para que le diera el trámite que conforme a derecho procediera.

66. El uno de marzo de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, adscrito a la Secretaría de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, emitió el acuerdo de recepción del expediente **INAI.3S.08.03-003/2017** para **continuar con el trámite** correspondiente.

67. El cinco de marzo de dos mil dieciocho, mediante el oficio **INAI/SPDP/DGEIVSP/0037/18** el director general de evaluación, investigación y verificación del sector público, comunicó al director general de normatividad y consulta de este Instituto, la transferencia del expediente **INAI.3S.08.03-003/2017** a la Dirección General de Evaluación, Investigación y Verificación del Sector Público, solicitándole que la opinión e interpretación requeridas relacionadas con el marco normativo aplicable al caso concreto sean enviadas a dicha dirección.

68. Mediante el oficio número **INAI/SPDP/DGEIVSP/0039/18** del cinco de marzo de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de atención al pleno de este Instituto, lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Me refiero al oficio INAI/STP/DGAP/105/2018, recibido el 30 de enero de 2018 en la entonces Dirección General de Investigación y Verificación de este Instituto, mediante el cual la Dirección general a su digno cargo atendió el requerimiento de información planteado en el diverso INAI/SPDP/DGIV/0171/18.

*Al respecto, me permito informarle que con motivo de la publicación en el Diario Oficial de la Federación del trece de febrero de dos mil dieciocho, del Acuerdo mediante el cual se aprueban las modificaciones de la Estructura Orgánica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; así como del Acuerdo mediante el cual se aprueban las modificaciones al Estatuto Orgánico de este Instituto, el original del expediente **INAI.3S.08.03-003/2017**, se remitió a la Dirección General de Evaluación, Investigación y Verificación del Sector Público para continuar con el trámite conducente, dentro del ámbito de atribuciones conferidas a esta Unidad Administrativa de reciente creación.*

En consecuencia, a efecto de continuar con el seguimiento del asunto que nos ocupa, con fundamento en los artículos [...], me permito solicitarle su amable colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- *Indique cuál es el estado procesal actual del recurso de revisión edificado con la clave RRA 6309/17, interpuesto en contra de la Procuraduría General de la República, turnado a la Ponencia de la Comisionada. Areli Cano Guadiana.*
- *Señale si a la fecha del presente, el Pleno de este Instituto ha emitido resolución al referido medio de impugnación, sirviéndose remitir copia simple de la misma.*
- *Mencione si tiene conocimiento de algún otro recurso de revisión en materia de acceso a la información y/o protección de datos personales, que se encuentre vinculado con información referente al uso del software (malware) identificado como "Pegasus"; de ser el caso, indique el número de expediente, el nombre del sujeto obligado en contra de quien se tramitó el asunto, así como su estado procesal, sirviéndose remitir copia de la resolución que, en su caso, haya recaído al mismo.*

*Le agradeceré haga del conocimiento de esta unidad administrativa lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo. De aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

El requerimiento se notificó a la Dirección General de Atención al Pleno, el seis de marzo de dos mil dieciocho.

69. El doce de marzo de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/STP/DGAP/260/2018** de la misma fecha, emitido y signado por la directora general de atención al pleno de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/0039/18** descrito en el **antecedente 68**, indicando lo siguiente:

[...]

Respecto de los primeros dos requerimientos antes citados, esta Dirección General informa que el recurso de revisión RRA 6309/17, se encuentra resuelto por el Pleno de este Instituto, como se muestran en la siguiente tabla y cuya resolución se anexa al presente en copia simple:

Expediente	Autoridad	Comisionado	Ingreso	Fecha de sesión en que se resolvió	Sentido
RRA 6309/17	PROCURADURÍA GENERAL DE LA REPÚBLICA (PGR)	ACG	18/09/2017	30/01/2018	Modifica

Ahora bien, en cuanto al último requerimiento, me permito informarle que esta Dirección General advierte que el único documento por medio del cual puede identificar asuntos dentro de su competencia que se relacionen con el "uso del software (malware) identificado como "Pegasus", es la Relación de Recursos de Revisión en materia de acceso a la información, interpuestos en contra de sujetos obligados del sector público.

Además, respecto de los medios de impugnación en materia de protección de datos personales, esta Dirección General no concentra el contenido de las solicitudes interpuestas por los particulares, sino únicamente almacena los datos de identificación de los expedientes que son turnados a las Ponencias de este Instituto.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Así las cosas, me permito informarle que esta Dirección General realizó una búsqueda dentro de la base de datos referida previamente, de la cual no localizó algún recurso de revisión diverso a los indicados en oficios previos, vinculado con información referente al uso del software (malware) "Pegasus".

[...]

a) Adjunto, se remitió la siguiente resolución:

- Resolución al recurso de revisión **RRA 6309/17**, en la que se determinó **modificar** la respuesta de la entonces Procuraduría General de la República, emitida por unanimidad del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el treinta de enero de dos mil dieciocho.

70. Mediante el oficio número **INAI/SPDP/DGEIVSP/0059/18** del doce de marzo de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al director general de cumplimientos y responsabilidades de este Instituto, lo siguiente:

[...]

En consecuencia, a efecto de continuar con el seguimiento del asunto que nos ocupa, con fundamento en los artículos [...], me permito solicitarle su amable colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda y se sirva proporcionar la siguiente información:

- *El estado que guarda el cumplimiento de la resolución emitida por el Pleno de este Instituto el treinta de enero de dos mil dieciocho, con motivo del recurso de revisión en materia de acceso a la información RRA 6309/17, interpuesto en contra de la Procuraduría General de la República.*

Al respecto, es importante mencionar que en la resolución en comento en su resolutivo PRIMERO modifica la respuesta de la Procuraduría General de la República y en su resolutivo SEGUNDO se le instruye al sujeto obligado para que en un plazo de diez días hábiles a partir del siguiente al de su notificación, cumpla con lo ordenado en el considerando Cuarto de la misma.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Copia simple de los documentos que acrediten la información que proporcione en relación con el recurso de revisión indicado, así como de cualquier otra información y documentación (física y electrónica) vinculada con el uso del software (malware) identificado como "Pegasus", en colaboración con la investigación que se sigue ante esta Dirección General.*

*Le agradeceré haga del conocimiento de esta unidad administrativa lo referido con anterioridad, en el domicilio abajo indicado, **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

[...]

El requerimiento se notificó a la Dirección General de Cumplimientos y Responsabilidades, el trece de marzo de dos mil dieciocho.

71. El veinte de marzo de dos mil dieciocho se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público, el oficio **INAI/SPDP/DGNC/046/18** de la misma fecha, emitido y signado por el director general de normatividad y consulta de este Instituto:

[...]

En atención a sus similares números INAI/SPDP/DGIV/0162/18 e INAI/SPDP/DGIV/0163/18, me permito adjuntar la orientación técnica correspondiente.

[...]

- a) Adjunto al oficio se remitió la orientación técnica:

[...]

I. Presentación



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

El presente documento tiene por objeto emitir una orientación técnica en materia de protección de datos personales respecto a los planteamientos formulados por la Dirección General de Investigación y Verificación del Sector Privado mediante los oficios INAI/SPDP/DGIV/0162/18 e INAI/SPDP/DGIV/0163/18.

[...]

IV. Competencia

El artículo 42, fracción II del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales dispone que entre las atribuciones de la Dirección General de Normatividad y Consulta se encuentra atender consultas en materia de protección de datos personales del sector público y privado.

En ese sentido, a continuación, se formulan una serie de consideraciones que pueden servir de orientación técnica a la Dirección General de Investigación y Verificación del Sector Privado a los planteamientos que formula, en las cuales se abordará lo siguiente:

1. *El concepto de tratamiento.*
2. *La naturaleza y alcance de la figura de responsable.*
3. *La naturaleza y alcance de la figura de encargado.*
4. *La inviolabilidad de comunicaciones a la luz del derecho de protección de datos personales.*
5. *Las reglas generales sobre la aplicación de normas sustantivas y procedimentales a un caso concreto.*

Lo anterior, con base en lo dispuesto en la Ley General, los Lineamientos Generales, la Ley Federal y su Reglamento.

V. Consideraciones

[...]

4. La inviolabilidad de comunicaciones a la luz del derecho de protección de datos personales

Al respecto, el artículo 16 de la Constitución dispone lo siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Por su parte, es menester traer a colación diversas tesis emitidas por el Poder Judicial de la Federación respecto al derecho a la inviolabilidad de las comunicaciones:

[...]

Así, de las tesis invocadas respecto del derecho a la inviolabilidad de las comunicaciones se desprenden las siguientes premisas:

- *El derecho a la inviolabilidad de las comunicaciones posee una autonomía propia reconocida por la Constitución. Dicho derecho tiene por objeto proteger las comunicaciones con independencia de su contenido, lo cual se extiende a aquellos datos que identifican la comunicación como, por ejemplo, el registro de los números marcados por un usuario de la red telefónica; la identidad de los comunicantes; la duración de la llamada telefónica o la identificación de una dirección de protocolo de Internet (IP).*
- *La violación de este derecho se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra una comunicación ajena sin el consentimiento de los interlocutores o sin autorización judicial, con independencia de que, con posterioridad, se difunda el contenido de la conversación interceptada.*
- *El derecho a la inviolabilidad de las comunicaciones es oponible tanto a las autoridades como a los gobernados, quienes al transgredir esta prerrogativa incurren en la comisión de un ilícito constitucional.*
- *El derecho a la inviolabilidad de las comunicaciones no se vulnera cuando uno de los interlocutores levanta la confidencialidad del contenido de ésta.*
- *Las comunicaciones privadas protegidas en -sede constitucional- no quedan restringidas a las comunicaciones de carácter escrito, la Constitución no limita los medios por los cuales pueda producirse la comunicación objeto de protección. En ese sentido, todas las formas existentes de comunicación quedan protegidas al amparo de este derecho.*
- *Para efectos de consumir la violación de este derecho humano se requiere la intencionalidad de un tercero ajeno a la comunicación y no como consecuencia de un error o casualidad.*
- *La intervención de comunicaciones no podrá autorizarse en razón de la materia electoral, fiscal, mercantil, civil, laboral o administrativa.*
- *Exclusivamente, la autoridad judicial federal es la única que se encuentra facultada para autorizar la intervención de comunicaciones.*
- *Resultan autoridades competentes para solicitar la intervención de comunicaciones las autoridades federales que la ley respectiva faculte o en su caso, el titular del Ministerio Público de la entidad federativa correspondiente. Esta petición deberá fundarse y motivarse expresando las causas legales de la solicitud, expresando, además, el tipo de intervención, los sujetos de la misma y su duración.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Cualquier grabación de la intervención de comunicaciones que no se encuentre autorizada en términos del precepto constitucional que lo tutela constituye una prueba ilícita que carece de todo valor probatorio.*
- *Si la intervención de comunicaciones se realiza sin autorización judicial, cualquier prueba que emane de ésta será considerada como ilícita, aún en investigaciones en materia de delincuencia organizada.*
- *Cuando la intervención de las comunicaciones privadas se realiza sin una autorización judicial, cualquier prueba extraída, o bien, derivada de ésta, será considerada como ilícita y no tendrá valor jurídico alguno.*

Por otro lado, conviene traer a colación lo dispuesto en el artículo 17 de la Ley General:

[...]

A su vez, el artículo 8 de los Lineamientos Generales prevé lo siguiente:

[...]

Por su parte, el artículo 7 de la Ley Federal dispone lo siguiente:

[...]

En este mismo sentido, el artículo 10 del Reglamento señala lo que a continuación se indica:

[...]

De las disposiciones citadas se advierte que el principio de licitud implica la obligación que tiene el responsable de tratar los datos personales con apego y cumplimiento de lo dispuesto por la legislación mexicana y el derecho internacional que le resulte aplicable.

Ahora bien, en caso de que a través del software aludido se hubiere intervenido comunicaciones sin el cumplimiento de las formalidades y requisitos previstos en la Constitución y señalados por la Suprema Corte de Justicia de la Nación se estaría vulnerando el principio de licitud y por consiguiente, el responsable de que se trate podría estar sujeto a una sanción o responsabilidad administrativa, según corresponda.

En caso contrario, la posible intervención de comunicaciones podría ser lícita y, en consecuencia, podría concluirse que los datos personales fueron tratados conforme al marco jurídico nacional y, en su caso, internacional que resulte aplicable.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. Las reglas generales sobre la aplicación de normas sustantivas y adjetivas a un caso concreto

De acuerdo con la función que desempeñan las normas jurídicas pueden clasificarse en sustantivas o adjetivas. Es decir, en la medida en que una disposición reconozca un derecho sustantivo o imponga alguna obligación sustantiva, se deberá considerar que se trata de una disposición de carácter sustantiva; pero si dicha disposición únicamente instrumenta el procedimiento para hacer efectivo un derecho o el cumplimiento de una obligación, aun cuando tal procedimiento establezca derechos y obligaciones de carácter procesal, deberá ser considerada como una norma procesal.

Bajo ese contexto, el Poder Judicial Federal ha manifestado que cuando una norma tiene una función instrumental será de carácter procesal y, consecuentemente, si regula el fondo de una situación jurídica tendrá el carácter de sustantiva.

5.1. Aplicación de normas adjetivas a un caso concreto

Al respecto, resulta necesario traer a colación lo manifestado por la Suprema Corte de Justicia de la Nación en la siguiente tesis.

"NORMAS PROCESALES. SON APLICABLES LAS VIGENTES AL MOMENTO DE LLEVARSE A CABO LA ACTUACIÓN RELATIVA, POR LO QUE NO PUEDE ALEGARSE SU APLICACIÓN RETROACTIVA. *Tratándose de normas procesales, las partes no adquieren el derecho a que la contienda judicial en la que intervienen se tramite al tenor de las reglas del procedimiento en vigor al momento en que haya nacido el acto jurídico origen del litigio, ni al de las vigentes cuando el juicio inicie, toda vez que los derechos emanados de tales normas nacen del procedimiento mismo y se agotan en cada etapa, de ahí que cada una de sus fases se rija por la regla vigente al momento en que se desarrolla, excepto en los casos en que en el decreto de reformas relativo se hayan establecido disposiciones expresas sobre su aplicación en otro sentido. En consecuencia, cuando se trata de normas de carácter adjetivo no puede alegarse la aplicación retroactiva de la ley, proscrita en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos."*

De lo anteriormente expuesto es posible advertir los siguientes razonamientos:

- Tratándose de normas procesales, las partes no adquieren el derecho a que la contienda judicial en la que intervienen se tramite al tenor de las reglas del procedimiento en vigor al momento en que haya nacido el acto jurídico origen del litigio, ni al de las vigentes cuando el juicio inicie.*
- Los derechos emanados de las normas adjetivas nacen del mismo procedimiento, por lo que se agotan en cada etapa procesal.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Cada una de las fases del procedimiento se debe regir por la regla vigente al momento en que se desarrolla, excepto en los casos en que en el decreto de reformas relativo se hayan establecido disposiciones expresas sobre su aplicación en otro sentido.*
- *Cuando se trata de normas de carácter adjetivo no puede alegarse la aplicación retroactiva de la ley, proscrita en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, al no existir derechos adquiridos, opuestamente a lo que ocurre en el caso de normas sustantivas.*

5.2. Aplicación de normas sustantivas a un caso concreto

En primer término, es de precisarse que la doctrina y la Suprema Corte de Justicia de la Nación han distinguido tres momentos de aplicación de las leyes:

- *Vigencia actual: cuando éstas se encuentran vigentes y rigen un hecho realizado bajo esa vigencia.*
- *Retroactividad: cuando se aplican a un hecho efectuado antes de su entrada en vigor.*
- *Ultractividad: cuando se aplican después que concluyó su vigencia.*

Por lo tanto, en la aplicación de normas a actos jurídicos que ocurrieron en diferente temporalidad. Se deberán observar las reglas que rigen lo relativo a la ultractividad y la retroactividad.

5.3. Retroactividad

Al respecto, resulta preciso traer a colación lo previsto por la Segunda Sala de la Suprema Corte de Justicia de la Nación en el amparo en revisión 607/2000:

[...]

De lo anteriormente expuesto es posible apreciar los siguientes razonamientos:

- *Un ordenamiento o su aplicación tienen carácter o efectos retroactivos cuando afectan situaciones o derechos que están estrechamente vinculados con su fuente y no pueden apreciarse de manera independiente. En ese sentido, la retroactividad de una ley guarda íntima relación con los derechos adquiridos.*
- *Los derechos adquiridos son aquéllos que han entrado al patrimonio del individuo, su dominio o a su haber jurídico y los cuales no se le pueden arrebatar. En otras palabras, son aquéllos que implican que se introduce un bien, una facultad o un provecho al patrimonio de una persona o haber jurídico.*
- *De esta forma, para la aplicación retroactiva de un ordenamiento jurídico resulta trascendental examinar y aquilatar los motivos de utilidad social que contribuyan a la*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

aplicación inmediata de la nueva ley, así como los derechos adquiridos que aspiran a protegerse en las normas de la antigua ley.

En resumen, el análisis sobre la aplicación retroactiva de una ley implica verificar si el acto concreto se lleva a cabo dentro de su ámbito temporal de validez sin afectar situaciones jurídicas definidas o derechos adquiridos por el gobernado con anterioridad a su entrada en vigor.

Ahora bien, para resolver sobre la retroactividad de una disposición jurídica es fundamental determinar las hipótesis que pueden presentarse en relación con el tiempo, ya que puede suceder que su realización ocurra fraccionada en el tiempo. Esto acontece, por lo general, cuando el supuesto y la consecuencia son actos complejos, compuestos por diversos actos parciales.

Al respecto, el Pleno de la Suprema Corte de Justicia de la Nación ha definido las siguientes hipótesis:

"RETROACTIVIDAD DE LAS LEYES, SU DETERMINACIÓN CONFORME A LA TEORÍA DE LOS COMPONENTES DE LA NORMA. [...]"

De la jurisprudencia anteriormente expuesta es posible advertir diversas hipótesis y la respectiva solución jurídica definida por el máximo Tribunal Constitucional:

- Cuando durante la vigencia de una norma jurídica se actualizan, de modo inmediato, el supuesto y la consecuencia establecidos en ella. En este caso, ninguna disposición legal posterior podrá variar, suprimir o modificar aquel supuesto o esa consecuencia sin violar la garantía de irretroactividad, atento que fue antes de la vigencia de la nueva norma cuando se realizaron los componentes de la norma sustituida.*
- En el caso en que la norma jurídica establezca un supuesto y varias consecuencias sucesivas. Si dentro de la vigencia de esta norma se actualiza el supuesto y alguna o algunas de las consecuencias, pero no todas, ninguna norma posterior podrá variar los actos ya ejecutados sin ser retroactiva.*
- También puede suceder que la realización de alguna o algunas de las consecuencias de la ley anterior, que no se produjeron durante su vigencia, no dependa de la realización de los supuestos previstos en esa ley, ocurridas después de que la nueva disposición entró en vigor, sino que tal realización estaba solamente diferida en el tiempo, ya sea por el establecimiento de un plazo o término específico, o simplemente porque la realización de esas consecuencias era sucesiva o continuada; en este caso la nueva disposición tampoco deberá suprimir, modificar o condicionar las consecuencias no realizadas, por la razón sencilla de que estas no están supeditadas a las modalidades señaladas en la nueva ley.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- *Cuando la norma jurídica contempla un supuesto complejo, integrado por diversos actos parciales sucesivos y una consecuencia. En este caso, la norma posterior no podrá modificar los actos del supuesto que se haya realizado bajo la vigencia de la norma anterior que los previó, sin violar la garantía de irretroactividad. Pero en cuanto al resto de los actos componentes del supuesto que no se ejecutaron durante la vigencia de la norma que los previó si son modificados por una norma posterior, ésta no puede considerarse retroactiva.*

En esta circunstancia, los actos o supuestos habrán de generarse bajo el imperio de la norma posterior y, consecuentemente, son las disposiciones de ésta las que deben regir su relación, así como la de las consecuencias que a tales supuestos se vinculan.

5.4. Ultractividad

El principio de ultractividad de la norma sustantiva tiende a satisfacer uno de los fines primordiales del derecho; la seguridad jurídica. Así, es posible que una norma, a pesar de haber perdido vigencia, se siga aplicando a hechos o actos producidos con posterioridad al inicio de la vigencia de una nueva ley.

Ahora bien, es de precisarse que la ultractividad opera bajo una prescripción temporal que, generalmente, dota de mayor seguridad jurídica al ciudadano, mediante la agilización de procedimientos que ya se encontraban en trámite. Ello, con la finalidad de evitar dificultades en su desarrollo ante lo contundente de las innovaciones previstas por una nueva legislación. Véase la siguiente tesis:

"IRRETROACTIVIDAD DE LA LEY. EL ARTÍCULO TERCERO TRANSITORIO DEL DECRETO POR EL QUE SE REFORMA EL CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL, PUBLICADO EN LA GACETA OFICIAL DE LA ENTIDAD EL 10 DE SEPTIEMBRE DE 2009, NO VIOLA ESE PRINCIPIO. [...]"

[Énfasis añadido]

En ese sentido, la ultractividad trae como consecuencia que siga teniendo vigencia una disposición o ley anterior, siempre y cuando la nueva norma suprima o afecte los efectos producidos por los hechos que se realizaron antes de su vigencia. Sirve de sustento a lo anteriormente expuesto la siguiente tesis:

"DERECHO A LA REDUCCIÓN DE UN TERCIO DE LA PENA MÍNIMA IMPUESTA Y A LA CONCESIÓN DE LOS BENEFICIOS QUE PROCEDAN PREVISTO EN EL ARTICULO 389, PÁRRAFO CUARTO, DEL CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL ESTADO DE MÉXICO. AL SER UNA PRERROGATIVA FUNDAMENTAL DEL INculpado Y NO UNA NORMA PROCESAL, ESTÁ SUJETO A LA EXCEPCIÓN



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

**CONTENIDA EN EL ARTICULO 14 CONSTITUCIONAL EN CUANTO A LA
APLICACIÓN ULTRA ACTIVA DE LA LEY EN BENEFICIO DEL QUEJOSO. [...]**

[Énfasis añadido]

Ahora bien, la ultractividad es improcedente cuando se reclama un derecho creado o reconocido por una norma administrativa que no rigió la relación jurídica pretendidamente generadora de él, sino que nació una vez terminada ésta y posteriormente dejó de estar en vigor. Sirve de sustento a lo anterior lo manifestado por el Poder Judicial de la Federación en la siguiente tesis:

"ULTRACTIVIDAD DE LAS LEYES. ES IMPROCEDENTE CUANDO SE RECLAMA UN DERECHO CREADO O RECONOCIDO POR UNA NORMA ADMINISTRATIVA QUE NO RIGIÓ LA RELACIÓN JURÍDICA PRETENDIDAMENTE GENERADORA DE ÉL, SINO QUE NACIÓ UNA VEZ TERMINADA ÉSTA Y POSTERIORMENTE DEJÓ DE ESTAR EN VIGOR, DE MODO QUE YA NO ERA APLICABLE CUANDO EL INTERESADO HIZO SU RECLAMACIÓN. [...]"

[Énfasis añadido]

Una vez aclarado lo anterior, es de precisarse que el principio de jerarquía normativa desempeña un papel primordial en la aplicación de la ultractividad. Por lo tanto, la derogación de las normas y la eventual orden de ultractividad del ordenamiento o de una parte de él solamente puede establecerse en una disposición del mismo rango o en una superior (que tenga idéntico ámbito material y goce de mayor fuerza). En ese orden de ideas, la Suprema Corte de Justicia de la Nación, durante la sustanciación del amparo directo en revisión 5609/2014, aclara lo siguiente:

"De modo que una ley puede derogar otra Ley y establecer los casos en que opere la ultractividad, como también una ley puede derogar un reglamento y prescribir que algunas de sus normas sigan vigentes o que, el reglamento -en su totalidad- debe seguir aplicándose a ciertos casos específicos; sin embargo, ese razonamiento no opera a la inversa, precisamente por qué, no puede una disposición transitoria contenida en la norma inferior, establecer la ultractividad de una ley que le es impropia pues, en todo caso, es la ley derogatoria la que debe establecer una prórroga de la vigencia de sus normas".

[Énfasis añadido]

Así, la ultractividad debe entenderse como un fenómeno por el cual una ley derogada o abrogada sigue produciendo efectos posteriores y continúa vigente para algunos casos concretos, ello, a pesar de su expulsión del orden jurídico.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Dicho en otras palabras, el principio de ultractividad de la ley consiste en que una determinada norma, a pesar de haber quedado sin efectos, se sigue aplicando a hechos o actos posteriores al inicio de la vigencia de la nueva ley, lo que implica que la ley eliminada siga teniendo vigencia. Una vez aclarado lo anterior, es de precisarse que es posible que una norma, a pesar de haber sido derogada o abrogada (eliminada del orden jurídico), se siga aplicando a hechos o actos que se producen con posterioridad al inicio de la vigencia de la nueva ley, siempre y cuando se trate de derechos sustantivos y en beneficio del gobernado.

De tal suerte que, la derogación impide la futura aplicación de una norma y la posibilidad de que produzca efectos jurídicos al destruir su vigencia, pero no elimina la aplicabilidad de la norma porque en ciertos casos continúa formando parte del sistema jurídico (ultractividad).

Así, la supervivencia temporal de las normas derogadas se permite en un sistema jurídico, como un recurso de justicia que actualiza la aplicación a casos pendientes de resolución para impedir la vulneración de derechos adquiridos.

Ahora bien, la ultractividad se activa bajo ciertos supuestos específicos, por ejemplo, cuando una norma suprime o afecta los efectos producidos por los hechos que se realizaron antes de la vigencia de una nueva ley. En ese caso, la ley anterior permanece vigente, y, por ende, se continúa aplicando.

[...] (sic)

72. El veintiuno de marzo de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/STP-DGCR/113/2018** de la misma fecha, emitido y signado por el director general de cumplimientos y responsabilidades de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/0059/18** descrito en el **antecedente 70**, indicando lo siguiente:

[...]

En atención al oficio INAI/SPDP/DGEIVSP/0059/18, primeramente, resulta pertinente destacar que de conformidad con lo dispuesto en el artículo 36, fracción II, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, esta Dirección General a mi cargo, es la encargada de verificar el cumplimiento que los sujetos obligados den a las resoluciones de los medios de impugnación emitidas por el Pleno de este Instituto con instrucción, por lo cual, el requerimiento efectuado se atenderá



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

con base en la información que en atención a su competencia resguarda esta Dirección General.

En tal virtud, me permito informar sobre lo solicitado en los siguientes términos:

- *El estado que guarda el cumplimiento de la resolución emitida por Pleno de este Instituto con motivo del recurso de revisión en materia de acceso a la información y/o protección de datos personales RRA 6309/17, interpuesto en contra de la Procuraduría General de la República.*

Al respecto, es importante mencionar que en la resolución en comento en su resolutivo PRIMERO modifica la respuesta de la Procuraduría General de la República y en su resolutivo SEGUNDO instruye para que en un plazo de diez días hábiles a partir del siguiente al de su notificación, cumpla con lo ordenado en el considerando CUARTO de la misma.

*R= Con fecha veinte de febrero de dos mil diecisiete, la Procuraduría General de la República notificó a la parte recurrente la respuesta emitida en vía de cumplimiento, que consistió **en la notificación de disponibilidad de la versión pública del instrumento contractual y anexo solicitados**, en la modalidad de copia simple y certificada, misma que obra en un total de sesenta y un fojas, indicando para tal efecto los costos por concepto de reproducción en ambas modalidades; asimismo hizo de su conocimiento que la información podría ser entregada en las instalaciones que ocupa su Unidad de Transparencia y Apertura Gubernamental, o bien, podría ser enviada a su domicilio previo pago del envío correspondiente, para lo cual solicitó al particular informara a la Unidad de Transparencia sobre la modalidad de su elección y señalara si era si deseo cubrir los costos de envío, para estar en posibilidad de generar la ficha de pago correspondiente.*

En relación con lo anterior, resulta oportuno señalar que el artículo 138 de la Ley Federal de Transparencia y Acceso a la Información Pública, señala que la información deberá de entregarse siempre que el solicitante compruebe haber cubierto el pago de las cuotas de reproducción correspondientes; asimismo, los diversos 135 de la Ley General de Transparencia y Acceso a la Información Pública, y 139 de la Ley Federal en comento, refieren que el pago respectivo deberá efectuarse en un plazo no mayor a treinta días.

*En ese sentido, se hace constar que **el plazo concedido a la parte promovente** para que informe a la Unidad de Transparencia si es de su interés obtener la información en la modalidad de copia simple o certificada, con el objeto de que le sea generada la ficha de pago por concepto de reproducción y en su caso de envío, **se encuentra transcurriendo fenece el día once de abril del año en curso**, de conformidad el*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

artículo 28 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a la materia, en relación con el artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública.

No se omite señalar que una vez cubiertos los costos de reproducción, se procederá a la elaboración de la versión pública, y el sujeto obligado deberá concertar una cita con esta área, con la finalidad de verificar la información, lo anterior en términos de lo dispuesto por el párrafo segundo del artículo 157 de la Ley Federal de Transparencia y Acceso a la Información Pública.

- *Copia simple de los documentos que acrediten la información que proporcione en relación con el recurso de revisión indicado, así como de cualquier otra información y documentación (física y electrónica) vinculada con el uso del software (malware) identificado como "Pegasus", en colaboración con la investigación que se sigue ante esa Dirección General.*

R= De acuerdo con la información con que cuenta esta Dirección General de acuerdo con su competencia en los términos precisados anteriormente, se remite la totalidad de la documentación a través de la que la Procuraduría General de la República pretende acreditar el cumplimiento al recurso de revisión RRA 6309/17, ello en el entendido de que dentro de las constancias -remitidas por la parte promovente a través del desahogo de la vista con la respuesta del sujeto obligado- se encuentran dos notas periodísticas en idioma extranjero, y se hace entrega tal cual fueron presentadas por las partes, en razón de que, dentro de las atribuciones de esta Dirección General, no se encuentra la de elaborar traducción de las mismas.

[...]

a) Adjunto, se remitió:

- Oficio PGR/UTAG/DG/000937/2018 del veinte de febrero de dos mil dieciocho, emitido por la titular de la Unidad de Transparencia y Apertura Gubernamental de la entonces Procuraduría General de la República, dirigido al director general de cumplimientos y responsabilidades de este Instituto, por el que informa sobre el cumplimiento dado a la resolución **RRA 6309/17**.
- Correo electrónico remitido el veintidós de febrero de dos mil dieciocho a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual el jefe de departamento de cumplimientos E de este Instituto,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

le solicitó manifestar lo que a su derecho convenga respecto del cumplimiento dado por la entonces Procuraduría General de la República a la resolución del recurso de revisión **RRA 6309/17**.

- Correo electrónico del veintisiete de febrero de dos mil dieciocho, por el que el recurrente realizó manifestaciones respecto del cumplimiento proporcionado por la entonces Procuraduría General de la República a la resolución del recurso de revisión **RRA 6309/17**.
- Correo electrónico remitido el doce de marzo de dos mil dieciocho a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual el jefe de departamento de cumplimientos E de este Instituto, le remitió un alcance enviado por la entonces Procuraduría General de la República.
- Correo electrónico remitido el trece de marzo de dos mil dieciocho a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual el jefe de departamento de cumplimientos E de este Instituto, le solicitó manifestar lo que a su derecho convenga respecto del alcance al cumplimiento remitido.

73. Mediante el oficio número **INAI/SPDP/DGEIVSP/139/18** del once de mayo de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al director general de cumplimientos y responsabilidades de este Instituto, lo siguiente:

[...]

Al respecto, a efecto de continuar con el seguimiento de la investigación previa que nos ocupa, con fundamento en los artículos [...], me permito solicitarle su amable colaboración a efecto de que se sirva girar sus apreciables instrucciones a quien corresponda a efecto de que se brinde la siguiente información a este Instituto:

1. *El estado que guarda el cumplimiento de la resolución emitida por el Pleno de ese Instituto con motivo del recurso de revisión en materia de acceso a la información y/o protección de datos personales RRA 6309/17, Interpuesto en contra de la Procuraduría General de la República; debiendo indicar, de acuerdo a lo referido en el oficio INAI/STP-DGCR/112/2018, si se cubrieron los costos de reproducción de la información*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

puesta a disposición del particular, de acuerdo a la modalidad elegida y, como consecuencia, indique si se procedió a la elaboración de la versión pública correspondiente y ésta fue entregada al recurrente. Asimismo, deberá indicar si cuenta en sus archivos con la versión pública de la información que se ordenó entregar al recurrente; en caso de ser así, solicito remita copia certificada de la misma.

2. *El estado que guarda el cumplimiento de la resolución emitida por el Pleno de este Instituto con motivo del recurso de revisión en materia de acceso a la información y/o protección de datos personales RRA 0115/18, Interpuesto en contra de la Procuraduría General de la República.*

Al respecto, es importante mencionar que en la resolución en comento en su resolutive PRIMERO modifica la respuesta de la Procuraduría General de la República y en su resolutive SEGUNDO se le instruye al sujeto obligado para que en un plazo de diez días hábiles a partir del siguiente al de su notificación, cumpla con lo ordenado en el considerando CUARTO de la misma.

No omito señalar, que resulta indispensable que al atender el presente requerimiento, se sirva remitir copia de los documentos que acrediten la información que proporcionará en relación con los recursos de revisión indicados, así como de cualquier otra información y documentación (física y electrónica) vinculada con el uso de software (malware) identificado como "Pegasus", con colaboración con la investigación que se sigue ante esta Dirección General.

[...] (sic)

El requerimiento se notificó a la Dirección General de Cumplimientos y Responsabilidades, el quince de mayo de dos mil dieciocho.

74. El veintidós de mayo de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/STP-DGCR/193/2018** de la misma fecha, emitido y signado por el director general de cumplimientos y responsabilidades de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/139/18** descrito en el **antecedente 73**, indicando lo siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En atención al oficio INAI/SPDP/DGEIVSP/139/18, primeramente, resulta pertinente destacar que conformidad con lo dispuesto en el artículo 36, fracción II, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, esta Dirección General a mi cargo, es la encargada de verificar el cumplimiento que los sujetos obligados den a las resoluciones de los medios de impugnación emitidas por el Pleno de este Instituto con instrucción, por lo cual, el requerimiento efectuado se atenderá con base en la información que en atención a su competencia resguarda esta Dirección General.

En tal virtud, me permito informar sobre lo solicitado en los siguientes términos:

- 1. El estado que guarda el cumplimiento de la resolución identificada como RRA 6309/17, es de cumplimiento por caducidad, ya que de acuerdo con lo informado a este Instituto por el sujeto obligado, transcurrido el término legal para ello, en razón de que el particular no cubrió los costos de reproducción de la información puesta a su disposición, asimismo hago de su conocimiento que esta Dirección General no cuenta en sus archivos con la versión pública de la información que se ordenó entregar al recurrente relacionado con el cumplimiento de marras.*
- 2. Con relación al estado que guarda el cumplimiento de la resolución identificada como RRA 0115/18, le informo que el día de hoy se encuentra en proceso, ya que en esta fecha el sujeto obligado solicitó a esta Dirección General la cita para realizar la verificación de la versión pública de la información puesta a disposición del recurrente en los términos ordenados para el efecto; diligencia que se llevará a cabo el día de mañana miércoles 23 de mayo del año en curso, en las instalaciones que para ello señaló la Procuraduría General de la República. Asimismo, le informo que a la fecha no obra en los archivos de esta Dirección General la versión pública de la información que deberá entregar el sujeto obligado en cumplimiento.*
- 3. Con relación a su solicitud de remisión de copias de los documentos que acrediten la información que se proporciona por parte de esta Dirección General en relación con los recursos de revisión anteriormente indicados, se adjunta al presente las copias solicitadas que dan cuenta de lo informado.*
- 4. Por último, respecto de la solicitud de envío de cualquier otra información y documentación vinculada con el uso del software (malware) identificado como "Pegasus"; le informo que después de una consulta a los responsables del seguimiento de las resoluciones turnadas a esta Dirección General, así como a las bases de datos con que se cuenta, se informa que no se advirtió ninguna otra resolución en seguimiento a cargo de esta Dirección, de la que se desprenda que lo solicitado por el particular interesado o de lo instruido por el Pleno, esté claramente vinculada con el software denominado "Pegasus" o que se cuente con alguna información o documentación adicional a lo que esta Dirección General ya ha hecho del conocimiento y proporcionado a esa Dirección General a su digno cargo: en este oficio y anteriores.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

a) Adjunto, se remitió:

- Correo electrónico del doce de abril de dos mil dieciocho, remitido por el director de acceso a la información de la entonces Procuraduría General a la República, a la Dirección General de Cumplimientos y Responsabilidades de este Instituto, por el que se solicita se emita el acta de cumplimiento en el **RRA 6309/17**.
- Acuerdo del trece de abril de dos mil dieciocho, emitido por el director general de cumplimientos y responsabilidades de este Instituto, por el que tuvo por cumplida por parte de la entonces Procuraduría General de la República, la resolución del recurso de revisión **RRA 6309/17**.
- Correo electrónico remitido el diecinueve de abril de dos mil dieciocho a la dirección señalada por el recurrente como medio para recibir notificaciones, a través del cual el jefe de departamento de cumplimientos E de este Instituto, le notificó el acuerdo dictado el trece de abril de dos mil dieciocho.
- Notificación a través de la Herramienta de Comunicación a la entonces Procuraduría General de la República, del acuerdo del trece de abril de dos mil dieciocho.
- Correo electrónico del veintidós de mayo de dos mil dieciocho, remitido por la Unidad de Transparencia y Apertura Gubernamental de la entonces Procuraduría General a la República al director general de cumplimientos y responsabilidades de este Instituto, por el que le informa que el particular acreditó haber cubierto el pago de los costos de reproducción de los documentos que se pusieron a su disposición para dar cumplimiento a la resolución dictada en el recurso de revisión **RRA 0115/18**; así como, el día y hora para que acudiera a sus oficinas a realizar la revisión de la versión pública.

75. Mediante el oficio número **INAI/SPDP/DGEIVSP/162/18** del veinticuatro de mayo de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Sector Público solicitó al director general de cumplimientos y responsabilidades de este Instituto, lo siguiente:

[...]

Me refiero al oficio número INAI/STP-DGCR/193/2018 del veintidós de mayo de dos mil dieciocho, mediante el cual dio atención al requerimiento formulado mediante oficio número INAI/SPDP/DGEIVSP/0139/18.

Al respecto, a efecto de continuar con el seguimiento de la investigación previa que nos ocupa, con fundamento en los artículos [...] y, con la finalidad de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público, se allegue de los elementos necesarios para resolver lo que en derecho corresponda, me permito solicitarle su amable colaboración a efecto de que se sirva girar sus apreciables instrucciones a quien corresponda a efecto de que se brinde la siguiente Información:

En relación con su informe relativo al cumplimiento de la resolución al recurso de revisión RRA 115/18, mediante el cual indicó lo siguiente:

"Con relación al estado que guarda el cumplimiento de la resolución identificada como RRA0115/18, le informo que el día de hoy se encuentra en proceso, ya que en esta fecha el sujeto obligado solicitó a esta Dirección General la cita para realizar la verificación de la versión pública de la información puesta a disposición del recurrente en los términos ordenados para el efecto: diligencia que se llevará a cabo el día de mañana miércoles 23 de mayo del año en curso, en las instalaciones que para ello señaló la Procuraduría General de la República. Asimismo, le informo que a la fecha no obra en los archivos de esta Dirección General la versión pública de la información que deberá entregar el sujeto obligado en cumplimiento".

Resulta indispensable conocer a) si se llevó a cabo la diligencia de verificación de la versión pública del contrato respectivo en la Procuraduría General de la República; b) si, en su caso, se autorizó la versión pública conducente para formalizar su entrega al particular y; c) si la Dirección General a su digno cargo, como resultado de la referida diligencia, cuenta con la versión pública de la documentación que se ordenó entregar al recurrente en cumplimiento a la resolución de mérito; debiendo en su caso, remitir copia certificada de la misma.

*Le agradeceré haga del conocimiento de esta unidad administrativa lo referido con anterioridad, en un término máximo de (5) **cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

El requerimiento se notificó a la Dirección General de Cumplimientos y Responsabilidades, el veinticuatro de mayo de dos mil dieciocho.

76. El treinta y uno de mayo de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/STP-DGCR/213/2018** de la misma fecha, emitido y signado por el director general de cumplimiento y responsabilidades de este Instituto, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/162/18** descrito en el **antecedente 75**, indicando lo siguiente:

[...]

En atención al oficio INAI/SPDP/DGEIVSP/162/18, primeramente, resulta pertinente destacar que de conformidad con lo dispuesto en el artículo 36, fracción II, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, esta Dirección General a mi cargo es la encargada de verificar el cumplimiento que los sujetos obligados den a las resoluciones de los medios de impugnación emitidas por el Pleno de este Instituto con instrucción, por lo cual, el requerimiento efectuado se atenderá con base en la información que en atención a su competencia resguarda esta unidad administrativa.

- *En tal virtud, me permito informar sobre lo solicitado, en los siguientes términos: En atención al inciso a), le comunico que los días veintitrés y veinticuatro de mayo de la presente anualidad, se llevó a cabo, en las instalaciones de la Agencia de Investigación Criminal, la verificación de la versión pública de la información instruida en el expediente RRA 0115/18, consistente en el contrato para la adquisición del sistema para la realización de actividades sustantivas y su anexo técnico, elaborada por la Procuraduría General de la República.*
- *En cuanto al apartado b), se informa que esta Dirección General autorizó la versión pública respectiva, para que procediera su entrega al particular; para ello, se remite copia certificada de la minuta de reunión de trabajo correspondiente.*
- *Por último, se hace de su conocimiento que en los archivos de esta unidad administrativa no obra la versión pública de la documentación que se ordenó entregar, tal y como consta en la minuta que se le hace llegar.*

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- a) Adjunto se remitió la MINUTA DE LA REUNIÓN DE TRABAJO CELEBRADA LOS DÍAS VEINTITRÉS Y VEINTICUATRO DE MAYO DE DOS MIL DIECIOCHO, EN LA AGENCIA DE INVESTIGACIÓN CRIMINAL, CON LA FINALIDAD DE VERIFICAR LA VERSIÓN PÚBLICA ELABORADA POR LA PROCURADURÍA GENERAL DE LA REPÚBLICA EN CUMPLIMIENTO A LA RESOLUCIÓN AL RECURSO DE REVISIÓN RRA 0115/18.

77. Mediante el oficio número **INAI/SPDP/DGEIVSP/191/18** del trece de junio de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

*Hago referencia al acuerdo dictado el treinta de junio del dos mil diecisiete, mediante el cual se ordenó iniciar, de oficio, el expediente de investigación preliminar, con el número **INAI.3S.08.03-003/2017**, relacionado con el tratamiento de datos personales que, en su caso, se haya efectuado derivado de la presunta existencia de espionaje y ciber vigilancia por parte del Gobierno Federal de los Estados Unidos Mexicanos, a través del software (malware) identificado como "Pegasus".*

En ese sentido, en seguimiento a las diligencias de investigación propias del expediente en que se actúa y toda vez que se tiene conocimiento de que en cumplimiento a la resolución del recurso de revisión RRA 115/18, emitida por el Pleno de este Instituto, se ha generado la versión pública del contrato para la adquisición de un sistema para realización de actividades sustantivas de la Procuraduría General de la República y de su anexo técnico; con fundamento en los artículos [...], con la finalidad de contar con mayores elementos para estar en posibilidad de resolver lo que en derecho corresponda en relación con los hechos que se investigan, me permito solicitar su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda, para que se sirva proporcionar la siguiente información y documentación:

1. *Copia de la versión pública del contrato para la adquisición del sistema para la realización de actividades sustantivas y su anexo técnico, celebrado por la Procuraduría General de la República y la persona moral Grupo Tech Bull, S.A. de C.V.*
2. *Indique si a través de la tecnología adquirida es factible recabar datos personales de particulares y de qué tipo serían estos.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Considerando los hechos que se investigan en el expediente citado al rubro y que han sido de su conocimiento, indique si a través de la tecnología adquirida se recabaron datos personales de particulares.*
4. *Indique las atribuciones legales que facultan a la Procuraduría General de la República para la contratación y uso de la tecnología adquirida.*
5. *Indique en términos generales, cuáles son las actividades sustantivas de la Procuraduría General de la República que se realizan a partir del uso de la tecnología adquirida.*
6. *Indique los motivos o supuestos legales por los cuales puede hacerse uso de la tecnología adquirida que nos ocupa.*
7. *Señale si ha recibido autorización judicial para el uso de la tecnología adquirida y, en su caso, remita el registro o constancia en la que consten las autorizaciones respectivas en cada caso que haya sido utilizada.*
8. *Explique en qué consiste el tratamiento de datos personales que la Procuraduría General de la República dio a partir del uso de la tecnología adquirida.*
9. *Indique si durante los años 2014, 2015 y 2016 se recabaron datos personales a través del uso de la tecnología adquirida.*
10. *Indicar si los datos personales recabados, en su caso, fueron integrados a un sistema de gestión de datos personales de la dependencia.*
11. *Indique, en su caso, si los datos personales recabados fueron objeto de transferencia a terceros.*
12. *Indique los medios o fuente de los datos personales que pueden recabarse a través del uso de la tecnología adquirida.*
13. *Proporcione la información adicional que pudiera coadyuvar con el desarrollo de la presente investigación.*

Le agradeceré haga del conocimiento de esta unidad administrativa lo referido con anterioridad, en un término máximo de (5) cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el quince de junio de dos mil dieciocho.

78. El veintiuno de junio de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

DGAJ/02212/2018 del veinte de junio de dos mil dieciocho, emitido y signado por la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/191/18** descrito en el **antecedente 77**, indicando lo siguiente:

[...]

*Con fundamento en los artículos 7, 10, fracción VI y 32 de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Directora General de Asuntos Jurídicos, en representación jurídica de la o el Titular de la Procuraduría General de la República, me refiero a su diverso **INAI/SPDP/DGEIVSP/191/18**, relativo al expediente **INAI.3S.08.03-003/2017** por el que solicita se proporcione la documentación e información adicional que en el ocurso de cuenta se detalla.*

Sobre el particular, en relación con la documentación e información adicional que se solicita. Le comunico lo siguiente:

1. *Copia de la versión pública del contrato para la adquisición del software, licencia o herramienta tecnológica desarrollada por la firma NSO Group (Grupo Tech Bull, S.A. de C.V.).*

Respuesta:

Se anexa copia de la versión pública del contrato requerido.

2. *Indique si a través de la tecnología adquirida es factible recabar datos personales de particulares, y de qué tipo serían estos.*

Respuesta:

Esta Institución está impedida para pronunciarse al respecto, ya que aún en el caso de que en el periodo que comprende la investigación realizada por ese órgano garante la tecnología adquirida no fue utilizada, la divulgación de cualquier dato relacionado con la misma comprometería la seguridad nacional en términos de lo dispuesto por los artículos 37, 42, 47 y 48 de la Ley de Seguridad Nacional y la estricta reserva de la información a que alude el artículo 218 del Código Nacional de Procedimientos Penales.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Indique si a través de la tecnología adquirida se recabaron datos personales de particulares.*

Respuesta:

Durante el periodo que comprende la investigación realizada por ese Instituto Nacional (2015-2016) no se recabó dato personal alguno.

4. *Indique las atribuciones legales que facultan a la Procuraduría General de la República para la contratación y uso de la tecnología.*

Dentro de las facultades y atribuciones conferidas a la Procuraduría General de la República, a más de la investigación y persecución de hechos que las leyes señalan como delito, también están aquéllas en materia de seguridad nacional; por tanto, el motivo y facultades para la adquisición de la tecnología relacionada con los hechos que dieron origen a las investigaciones que ese órgano garante realiza, se fundan en:

- a. *Artículos 21, y 102, Apartado A, de la Constitución Política de los Estados Unidos Mexicanos;*
 - b. *Artículo 291 del Código Nacional de Procedimientos Penales;*
 - c. *Artículos 1, 2, 3, 4, 5 y 9, de la ley Orgánica de la Procuraduría General de la República;*
 - d. *Ley de Seguridad Nacional;*
 - e. *1, 3, 4, 10, y 12 del Reglamento de la ley Orgánica de la Procuraduría General de la República;*
 - f. *Acuerdo A/018/15 del Procurador General de la República, publicado en el Diario Oficial de la Federación el 23 de febrero de 2015, por el que el Titular de esta Institución, delegó en los servidores públicos que en dicho instrumento jurídico se indican, la facultad, entre otras, de intervenir comunicaciones privadas, conforme a lo dispuesto en el artículo 291 del Código Nacional de Procedimientos Penales.*
5. *Indicar en términos generales, cuáles son las actividades sustantivas de la Procuraduría General de la República que se realizan a partir del uso de la tecnología adquirida.*

Respuesta:

Como se mencionó, durante el periodo que comprende la investigación realizada por ese Instituto Nacional (2015-2016) no se recabó dato personal alguno.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

6. *Indicar los motivos o supuestos legales por los cuales puede hacerse uso de la tecnología adquirida que nos ocupa.*

Respuesta:

Como se mencionó, dentro de las facultades y atribuciones conferidas a la Procuraduría General de la República, a más de la investigación y persecución de hechos que las leyes señalan como delito, también están aquellas en materia de seguridad nacional; por tanto, el motivo y facultades para la adquisición de la tecnología relacionada con los hechos que dieron origen a las investigaciones que ese órgano garante realiza, se fundan en:

- a. **Artículos 21, y 102, Apartado A, de la Constitución Política de los Estados Unidos Mexicanos;**
 - b. **Artículo 291 del Código Nacional de Procedimientos Penales;**
 - c. **Artículos 1, 2, 3, 4, 5 y 9. de la Ley Orgánica de la Procuraduría General de la República;**
 - d. **Ley de Seguridad Nacional;**
 - e. **1, 3. 4. lo, y 12 del Reglamento de la Ley Orgánica de la Procuraduría General de la República;**
 - f. **Acuerdo A/018/15 del Procurador General de la República. publicado en el Diario Oficial de la Federación el 23 de febrero de 2015, por el que el Titular de esta Institución, delegó en los servidores públicos que en dicho instrumento jurídico se indican, la facultad, entre otras, de intervenir comunicaciones privadas, conforme a lo dispuesto en el artículo 291 del Código Nacional de Procedimientos Penales.**
7. *Señale si se recibió autorización judicial para el uso de la tecnología adquirida y, en su caso, remita el registro o constancia en la que consten las autorizaciones respectivas en cada caso que haya sido utilizada.*

Respuesta:

No aplica, en razón de que como se mencionó, durante el periodo que comprende la investigación realizada por ese órgano garante, no se recabó dato personal alguno.

8. *Explique en qué consiste el tratamiento de datos personales que la Procuraduría General de la República dio a partir del uso de la tecnología adquirida.*

Respuesta:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

No aplica, en razón de que como se mencionó, durante el periodo que comprende la investigación realizada por ese órgano garante, no se recabó dato personal alguno.

9. *Indique si durante los años 2014, 2015 y 2016 se recabaron datos personales a través del uso de la tecnología adquirida.*

Respuesta:

Durante el periodo que comprende la investigación realizada por ese Instituto Nacional no se recabó dato personal alguno.

10. *Indique si los datos personales recabados, en su caso, fueron integrados a un sistema de gestión de datos personales de la dependencia.*

Respuesta:

No aplica, en razón de que como se mencionó, durante el periodo que comprende la investigación realizada por ese órgano garante, no se recabó dato personal alguno.

11. *Indique, en su caso, si los datos personales recabados fueron objeto de transferencia a terceros.*

Respuesta:

No aplica, en razón de que como se mencionó, durante el periodo que comprende la investigación realizada por ese órgano garante, no se recabó dato personal alguno.

12. *Indique los medios o fuente de datos los datos personales que pueden recabarse a través del uso de la tecnología.*

Respuesta:

Esta Institución está impedida para pronunciarse al respecto, ya que aún en el caso de que en el periodo que comprende la investigación realizada por ese órgano garante (2015-2016) la tecnología adquirida no fue utilizada, la divulgación de cualquier dato relacionado con la misma comprometería la seguridad nacional en términos de lo dispuesto por los artículos 37, 42, 47 y 48 de la ley de Seguridad Nacional y la estricta reserva de la información a que alude el artículo 218 del Código Nacional de Procedimientos Penales.

13. *Proporcione la información adicional que pudiera coadyuvar con el desarrollo de la presente investigación.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Respuesta:

No se cuenta con información adicional.

[...] (sic)

a) Adjunto, la entonces Procuraduría General de la República remitió:

- Versión pública del contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V.
- Versión pública del **ANEXO TÉCNICO. ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"**, del contrato celebrado el veintinueve de octubre de dos mil catorce.

79. El veintiuno de junio de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **DGAJ/02212/2018** descrito en el **antecedente 78**.

80. Mediante el oficio número **INAI/SPDP/DGEIVSP/242/18** del seis de julio de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

Me refiero a su oficio número DGAJ/02212/2018, recibido el 21 de junio de 2018 en esta Dirección General, mediante el cual da respuesta al requerimiento formulado a través del diverso número INAI/SPDP/DGEIVSP/191/18.

Al respecto, considerando que de manera adjunta al oficio DGAJ/02212/2018, remitió la versión pública del contrato requerido y de su anexo técnico relativo a la adquisición del sistema para la realización de actividades sustantivas de esa Procuraduría denominado



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

"Pegasus"; es preciso señalar que de su análisis, se advirtió que a foja 34 y siguientes se prevé un apartado respecto a un mecanismo que se indica como "Recolección de datos".

En este sentido, es necesario que este Instituto tenga acceso a la versión íntegra del citado apartado a efecto de continuar con la investigación que se originó a partir del posible uso del software respectivo.

De esta manera, con fundamento en los artículos [...]; y a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan, me permito solicitar su atenta colaboración para que gire sus apreciables instrucciones a quien corresponda, para que dicha Procuraduría General de la República autorice y fije día y hora para que un servidor con el carácter de Titular de esta unidad administrativa, acuda a sus oficinas a consultar dicho apartado del contrato de marras, pudiendo levantar constancia de dicha actuación.

Asimismo, en relación con la cláusula sexta del referido contrato, se indica que la vigencia del mismo va del veintinueve de octubre al treinta y uno de diciembre de dos mil catorce; sin embargo, resulta necesario para esta Dirección General que ese sujeto obligado especifique la temporalidad en que la Procuraduría General de la República dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo, en razón de su licenciamiento, de acuerdo a los alcances y términos del contrato que nos ocupa.

Le agradeceré haga del conocimiento de este Instituto lo referido **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 32, 35 y 38 de la Ley Federal de Procedimiento Administrativo.

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el once de julio de dos mil dieciocho.

81. El uno de agosto de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/02621/2018** de la misma fecha, emitido y signado por la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/242/18** descrito en el **antecedente 80**, indicando lo siguiente:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

*Por lo que respecta a dicha solicitud, con fundamento en el artículo 12 fracción IX, del Reglamento de la Ley Orgánica de la Procuraduría General de la República, se le autoriza el acceso en su carácter de Titular de esa Dirección General, el día 09 de agosto de 2018, a las 11:00 horas, en las instalaciones que ocupa la **UNIDAD DE INVESTIGACIONES CIBERNÉTICAS Y OPERACIONES TECNOLÓGICAS** de la Agencia de Investigación Criminal, en el domicilio ubicado en Avenida Casa de la Moneda Número 333, Colonia Lomas de Sotelo, Delegación Miguel Hidalgo, código postal 11200, en esta Ciudad de México, siendo necesaria la confirmación previa con la licenciada Ivonne Cruz Tovar, con número de extensión 516713 y correo electrónico Ivonne.cruz@pgr.gob.mx. Por lo que respecta a la solicitud consistente en:*

"Asimismo, en relación con la cláusula sexta del referido contrato, se indica que la vigencia del mismo va del veintinueve de octubre al treinta y uno de diciembre de dos mil catorce; sin embargo, resulta necesario para esta Dirección General que ese sujeto obligado especifique la temporalidad en que la Procuraduría General de la República dio uso a la tecnología adquirida estuvo en condiciones de hacerlo, en razón de su licenciamiento, de acuerdo a los alcances y términos del contrato que nos ocupa".

Se señala que la temporalidad en que la Procuraduría General de la República estuvo en condiciones de hacerlo, lo fue la propia vigencia del contrato que nos ocupa (en la cláusula sexta se especifica la vigencia correspondiente), tal y como hace referencia en su oficio, precisando que no fue utilizada la tecnología referida.

[...]

82. El dos de agosto de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **DGAJ/02621/2018** descrito en el **antecedente 81**.

83. Mediante el oficio número **INAI/SPDP/DGEIVSP/307/18** del ocho de agosto de dos mil dieciocho, la Dirección General de Evaluación, Investigación y Verificación del Sector Público notificó a los servidores públicos de dicha dirección el acuerdo del dos de agosto de dos mil dieciocho, en el que se determinó establecer la comisión para llevar a cabo una diligencia con la finalidad de consultar el apartado **Recolección de Datos del ANEXO TÉCNICO. ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA**



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

REPÚBLICA DENOMINADO “PEGASUS”, del contrato celebrado el veintinueve de octubre de dos mil catorce.

84. El veintitrés de agosto de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibida la minuta de la diligencia celebrada el nueve de agosto de dos mil dieciocho en las instalaciones que ocupa la Agencia de Investigación Criminal de la entonces Procuraduría General de la República, ordenó su resguardo en sobre cerrado y que el análisis de su contenido se realizara al momento de resolver.

85. Mediante el oficio número **INAI/SPDP/DGEIVSP/489/18** del veinticuatro de septiembre de dos mil dieciocho, a efecto de allegarse de los elementos necesarios para resolver, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al director general de asuntos internacionales de este Instituto, lo siguiente:

[...]

Como antecedente, me refiero al oficio INAI/SE/DGAI/098/17 del tres de agosto de dos mil diecisiete, en el que informa que cotizó el costo de servicios de traducción certificada de tres documentos y posteriormente remitió dicha traducción a la entonces Dirección General de Investigación y Verificación.

Al respecto, con fundamento en los artículos [...]; a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan, me permito solicitar su atenta colaboración para que:

- *Realice la cotización de los servicios de traducción certificada del documento intitulado HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, publicado el dieciocho de septiembre de dos mil dieciocho, el cual se adjunta al presente oficio; así como, el trámite para obtener dicha traducción.*

Una vez que cuente con la traducción certificada, remitirla a la Dirección General de Evaluación, Investigación y Verificación del Sector Público.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- a) Adjunto a la solicitud se remitió el documento intitulado *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, publicado¹⁶ el dieciocho de septiembre de dos mil dieciocho, en el portal de *The Citizen Lab*.

La solicitud se notificó a la Dirección General de Asuntos Internacionales, el veinticuatro de septiembre de dos mil dieciocho.

86. Mediante el oficio número **INAI/SPDP/DGEIVSP/504/18** del veinticinco de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

Me refiero al software PEGASUS, adquirido por dicho sujeto obligado y que es objeto de investigación, en términos de lo que dispone la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En este sentido, ante la posibilidad de que al día de hoy dicho software pudiera estar en uso y deba ajustarse a los parámetros de tratamiento de datos personales que dispone la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan.

*Al respecto, si bien adquirió el software PEGASUS en dos mil catorce y de acuerdo con la cláusula sexta de dicho contrato, **la vigencia del mismo fue del veintinueve de octubre al treinta y uno de diciembre de dos mil catorce**, resulta necesario que precise lo siguiente:*

1. *Indique si ha cedido por cualquier medio la licencia de uso del software PEGASUS a algún tercero, debiendo señalar el nombre y remitir el documento que de cuenta de la referida cesión.*

¹⁶ <https://citizenlab.ca/2018/09/hidden-and-seeking-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> vínculo consultado el veintitrés de enero de dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

2. *Si del dos mil quince a julio de dos mil dieciocho, ha realizado adquisiciones diversas del software PEGASUS o de sus actualizaciones, debiendo indicar si aún cuenta con la licencia que le permita el uso de la tecnología.*
3. *En caso de que durante el periodo señalado en el punto anterior hubiere adquirido el software PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
4. *Indique si del dos mil quince a julio de dos mil dieciocho, se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
5. *Indique si cuenta con una bitácora de uso o registro del referido software, debiendo remitir, en su caso, copia certificada de la misma.*
6. *Precise las medidas de las que dispone para el tratamiento de datos personales, relacionado con el uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
7. *Manifieste lo que a derecho corresponda respecto de la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho, relacionada con las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.*

Le agradeceré haga del conocimiento de este Instituto lo referido en un término máximo de (5) cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el veintisiete de septiembre de dos mil dieciocho.

87. Mediante el oficio número **INAI/SPDP/DGEIVSP/505/18** del veinticinco de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al director general de asuntos jurídicos de la Policía Federal, lo siguiente:

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Considerando las atribuciones legales en materia de investigación de delitos y de seguridad pública que le han sido conferidas a la Policía Federal, me refiero a la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho respecto de las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.

Al respecto, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan en el expediente citado al rubro, en coadyuvancia institucional con esta autoridad investigadora, se le solicita proporcione la siguiente información:

- 1. Si del dos mil quince a julio de dos mil dieciocho, adquirió, compró, arrendó o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS.*
- 2. Precise el nombre, denominación y/o razón social de la persona física y/o moral que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instaló u operó el software.*
- 3. Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a los que puede tener acceso.*
- 4. Nombre de los servidores públicos y/o personal, perteneciente o no a la Policía Federal, autorizados para la utilización del software PEGASUS.*
- 5. Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.*
- 6. En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
- 7. Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
- 8. Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
- 9. Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

Le agradeceré haga del conocimiento de este Instituto lo referido en un término máximo de (5) cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la Policía Federal, el veintisiete de septiembre de dos mil dieciocho.

88. Mediante el oficio número **INAI/SPDP/DGEIVSP/508/18** del veinticinco de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al titular de la unidad general de asuntos jurídicos de la Secretaría de Gobernación, lo siguiente:

[...]

Considerando las atribuciones legales que en materia de conducción de política interior le han sido conferidas a la Secretaría de Gobernación, me refiero a la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho respecto de las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.

Al respecto, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan en el expediente citado al rubro, en coadyuvancia institucional con esta autoridad investigadora, se le solicita proporcione la siguiente información:

- 1. Si del **dos mil quince a julio de dos mil dieciocho** la Secretaría de Gobernación adquirió, compró, arrendó o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS, para uso de los órganos desconcentrados que tiene adscritos.*
- 2. De ser el caso, resulta indispensable que precise el nombre, denominación y/o razón social de la persona física y/o moral de la que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instaló u operó el software.*
- 3. Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a los que puede tener acceso.*
- 4. Nombre de los servidores públicos y/o personal, perteneciente o no a la Secretaría de Gobernación, autorizados para la utilización del software PEGASUS.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. *Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.*
6. *En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
7. *Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
8. *Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
9. *Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

*Le agradeceré haga del conocimiento de este Instituto lo referido **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.*

[...]

El requerimiento se notificó a la Unidad General de Asuntos Jurídicos de la Secretaría de Gobernación, el dos de octubre de dos mil dieciocho.

89. Mediante el oficio número **INAI/SPDP/DGEIVSP/506/18** del veintisiete de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, lo siguiente:

[...]

Tomando como antecedente el oficio número J-CONS-V-22079 del uno de septiembre de dos mil diecisiete, emitido por el jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional en el que manifestó la inexistencia de la información solicitada respecto al uso del software PEGASUS, del periodo comprendido del dos mil quince al dos mil dieciséis, en relación directa y considerando las atribuciones legales que en materia de seguridad interior le han sido conferidas a la Secretaría de la Defensa Nacional, me refiero a la publicación de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

The Citizen Lab del dieciocho de septiembre de dos mil dieciocho respecto de las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.

Al respecto, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan en el expediente citado al rubro, en coadyuvancia institucional con esta autoridad investigadora, se le solicita proporcione la siguiente información:

- 1. Si del **dos mil diecisiete a julio de dos mil dieciocho** la Secretaría de la Defensa Nacional adquirió, compró, arrendó o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS.*
- 2. De ser el caso, resulta indispensable que precise el nombre, denominación y/o razón social de la persona física y/o moral de la que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instaló u operó el software.*
- 3. Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a los que puede tener acceso.*
- 4. Nombre de los servidores públicos y/o personal, perteneciente o no a la Secretaría de la Defensa Nacional, autorizados para la utilización del software PEGASUS.*
- 5. Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.*
- 6. En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
- 7. Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
- 8. Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
- 9. Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

*Le agradeceré haga del conocimiento de este Instituto lo referido **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

El requerimiento se notificó a la Unidad de Asuntos Jurídicos de la Secretaría de la Defensa Nacional, el dos de octubre de dos mil dieciocho.

90. Mediante el oficio número **INAI/SPDP/DGEIVSP/507/18** del veintisiete de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al titular del área jurídica del Centro de Investigación y Seguridad Nacional, lo siguiente:

[...]

Tomando como antecedente el oficio número SG/AJ/009/18 del diecisiete de enero de dos mil dieciocho, emitido por el titular del área jurídica del Centro de Investigación y Seguridad Nacional en el que manifestó la inexistencia de la información solicitada respecto al uso del software PEGASUS, del periodo comprendido del dos mil quince al dos mil dieciséis, en relación directa y considerando las atribuciones legales en materia de inteligencia como parte del sistema de seguridad nacional que le han sido conferidas al Centro de Investigación y Seguridad Nacional, me refiero a la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho respecto de las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.

Al respecto, con fundamento en los [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan en el expediente citado al rubro, en coadyuvancia institucional con esta autoridad investigadora, se le solicita proporcione la siguiente información:

1. *Si del dos mil diecisiete a julio de dos mil dieciocho el Centro de Investigación y Seguridad Nacional adquirió, compró, arrendó o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS.*
2. *De ser el caso, resulta indispensable que precise el nombre, denominación y/o razón social de la persona física y/o moral de la que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instaló u operó el software.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. *Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a los que puede tener acceso.*
4. *Nombre de los servidores públicos y/o personal, perteneciente o no al Centro de Investigación y Seguridad Nacional, autorizados para la utilización del software PEGASUS.*
5. *Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.*
6. *En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
7. *Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
8. *Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
9. *Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

*Le agradeceré haga del conocimiento de este Instituto lo referido **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.*

[..]

El requerimiento se notificó al Área Jurídica del Centro de Investigación y Seguridad Nacional, el veintiocho de septiembre de dos mil dieciocho.

91. Mediante el oficio número **INAI/SPDP/DGEIVSP/509/18** del veintisiete de septiembre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al jefe de la unidad jurídica de la Secretaría de Marina, lo siguiente:

[..]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Considerando las atribuciones legales que en materia de defensa exterior y seguridad interior le han sido conferidas a la Secretaría de Marina, me refiero a la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho respecto de las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.

Al respecto, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se investigan en el expediente citado al rubro, en coadyuvancia institucional con esta autoridad investigadora, se le solicita proporcione la siguiente información:

- 1. Si del dos mil quince a julio de dos mil dieciocho la Secretaría de Marina adquirió, compró, arrendó o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS.*
- 2. De ser el caso, resulta indispensable que precise el nombre, denominación y/o razón social de la persona física y/o moral de la que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instaló u operó el software.*
- 3. Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a los que puede tener acceso.*
- 4. Nombre de los servidores públicos y/o personal, perteneciente o no a la Secretaría de Marina, autorizados para la utilización del software PEGASUS.*
- 5. Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.*
- 6. En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*
- 7. Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*
- 8. Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*
- 9. Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

Le agradeceré haga del conocimiento de este Instituto lo referido en un término máximo de (5) cinco días hábiles, contados a partir de que surta efectos la notificación del presente, de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

conformidad con los artículos 195, fracción I y 197 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

[...]

El requerimiento se notificó a la Unidad Jurídica de la Secretaría de Marina, el uno de octubre de dos mil dieciocho.

92. El veintisiete de septiembre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/SE/DGAI/152/18** de la misma fecha, emitido y signado por el director general de asuntos internacionales de este Instituto, mediante el cual remitió información respecto a la atención brindada a la solicitud formulada a través del oficio **INAI/SPDP/DGEIVSP/489/18** descrita en el **antecedente 85**.

93. El tres de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **PF/DGAJ/DGA/1379/2018** de la misma fecha, emitido y signado por el director general adjunto de la Dirección General de Asuntos Jurídicos de la Policía Federal, mediante el cual en relación con el oficio **INAI/SPDP/DGEIVSP/505/18** descrito en el **antecedente 87**, precisó lo siguiente:

[...]

Por instrucciones superiores, me refiero al oficio INAI/SPDP/DGEIVSP/505/18 de fecha 25 de septiembre de 2018, recibido el 27 de septiembre del presente año, por el que solicita diversa información relativa al software PEGASUS, con número de expediente INAI.3S.08.03-003/2017.

Al respecto, con fundamento en lo dispuesto por los artículos 21 párrafo noveno y 123 apartado B, fracción XIII de la Constitución Política de los Estados Unidos Mexicanos; 1 y 3 de la Ley de la Policía Federal; 5 fracción VII, inciso 1), 9 fracción XX, 44 fracciones I, IV y XXVIII, del Reglamento de la Ley de la Policía Federal; 146 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 32 de la Ley Federal de Procedimiento Administrativo de aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, solicito a usted con todo respeto, se conceda a esta Dirección General de Asuntos Jurídicos de la Policía Federal, una prórroga de 5 días



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

hábiles más, a efecto de conjuntar a efecto de conjuntar la totalidad de la información requerida por esa autoridad.

[...]

94. El cuatro de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **INAI/SE/DGAI/158/18** de la misma fecha, emitido y signado por el director general de asuntos internacionales de este Instituto, mediante el cual remitió la atención brindada a la solicitud formulada a través del oficio **INAI/SPDP/DGEIVSP/489/18** descrita en el **antecedente 85**, indicando lo siguiente:

[...]

En seguimiento al oficio INAI/SE/DGAI/152/18, mediante el cual se notificó la fecha de entrega de la traducción solicitada por la Unidad Administrativa a su digno cargo, mediante oficio INAI/SPDP/DGEIVSP/489/18, por medio del presente le hago entrega de la versión impresa de dicha traducción certificada.

[...]

a) Adjunto se remitió la traducción del documento intitulado *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, publicado¹⁷ el dieciocho de septiembre de dos mil dieciocho, en el portal de *The Citizen Lab*.

95. El cuatro de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **INAI/SE/DGAI/158/18** descrito en el **antecedente 94** y el documento adjunto.

96. El cuatro de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/03482/2018** de la misma fecha, emitido y signado por la directora general de

¹⁷ <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> vínculo consultado el veintitrés de enero de dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/504/18** descrito en el **antecedente 86**, indicando lo siguiente:

[...]

*Con fundamento en los artículos 7, 10, fracción VI y 32 de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Directora General de Asuntos Jurídicos, en representación jurídica de la o el Titular de la Procuraduría General de la República, me refiero a su diverso **INAI/SPDP/DGEIVSP/504/18** de 25 de septiembre del año en curso, relativo al expediente **INAI.3S.08.03-003/2017** por el en relación con la adquisición del software PEGASUS, solicita se realicen diversas precisiones respecto del siguiente cuestionario:*

1. *Indique si ha cedido por cualquier medio la licencia del uso del software PEGASUS a algún tercero, debiendo señalar el nombre y remitir el documento de cuenta de la referida cesión.*

Respuesta No.

2. *Si del **dos mil quince a julio de dos mil dieciocho**, ha realizado adquisiciones diversas del software PEGASUS o de sus actualizaciones, debiendo indicar si aún cuenta con la licencia que le permita el uso de la tecnología.*

Respuesta: *No se ha realizado adquisición diversa, ni actualización alguna del software mencionado; siendo oportuno reiterar que la vigencia del contrato de adquisición de la tecnología mencionada lo fue del 29 de octubre al 31 de diciembre de 2014.*

3. *En caso de que durante el periodo señalado en el punto anterior hubiere adquirido el software PEGASUS, es necesario precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*

Respuesta: *No aplica, en razón de que la interrogante anterior se respondió en sentido negativo.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

4. *Indique si del dos mil quince a julio de dos mil dieciocho, se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*

Respuesta: No se recabaron datos personales a través del uso de la tecnología adquirida.

5. *Indique si cuenta con la bitácora de uso o registro del referido software, debiendo remitir, en su caso, copia certificada de la misma.*

Respuesta: No se cuenta.

6. *Precise las medidas de las que dispone para el tratamiento de datos personales, relacionado con el uso de dicho software en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

Respuesta: No aplica realizar manifestación alguna, en razón de las respuestas anteriormente emitidas a las interrogantes marcadas con los números 2, 3, 4 y 5.

7. *Manifieste lo que a su derecho corresponda respecto de la publicación de The Citizen Lab del dieciocho de septiembre de dos mil dieciocho, relacionada con las operaciones del spyware PEGASUS de la compañía NSO Group, a julio de dos mil dieciocho y la existencia de tres operadores que podrían continuar activos en México.*

Respuesta: Esta autoridad no emite manifestación alguna respecto de la publicación The Citizen Lab del dieciocho de septiembre de dos mil dieciocho, toda vez que es una nota periodística.

[...]

97. El cuatro de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **DGAJ/03482/2018** descrito en el **antecedente 96**.

98. El cinco de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **PF/DGAJ/DGA/1379/2018 (antecedente 93)** y otorgó a la Dirección General de Asuntos Jurídicos de la Policía Federal una prórroga para dar respuesta al requerimiento formulado.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

99. El cinco de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público emitió el oficio **INAI/SPDP/DGEIVSP/532/2018** a través del cual notificó al director general de asuntos jurídicos de la Policía Federal, el acuerdo descrito en el **antecedente 98**.

100. El cinco de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **SG/AJ/318/18** de la misma fecha, emitido y signado por el titular del área jurídica del Centro de Investigación y Seguridad Nacional, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/507/18** descrito en el **antecedente 90**, indicando lo siguiente:

[...]

En alcance a mi diverso oficio SG/AJ/009/18 y en atención a su requerimiento INAI/SPDP/DGEIVSP/507/18, en el cual hace referencia a la publicación en The Citizen Lab el 18 de septiembre de 2018, relativa a las operaciones del spyware PEGASUS de la compañía NSO Group, y la existencia de tres operadores que podrían continuar activos en México, motivo por el cual solicita se proporcione cierta información a fin de que dicha Dirección General cuente con los elementos necesarios para resolver lo que en derecho corresponda, requiriendo lo siguiente:

[...]

*Sobre el particular, y en atención a su petición, se manifiesta que se llevó a cabo por las áreas competentes del Centro una búsqueda exhaustiva de la información, manifestando mediante tarjetas número UAFDH/107/18 y SG/04/25/18, que no se cuenta con documentos relacionados con el presente requerimiento, por lo que se declara la **INEXISTENCIA** de la información solicitada.*

Asimismo, se precisa que no es posible indicar los nombres de las unidades administrativas a las cuales se turnó la solicitud y declararon la inexistencia, derivado de la reserva de estructura y directorio del CISEN.

Aunado a lo anterior, es importante señalar que de la lectura de la publicación en The Citizen Lab, en ningún momento se hace referencia específica al Centro de Investigación y Seguridad Nacional (CISEN), ya que la mención se formula de manera genérica como México, el cual



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

está integrado por una multiplicidad de dependencias y entidades en los tres niveles de gobierno (federal, estatal y municipal).

De igual forma, es importante recordar que las notas periodísticas solo reflejan el punto de vista de su autor y no hacen prueba plena.

[...]

En consecuencia, de la lectura de las tesis antes señaladas, se puede concluir que una nota periodística carece de valor probatorio por sí misma para acreditar los hechos a que se contrae, debido a que es producto de la investigación e interpretación personal de su autor, y en ese sentido, al no reunir las características de un documento público, lo consignado en ella no debe tenerse como un hecho verídico, por lo que no puede constituir un medio de convicción.

[...]

101. El ocho de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **SG/AJ/318/18** descrito en el **antecedente 100**.

102. El ocho de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **J-CONS-V-35525** de la misma fecha, emitido y signado por el jefe de la unidad de asuntos jurídicos de la Secretaría de la Defensa Nacional, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/506/18** descrito en el **antecedente 89**, indicando lo siguiente:

[...]

En relación con su oficio No. INAI/SPDP/DGEIVSP/506/18 de fecha 27 Sep. 2018, por el que requiere a esta Unidad de Asuntos Jurídicos, información relacionada con la investigación que realiza dentro del expediente INAI.3S.08.03-003/2017, al respecto, la Dirección General de Transmisiones dice a esta Unidad de Asuntos Jurídicos lo siguiente:

En esta Secretaría de la Defensa Nacional no se localizó información respecto a que ACTUALMENTE se haya recabado, obtenido, transmitido, manejado o se haya dado algún tratamiento a datos personales que se hayan obtenido a través del software "PEGASUS" del



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

año 2017 a julio de 2018, periodo en el cual no se ha adquirido, arrendado o poseído, el software de referencia o alguno con funcionamiento similar.

En consecuencia, resulta procedente dar respuesta a sus cuestionamientos, de la a continuación se indica:

1. Si del dos mil diecisiete a julio de dos mil dieciocho la Secretaría de la Defensa Nacional adquirió, compro, arrendo o se encuentra en posesión bajo cualquier figura jurídica del software PEGASUS.

No se localizó información de que del año 2017 a la fecha esta secretaría haya obtenido por alguna de las formas a que se refiere la pregunta o haya tenido, o tenga en posesión del software "PEGASUS" que refiere.

2. De ser el caso, resulta indispensable que precise el nombre, denominación y/o razón social de la persona física y/o moral de la que haya adquirido el software PEGASUS, debiendo proporcionar copia certificada del instrumento por el que adquirió, instalo u opero el software.

En relación a la respuesta a la pregunta número uno, no existe información de ninguna persona física y/o moral de quien haya adquirido el software "PEGASUS", por lo que se carece de la documentación que solicita.

3. Indique de forma detallada las acciones que lleva a cabo dicho sujeto obligado con el software PEGASUS, describiendo puntualmente la información y los datos personales a lo que puede tener acceso.

En atención a la respuesta dada a la pregunta número uno, no se localizó información que indique de forma detallada las acciones que pueden llevarse a cabo con el software "PEGASUS" y/o cual es la información y datos personales a los que se puede tener acceso con el mismo.

4. Nombre de los servidores públicos y/o personal perteneciente o no a la Secretaría de la Defensa Nacional, autorizados para la utilización del software PEGASUS.

En atención a la respuesta dada a la pregunta número uno, no existen servidores públicos y/o personal, perteneciente a la Secretaría de la Defensa Nacional, autorizado para la utilización del software "PEGASUS".

5. Describa los procedimientos técnicos, informáticos y legales, seguidos para la adquisición, instalación, operación y utilización del software PEGASUS.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En relación a la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento.

6. *En caso de que durante el periodo señalado hubiere adquirido el sistema PEGASUS, es necesario que se precise la temporalidad en que dio uso a la tecnología adquirida o estuvo en condiciones de hacerlo en razón de su licenciamiento.*

En relación a la respuesta a la pregunta número uno, no se localizó información sobre los procedimientos señalados en la presente pregunta.

7. *Indique si se recabaron datos personales a través del uso de la tecnología adquirida, cuáles fueron los datos personales recabados, si fueron integrados a un sistema de gestión de datos personales o si fueron objeto de transferencia a terceros.*

En atención a la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento, ya que como se indica, en el periodo que se investiga y hasta la fecha esta Secretaría no cuenta con el software citado.

8. *Precise las medidas de las que dispone para el posible uso de dicho software en términos de lo dispuesto en la Ley General de protección de Datos Personales en Posesión de Sujetos Obligados.*

En relación a la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento.

9. *Manifieste lo que a su derecho convenga y aporte la demás información y documentación relacionada con el presente requerimiento, en coadyuvancia institucional.*

En relación con la respuesta a la pregunta número uno, no se localizó información que permita atender su requerimiento.

Por lo anterior se solicita:

ÚNICO: Que esa Dirección General a su digno cargo, archive el presente asunto sin ninguna responsabilidad para esta Secretaría de la Defensa Nacional, ya que no se localizó información respecto a los hechos que se investigan en el periodo que solicita ... "

Es necesario puntualizar que, en este Instituto Armado, no se localizó información respecto a que ACTUALMENTE se haya recabado, obtenido, transmitido, manejado o se haya dado algún tratamiento a datos personales que se hayan obtenido a través del citado software "PEGASUS" en el periodo comprendido del ario 2017 a julio de 2018, como refiere, máxime



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

que, hasta la fecha, no se adquirió, arrendo o tuvo en posesión, el software de referencia, y, por lo tanto, no se cuenta con esa herramienta informática.

En el requerimiento de referencia, no se señala cuáles fueron los datos personales desprotegidos, los cuales señala que supuestamente fueron obtenidos por el uso del software en el periodo de 2017 a julio de 2018, y que pueden usarse actualmente por esta Secretaría de Estado; además de que no obra una denuncia o medios de prueba específicos ofrecidos por quien se haya considerado afectado; en consecuencia, normativamente no existe materia de controversia o investigación, lo que con lleva a resolver la conclusión del expediente INAI. 3S.08.03-003/2017, sin ninguna responsabilidad por cuanto hace a esta Secretaría de la Defensa Nacional.

Por lo que, esa Dirección General pretende ampliar su investigación dentro de un expediente que se inició con sustento en un marco normativo cuyo inicio de vigencia es posterior a los hechos que se pretendían investigar, lo cual se estima que jurídicamente es improcedente.

Asimismo, esa Dirección General pretende sustentar su petición bajo el argumento que "...en relación directa y considerando las atribuciones legales que en materia de seguridad interior le han sido conferidas a la Secretaría de la Defensa Nacional..."; sin que especifique cuáles son esas atribuciones conferidas a este Instituto Armado, aunado a que no sería la el precepto legal que en materia de seguridad interior de sustento jurídico a su petición o en su caso, establezca el ordenamiento legal que supuestamente esta Secretaría de Estado está trasgrediendo en perjuicio de persona alguna en materia de protección de datos personales en posesión de sujeto obligado.

Aunado a que los hechos por los que requiere información, no se adecuan a ninguna de las hipótesis sancionables por ese INAI, señaladas en el artículo 186 de la Ley Federal de Transparencia y Acceso a la Información Pública; así como los numerales 5 y 163 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por lo que se solicita con sustento en los argumentos vertidos en el presente escrito, se archive sin responsabilidad para esta Secretaría de la Defensa Nacional.

[...]

103. El nueve de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **J-CONS-V-35525** descrito en el **antecedente 102**.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

104. El nueve de octubre de dos mil dieciocho, tras una prórroga, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **PF/DGAJ/DGA/1411/2018** del ocho de octubre de dos mil dieciocho, emitido y signado por el director general adjunto de la Dirección General de Asuntos Jurídicos de la Policía Federal, mediante el cual, tras la prórroga concedida, remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/505/18** descrito en el **antecedente 87**, indicando lo siguiente:

[...]

*Por instrucciones superiores, me refiero a los oficios **INAI/SPDP/DGEIVSP/505/18** y **INAI/SPDP/DGEIVSP/532/18**, el primero de fecha 25 de septiembre de 2018, recibido el 27 de septiembre del presente año, por el que requiere diversa información relativa al software "Pegasus"; el segundo mediante el cual concede prórroga, en relación con el expediente de número **INAI.3S.08.03-003/2017**.*

Al respecto, con fundamento en lo dispuesto por los artículos 21 párrafo noveno y 123 apartado B, fracción XIII de la Constitución Política de los Estados Unidos Mexicanos; 1 y 3 de la Ley de la Policía Federal; 5 fracción VII, inciso 1), 9 fracción XX, 18 fracción XII, 44 fracciones I, IV y XXVIII y 45, del Reglamento de la Ley de la Policía Federal; 146 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 204 fracción I, incisos a) y b), de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en cumplimiento del plazo establecido, se remite la información proporcionada por las siguientes áreas administrativas:

A. Texto de la respuesta de la Dirección General de Enlace de la Policía Federal, oficio PF/OCG/DGE/4891/2018:

Sobre el particular y en el ámbito de colaboración, me permito hacer de su conocimiento que después de realizar una búsqueda de las solicitudes de información recibidas en esta Unidad Administrativa de la Policía Federal correspondientes a los ejercicios fiscales 2016 y 2017 se localizaron las solicitudes de información identificadas con los números de folio que a continuación se detallan en las cuales se declaró la inexistencia de la información:

NÚMERO DE SOLICITUD	ASUNTO	MODALIDAD DE RESPUESTA
0413100084516	Se solicita La siguiente información disponible relacionada con la adquisición de cualquier software o herramienta tecnológica desarrollada por la firma NSO Group, o alguna de sus filiales y/o	INEXISTENCIA



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

	<p>subsidiarias. La información solicitada debe incluir, mas no limitarse a: A) Gasto en la adquisición y/o uso de cualquier software y/o herramienta tecnológica desarrollada por la firma mencionada anteriormente (NSO Group). b) Detalles de los contratos (fecha, duración, monto, objetivos y razones de la contratación, forma de adjudicación del contrato -directa o licitación) celebrados con NSO Group y/o proveedores de cualquier producto y/o servicio de dicha empresa. Se solicita incluir una versión pública de dichos contratos. e) Resultados y/o la versión pública de los reportes relacionados con el uso del software y/o herramientas tecnológicas desarrolladas por la firma NSO Group. D) funcionarios públicos y/o contratistas involucrados, en la contratación, administración y/o uso de cualquier software o herramienta tecnológica desarrollada por la firma NSO Group, o a la una de sus filiales y/o subsidiarias.</p>	
0413100089116	<p>Informe si de 2012 a la fecha esta dependencia suscribió algún convenio, contrato o documento jurídico de similar indole, con la empresa NSO Group para la adquisición de servicios de inteligencia y monitoreo de telefonía celular, entre otros, y en su caso provea versión pública de los documentos donde se detalles los servicios contratados. No se omite señalar que la adquisición de dichos servicios por el Estado mexicano fue referida por el periódico norteamericano The New York Times, en la nota que puede consultarse en el siguiente vinculo: http://www.nytimes.com/2016/09103/technology/inso-group-how-spy-techfirms-let-governments-see-everything-on-a-smartphone.html?r=0.</p>	INEXISTENCIA
0413100059317	<p>Se solicita versión pública de cualquier documento relacionado con la contratación de cualquier software, licencia o herramienta tecnológica desarrollada por la firma NSO Group o por alguna de sus filiales y/o subsidiarias incluyendo versión pública de los contratos correspondientes. Gracias.</p>	INEXISTENCIA
0413100068917	<p>Solicito copia simple y en su caso versión pública de todos los contratos celebrados por esas dependencias en su calidad de área requirente con las empresas denominadas Balam Seguridad Privada SA de CV, o Grupo Tech Bull, o Elbit, Orion Trust, Hacking Team, así como de cualquier otra empresa que hubiese proporcionado el servicio o el equipo denominado Pegasus, de supuesta fabricación israelí, y si es en efecto fabricado por parte de la empresa NSO Group. copia simple de cualquier contrato celebrado con cualquier empresa, cuyo fin haya sido proporcionar a alguna de esas dependencias equipo o programas de cómputo destinados a la interceptación de comunicaciones o señales de radio. Copia simple de la justificación por virtud de la cual el comité de adquisiciones o quien hubiese decidido, en cada una de esas dependencias, optó por contratar a esa empresa y no a cualquier otra que hubiera podido proporcionar el servicio. Copia simple del oficio donde el titular de esas dependencias ordenó al oficial mayor o equivalente de las mismas, la adquisición de ese tipo de equipo y Productos.</p>	INEXISTENCIA
0413100069517	<p>Hola Solicito saber si esta dependencia federal utiliza o ha utilizado en los últimos 10 años el software Pegasus de la empresa NSO Group. De</p>	INEXISTENCIA



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

	<i>ser afirmativo ¿Desde qué año se utiliza el software Pegasus, ¿cuál fue el costo de compra del software, así como cuánto cuesta mantener sus actualizaciones? Además, ¿para qué adquirieron el software Pegasus, ¿cuál fue la justificación para la compra y para qué se utiliza o para qué se utilizó? Por otro lado, 041310006957 quisiera saber si esta dependencia utiliza otro tipo de programas o software con el que mantenga prácticas de espionaje a miembros del crimen organizado o delincuentes. De ser afirmativa la respuesta ¿cuál es el nombre del software y a que empresa se le compró desde que año se utiliza ese software, ¿cuál fue el costo de compra del software, así como cuánto cuesta mantener sus actualizaciones? Además ¿para que adquirieron ese software, ¿cuál fue la justificación para la compra y para que se utiliza o para que se utilizó? .</i>	
0413100070517	<i>Se solicita versión pública de cualquier documento del año 2000 al 2017 relacionado con la contratación de cualquier software, licencia o herramienta tecnológica desarrollada por la firma NSO Group o por alguna de sus filiales y/o subsidiarias incluyendo versión pública de los contratos correspondientes Gracias.</i>	INEXISTENCIA

Lo anterior, de conformidad con lo previsto en los artículos 61 de la Ley Federal de Transparencia y Acceso a la Información Pública y 45 del Reglamento de la Ley de la Policía Federal

Se anexa copia simple del oficio PF/OCG/OGE/4891/2018, así como las copias certificadas de las solicitudes de información mencionadas en el cuadro que antecede.

B. Texto de la respuesta de la Secretaría General. oficio PF/SG/EJ/4301/2018;

Respetuosamente hago referencia al oficio PF/DGAJ/779/2018, mediante el cual informé que en el similar INAI/SPDP/DGEIVSP/505/18, el Director General de Evaluación, Investigación y Verificación del Sector Público del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), requirió datos relacionados a los hechos que se investigan en el expediente INAI.3S.08.03-003/2017, sobre la publicación de The Citizen Lab del 18 de septiembre de 2018, referente a las operaciones del spyware.

Se anexa copia simple del oficio PF/SG/EJ/4301/2018, así como las copias certificadas de los oficios números PF/SG/CSG/ET/0648/2018 y PF/SG/CST/DGI/676/2018; así como la certificación emitida por la Coordinación de Servicios Generales de los oficios PF/SG/CSG/DGRF/3782/2018, PF/SG/CSG/DGRM/DA/0990/2018 y PF/SG/CSG/DGRM/6033/2018 y de las atentas notas números 80, 142, 272 y S/N emitidas por las Direcciones adscritas a la DGRF.

Con lo anterior, se solicita se dé por atendido su requerimiento de información con el numeral 1, en el entendido de que no cuenta se cuenta con antecedentes de adquisición, compra,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

arrendamiento o posesión del software PEGASUS, de la compañía NSO Group y la existencia de los operadores que se señalan. Por lo que en concordancia con el principio general del derecho "Accesorium sequitur principale" (lo accesorio sigue la suerte de lo principal), al no contar con registro de instrumento jurídico relacionado con el software PEGASUS, no se cuenta con el resto de la información solicitada en su escrito de requerimiento de información, según los numerales 2 al 9.

[...]

- a) Adjunto a la atención al requerimiento de información, la Policía Federal remitió los oficios por los que sus unidades administrativas dieron respuesta, los cuales se describen en el oficio **PF/DGAJ/DGA/1411/2018 (antecedente 104)**.

105. El nueve de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **PF/DGAJ/DGA/1411/2018** descrito en el **antecedente 104** y los documentos adjuntos.

106. El diez de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **UGAJ/DGCCC/2534/2018** del ocho del mismo mes y año, emitido y signado por el director general de los consultivo y de contratos y convenios de la Secretaría de Gobernación, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/508/18** descrito en el **antecedente 88**, indicando lo siguiente:

[...]

Me refiero a su oficio No. INAI/SPDP/DGEIVSP/508/18, de fecha 25 de septiembre de 2018, recibido el dos de octubre del año en curso, mediante el cual refiere a la publicación de The Citizen Lab del 18 de septiembre de 2018, respecto de las operaciones del spyware PEGASUS y solicita sea proporcionada información relacionada al software PEGASUS, otorgando para tales efectos un término máximo de cinco días hábiles.

Al respecto y con fundamento en los artículos 2 inciso B fracción XV, 9 fracción III y VII y 64 fracciones VI, VII y XXII del Reglamento Interior de la Secretaría de Gobernación, se da respuesta al requerimiento en los siguientes términos:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

- *El artículo 18 de la Ley de Seguridad Nacional señala que el Centro de Investigación y Seguridad Nacional, es un órgano administrativo desconcentrado de la Secretaría de Gobernación, con autonomía, técnica, operativa y de gasto.*
- *El artículo 8 fracción XXIX de la Ley de la Policía Federal señala que la misma tiene como atribución solicitar por escrito ante el juez de control, en términos del capítulo XI de la dicha Ley, la autorización para la **intervención de comunicaciones** privadas para la investigación de los delitos.*
- *Conforme al artículo 23 de la Ley General de Transparencia y Acceso a la Información Pública y 1° de la Ley Federal de Transparencia y Acceso a la Información Pública, tanto Policía Federal como el Centro de Investigación y Seguridad Nacional son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder. Además, es importante resaltar que ambos cuentan con su respectiva Unidad de Transparencia.*

Lo anterior deja claro que la Secretaría de Gobernación no tiene atribuciones para conocer en materia de intervención de comunicaciones, por lo que, al carecer de competencia en dicho tema, se sugiere dirigir su petición a los órganos administrativos desconcentrados antes señalados.

Así mismo, es importante señalar que dicha incompetencia ya fue materia de la resolución del propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, de fecha 13 de septiembre de 2017, dictada en el Recurso de Revisión RRA 4744/17 del folio de la solicitud 0000400189617.

Por lo antes expuesto y fundado, solicito tener por desahogado en tiempo y forma el requerimiento de mérito.

[...]

107. El diez de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **UGAJ/DGCC/2534/2018** descrito en el **antecedente 106**.

108. Mediante el oficio número **INAI/SPDP/DGEIVSP/549/18** del doce de octubre de dos mil dieciocho, con el objeto de estar en condiciones de esclarecer los hechos motivo de la investigación, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al jefe de la unidad jurídica de la Secretaría de Marina, desahogar



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

el requerimiento de información que se le realizó a través del oficio **INAI/SPDP/DGEIVSP/509/18** descrito en el **antecedente 91**.

109. El dieciséis de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **16570/AP/18** de la misma fecha, emitido y signado por el jefe de la unidad jurídica de la Secretaría de Marina, mediante el cual remitió parte del desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/509/18** descrito en el **antecedente 91**, relacionado con el oficio **INAI/SPDP/DGEIVSP/549/18** mencionado en el **antecedente 108**, indicando lo siguiente:

[...]

Esta unidad jurídica en atención a su oficio INAI/SPDP/DGEIVSP/549/18 del 12 actual, hace de su conocimiento, que se solicitó a las diferentes áreas y unidades de este instituto Armado, la información solicitada en su requerimiento de mérito, habiéndose recibido respuesta por parte de la Dirección General Adjunta de Adquisiciones de esta Secretaría, en términos de lo que a continuación se transcribe:

"...Esta Unidad Administrativa, en el ámbito de su competencia, realizó la búsqueda en los sistemas y expedientes que obran en el archivo de la expresada, sin que se localizara información o documentación alguna de contrataciones implementadas al amparo de la Ley de Adquisiciones, arrendamientos y Servicios del Sector Público con la Compañía NSO Group para la compra de bienes o prestación de servicio alguno..."

No omitiendo participarle que dicha información, se solicitó a cuatro áreas más, las cuales están pendientes de pronunciarse, por lo que, al recibirse respuesta de las mismas, se le proporcionarán los datos que se deriven.

*Lo anterior para los efectos legales a que haya lugar dentro del expediente **INAI.3S.08.03-003/2017**.*

[...]

110. El veinticuatro de octubre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **16816/AP/18** del diecinueve del mismo mes y año, emitido y signado por el jefe de la unidad jurídica de la Secretaría de Marina, mediante el cual remitió la segunda parte del



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/509/18** descrito en el **antecedente 91**, relacionado con el oficio **INAI/SPDP/DGEIVSP/549/18** mencionado en el **antecedente 108**, indicando lo siguiente:

[..]

Esta Unidad Jurídica, en alcance a mi oficio 16570/AP/18 del 16 del actual, hace de su conocimiento que las Jefaturas de la Unidad de Inteligencia Naval y de la Sección Segunda del Estado Mayor General de la Armada, así como la Dirección General Adjunta de Comunicaciones e Informática, comunicaron a esta Unidad administrativa que una vez que realizaron una búsqueda minuciosa en sus expedientes y bases de datos, no contando con la información solicitada.

*Lo anterior para los efectos legales a que haya lugar dentro del expediente **INAI.3S.08.03-003/2017**.*

[..]

111. El veinticuatro de octubre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibidos los oficios **16570/AP/18** descrito en el **antecedente 109** y el **16816/AP/18** descrito en el **antecedente 110**.

112. El veintitrés de noviembre de dos mil dieciocho, en cumplimiento a lo dispuesto en el artículo 149 segundo párrafo de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por tratarse de una instancia de seguridad pública y nacional, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó por unanimidad el acuerdo número ACT-PUB/23/11/2018.08, mediante el cual **autorizó el inicio de una verificación** a la entonces Procuraduría General de la República, hoy Fiscalía General de la República, en el ámbito de aplicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con motivo de los elementos derivados de la sustanciación del procedimiento de investigación previa de oficio, identificada con el número de expediente **INAI.3S.08.03-003/2017**.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

113. El veintitrés de noviembre de dos mil dieciocho, se emitió el acuerdo de inicio de procedimiento de verificación, en el que se determinó que:

- a) No se cuentan con elementos suficientes para acreditar actos u omisiones; o bien, alguna posible vinculación por parte de la Secretaría de Gobernación, de la Secretaría de Marina, de la Secretaría de la Defensa Nacional, de la Policía Federal o del Centro de Investigación y Seguridad Nacional, que presuntamente constituyan un incumplimiento a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en relación con los hechos y circunstancias investigadas.

El acuerdo en comento se notificó a la Policía Federal el veintiséis de noviembre de dos mil dieciocho, a la Secretaría de la Defensa Nacional, a la Secretaría de Marina y al Centro de Investigación y Seguridad Nacional el veintisiete de noviembre de dos mil dieciocho, a la Secretaría de Gobernación el veintiocho de noviembre de dos mil dieciocho y a la Red en Defensa de los Derechos Digitales A.C. el treinta de noviembre de dos mil dieciocho.

- b) **Iniciar a la entonces Procuraduría General de la República, hoy Fiscalía General de la República, el procedimiento de verificación respectivo**, bajo el número de expediente **INAI.3S.07.01-007/2018**¹⁸; así como, comisionar al personal adscrito a la Dirección General de Evaluación, Investigación y Verificación del Sector Público para sustanciar el procedimiento de verificación, de conformidad con lo dispuesto en el artículo 149 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el ámbito de las atribuciones que le confiere el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

El acuerdo de inicio de procedimiento de verificación se notificó a la entonces Procuraduría General de la República el veintitrés de noviembre de dos mil dieciocho a través del oficio número **INAI/SPDP/DGEIVSP/623/18** de la misma

¹⁸ El expediente número **INAI.3S.07.01-007/2018** derivó del procedimiento de investigación previa **INAI.3S.08.03-003/2017**.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

fecha, concediéndole un plazo de cinco días hábiles para aportar pruebas y manifestar lo que a su derecho conviniera.

114. El treinta de noviembre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/04002/2018** de la misma fecha, emitido y signado por la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual solicitó en relación con el oficio **INAI/SPDP/DGEIVSP/623/18** del veintitrés de noviembre de dos mil dieciocho y con lo señalado en el acuerdo de inicio de procedimiento de verificación, una prórroga para ofrecer pruebas.

115. El tres de diciembre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **DGAJ/04002/2018** (**antecedente 114**) y otorgó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República una prórroga.

116. El tres de diciembre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público emitió el oficio **INAI/SPDP/DGEIVSP/645/18** a través del cual notificó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, el acuerdo descrito en el **antecedente 115**.

117. El cinco de diciembre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/04083/2018** de la misma fecha, emitido y signado por la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual en relación con el oficio **INAI/SPDP/DGEIVSP/623/18** del veintitrés de noviembre de dos mil dieciocho y con lo señalado en el acuerdo de inicio de procedimiento de verificación, rindió pruebas e indicó lo siguiente:

[...]

Con fundamento en los artículos 7, 10, fracción VI, de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Directora General de Asuntos Jurídicos, en representación jurídica de la o el Titular de la Procuraduría General de la República, me refiero a su diverso INAI/SPDP/DGEIVSP/623/18, relativo al expediente INAI.3S.08.03-003/2017, a través del cual, en relación con el acuerdo de inicio de procedimiento de verificación, se otorga un plazo a esta Institución para el ofrecimiento de pruebas en relación con las acciones emprendidas por la Procuraduría General de la República, como sujeto obligado, esto es, que se diseñaron, desarrollaron e implementaron políticas públicas de conformidad con las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO), que garanticen el cumplimiento.

Sobre el particular, estando dentro del plazo otorgado en la prórroga concedida, ofrezco las siguientes pruebas con las que se acreditan el principio de responsabilidad y el deber de seguridad, rectores de la protección de datos personales, previstos en los artículos 30, 31 y 32 de la LGPDPSO, a saber los siguientes:

- *Documento de Seguridad (...)*
- *Documento que contiene la Estrategia de Ciberseguridad de la Procuraduría General de la República.*

No omito mencionar, que las documentales que se remiten en sobre cerrado, para su debido resguardo y manejo, contienen información que encuadra los supuestos previstos en el artículo 55 de la LGPDPSO, en relación con el numeral 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

[...] (sic)

118. El seis de diciembre de dos mil dieciocho, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibido el oficio **DGAJ/04083/2018 (antecedente 117)**, sus documentos adjuntos, a petición del sujeto obligado ordenó su resguardo en sobre cerrado y que el análisis de su contenido se realizara al momento de resolver.

119. Mediante el oficio número **INAI/SPDP/DGEIVSP/662/2018** del once de diciembre de dos mil dieciocho, a efecto de allegarse de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, la Dirección



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[..]

Me refiero a su oficio número DGAJ/04083/2018 del cinco de diciembre de dos mil dieciocho recibido en la Dirección General de Evaluación, Investigación y Verificación del Sector Público del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en la misma fecha, mediante el cual ofrece pruebas en el expediente citado al rubro.

En este sentido, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, me permito solicitar su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda, a efecto de que se sirva proporcionar a este Instituto, la siguiente información con el soporte documental certificado que corresponda para cada caso:

- 1. Indique si el documento Estrategia de Seguridad de la Información de la PGR contempla el sistema de gestión y/o el documento de seguridad en el caso del software (sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS"), contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., con el objeto de realizar sus actividades sustantivas. Precizando la justificación o el sustento de ello.*
- 2. Indique si el documento Plataforma (...) contempla el sistema de gestión y/o el documento de seguridad en el caso del software (sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS"), contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., con el objeto de realizar sus actividades sustantivas. Precizando la justificación o el sustento de ello.*
- 3. Indique si existe alguna vinculación de los documentos (Estrategia de Seguridad de la Información de la PGR y Plataforma (...)), con el registro de uso del software denominado "PEGASUS".*
- 4. De acuerdo con lo señalado en la Estrategia de Seguridad de la Información de la PGR, es preciso que informe a este Instituto respecto del software denominado "PEGASUS", lo siguiente:*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- a) *En relación con lo dispuesto en el **punto 1.9** (páginas 7 y 8), el número de licencias compradas e instaladas, la fecha de activación y vencimiento de las licencias.*
 - b) *Respecto del **punto 2.3** (página 11), detalle el documento en el que obra el registro documental de cada uno de los accesos, en donde estén identificados los accesos asignados por los usuarios con su respectiva autorización.*
5. *Tomando en cuenta lo establecido en la Plataforma ..., que aportó como prueba, respecto al software denominado "PEGASUS", es necesario precise a partir de la posible utilización del mismo, lo siguiente:*
- a) *Tomando en cuenta lo señalado en el **punto 3** (página 1), ¿cuáles son, en general, los datos personales que se obtendrían?*
 - b) *En términos de lo contemplado en el **punto 5** (página 2), precise si los responsables detallados aplican también en el caso del software en mención.*
 - c) *De conformidad con lo establecido en el **punto 7** (páginas 2 y 3), es necesario indique ¿qué unidades administrativas participan o pueden participar en el proceso de recolección de la información a partir de un posible uso del software denominado "PEGASUS"? y ¿cuál es el fundamento legal de su actuación?*
 - d) *De acuerdo con lo señalado en el documento Plataforma ..., únicamente se investiga a partir de requerimientos y/o mandatos realizados por el ministerio público de la federación, bajo esta premisa, resulta indispensable que:*
 - *La forma en la que se lleva el registro de los requerimientos y/o mandatos.*
 - *Descripción del tipo de registro que se lleva, rubros que lo integran, personal que tiene acceso, medidas de seguridad aplicadas a su resguardo.*
 - *¿Qué tipo de personal realiza las ejecuciones de los requerimientos y/o mandatos? ¿qué pasa con los registros una vez que se cumple con el requerimiento y/o mandato?*
 - *Forma en la que se transfiere la información recabada al área competente (área que realizó el requerimiento y/o mandato); así como, las medidas de seguridad establecidas para la transferencia.*
 - *Criterios considerados para la cancelación, supresión o destrucción de los datos personales y mecanismos implementados en cada caso, precisando los servidores públicos que participan en la custodia de los datos durante la cancelación, supresión o destrucción.*
 - e) *Tomando en cuenta lo dispuesto en el **punto 8** (página 3), unidad que realiza la recolección y obtención de los datos personales, objeto de la recolección y*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

obtención, área que los almacena, uso que se les da y si se divulgan, proceso de bloqueo y de destrucción.

*Le agradeceré haga del conocimiento de este Instituto lo referido **en un término máximo de (5) cinco días hábiles**, contados a partir de que surta efectos la notificación del presente, de conformidad con los artículos 204, fracción I de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.*

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el once de diciembre de dos mil dieciocho.

120. El dieciocho de diciembre de dos mil dieciocho, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/04317/2018** del diecisiete del mismo mes y año, emitido y signado por la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/662/2018** descrito en el **antecedente 119**, indicando lo siguiente:

[...]

*Con fundamento en los artículos 7, 10, fracción VI y 32 de la Ley Orgánica de la Procuraduría General de la República, y 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Directora General de Asuntos Jurídicos, en representación jurídica de la o el Titular de la Procuraduría General de la República, me refiero a su diverso **INAI/SPDP/DGEIVSP/662/2018** de 11 de diciembre del año en curso, relativo al expediente **INAI.3S.07.01-007/2018**, en el que, en relación con los hechos que ese órgano garante verifica, requiere se le proporcione diversa información con el soporte documental certificado que corresponda, respecto de los planteamientos formulados en el siguiente cuestionario:*

Previo al desahogo de los cuestionamientos formulados por ese órgano garante, se estima necesario puntualizar que dicho desahogo se realizará sobre la base de la siguiente consideración y precisiones que se exponen:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Consideración: Mediante oficio INAI/SPDP/DGEIVSP/623/18 de 23 de noviembre del año en curso, deducido del acuerdo de inicio de procedimiento de verificación, se otorgaron a esta Institución, cinco días para ofrecer pruebas en relación con las acciones emprendidas, para:

[...]

En ese sentido y tomando como punto de partida el contenido del oficio INAI/SPDP/DGEIVSP/623/18, concretamente en la parte conducente de su foja 01, misma que en lo que interesa a la letra refirió que:

[...]

Sobre la base de los requerimientos formulados por ese Instituto Nacional en el procedimiento INAI.3S.07.01-007/2018, se estima necesario puntualizar que cualquier cuestión ajena al periodo comprendido del 29 de octubre al 31 de diciembre de 2014 relacionado con la tecnología adquirida por esta Institución resulta inatendible.

En comunión con la consideración hecha, se procede a realizar las siguientes precisiones:

Primera Precisión. *La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT) fue creada mediante Acuerdo A/076/17 publicado el 5 de septiembre de 2017, con el objeto de ser una unidad de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyan las investigaciones relacionadas con medios electrónicos y tecnológicos, con la finalidad de combatir tácticamente el fenómeno delictivo y la delincuencia. Por lo cual la UICOT solo investiga y labora a requerimiento de y/o mandatos que realiza el Ministerio Público de la Federación; lo anterior, tal y como se desprende de la parte considerativa del Acuerdo de creación, mismo que en lo que interesa establece:*

CONSIDERANDO

(Primer párrafo) Que la Constitución Política de los Estados Unidos Mexicanos establece en su artículo 21, párrafos primero y noveno, que la investigación de los delitos corresponde al Ministerio Público y a las policías, bajo la conducción y mando de aquel; siendo la seguridad pública una función que comprende, entre otros aspectos, la investigación y persecución de los delitos para hacerla efectiva.

Por su parte, el párrafo primero del artículo primero del Acuerdo de mérito, a la letra establece lo siguiente:

PRIMERO. *Se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas como la instancia de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyan las investigaciones relacionadas con medios*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

electrónicos y tecnológicos bajo la conducción y mando del Ministerio Público de la Federación.

Con base en ello y derivado de las facultades, atribuciones y funciones que se describen en el Acuerdo indicado, la UICOT, después de haber realizado una búsqueda en sus archivos, mediante oficio PGR/AIC/UICOT/02052/2018, comunicó a la suscrita que no encontró documento alguno que esté relacionado con la materia de verificación en el procedimiento en que se actúa, esto es, concretamente a la materia de lo requerido en el oficio INAI/SPDP/DGEIVSP/623/18, es decir:

- *Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la ley y en la demás normatividad aplicable.*
- *Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con las obligaciones previstas en la presente ley y en las demás normativa aplicable.*

Segunda precisión. *El cuerpo legal que tutelaba la protección de datos personales lo era la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, misma que, por cuanto hace a la protección de datos personales, estuvo vigente hasta el 26 de enero de 2017 por ser esta la fecha en la que se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por virtud de la previsión contenida en el artículo tercero transitorio de la Ley General de Transparencia y Acceso a la Información Pública que extendió la vigencia de la mencionada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.*

Con base en la consideración hecha y las precisiones formuladas, es claro concluir que los hechos relacionados con la materia de verificación en el procedimiento que se investiga, no pueden vincularse a las obligaciones que dimanen de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, pues sobre este aspecto, se insiste, no debe perderse de vista que la contratación de la tecnología adquirida por esta Institución es anterior a la entrada en vigor de las disposiciones contenidas en la ley que tutela la protección de datos personales, por lo que el documento denominado Estrategia de Seguridad de la Información de la Procuraduría General de la República no contempla el sistema de gestión y/o el documento de seguridad en el caso del software (sistema para la realización de actividades sustantivas denominado "PEGASUS"), contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., por ser la Estrategia de Seguridad referida, posterior a aquella en la que se materializó la adquisición de la tecnología indicada.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Sentado lo anterior, se procede al desahogo de los cuestionamientos hechos en los términos siguientes:

1. *Indique si el documento Estrategia de Seguridad de la Información de la PGR contempla el sistema de gestión y/o el documento de seguridad en el caso del software (sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS"), contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., con el objeto de realizar sus actividades sustantivas. Precisando la justificación o el sustento de ello.*

Respuesta: *En el caso, el documento Estrategia de Seguridad de la Información de la PGR no contempla el sistema de gestión y/o el documento de seguridad del software (sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS"), pues como se ha dicho, el instrumento normativo denominado Estrategia de Seguridad de la Información fue elaborado con fecha posterior a la celebración del contrato celebrado entre esta Institución y la empresa Grupo Tech Bull, S.A. de C.V.*

No obstante lo anterior, es decir, que el instrumento normativo denominado Estrategia de Seguridad de la Información, como se ha dicho fue emitido con fecha posterior a la celebración del contrato celebrado entre esta Institución y la empresa Grupo Tech Bull, S.A. de C.V., no menos cierto lo es que el citado instrumento se proyectó bajo una visión que permitiera que la Estrategia de Seguridad de la Información se desarrollará, gestionará e implementará de manera gradual, con un proceso de mejora continua que permitiera incorporar, modificar o eliminar tareas, que incluyan a tecnologías, personal y procesos de la Procuraduría, tal y como se advierte de la lectura del apartado denominado "Alcance" -foja 3-, de lo que se sigue que en el caso, bajo las directrices que contiene el multicitado instrumento, cualquier tipo de innovación tecnológica podría ser incorporada, modificada o eliminada.

Empero, en el caso que nos ocupa, es decir, respecto de la adquisición de la tecnología materia del contrato indicado, es de señalar que dicha tecnología nunca fue utilizada; con el fin de acreditar lo anterior, anexo en copia certificada, el oficio PGR/AIC/0302/2018 de primero de agosto de dos mil dieciocho, firmado por el Director en Jefe de la Agencia de Investigación Criminal.

Asimismo, se estima necesario puntualizar que estando dentro del plazo fijado por el artículo séptimo transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esto es durante el periodo de 18 meses con que contaba esta Institución en su calidad de sujeto obligado para tramitar, expedir o modificar su normatividad interna en la materia, elaboró el



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

documento de seguridad relativo a la tecnología que en la actualidad se encuentra vigente; sin que a la fecha se cuente con documento de seguridad diverso.

2. *Indique si el documento Plataforma ... contempla el sistema de gestión y/o documento de seguridad en el caso del software (sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS"), contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., con el objeto de realizar sus actividades sustantivas. Precizando la justificación o el sustento de ello.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

3. *Indique si existe alguna vinculación de los documentos (Estrategia de Seguridad de la Información de la PGR y Plataforma ..., con el registro de uso del software denominado "PEGASUS").*

Respuesta: No, en razón de que tal y como se mencionó al producir la contestación al primer cuestionamiento, la Estrategia de Seguridad de la Información fue proyectada sobre la base de que en el futuro se desarrollará, gestionará e implementará de manera gradual, un proceso de mejora continua que permitirá la incorporación, modificar o eliminar tareas, que incluyan a tecnologías, personal y procesos de la Procuraduría General de la República, la Plataforma ... no contempla el software denominado "PEGASUS".

4. *De acuerdo con lo señalado en la Estrategia de Seguridad de la Información de la PGR, es preciso que informe a este Instituto respecto del software denominado "PEGASUS", lo siguiente:*

a) *En relación con lo dispuesto en el punto 1.9 (páginas 7 y 8), el número de licencias compradas e instaladas, la fecha de activación y vencimiento de las licencias.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

b) *Respecto del punto 2.3 (página 11), detalle el documento en el que obra el registro documental de cada uno de los accesos en donde estén identificados los accesos asignados por los usuarios con su respectiva autorización.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

5. *Tomando en cuenta lo establecido en la Plataforma, que aportó como prueba, respecto al software denominado "PEGASUS", es necesario precise a través de la posible utilización del mismo, lo siguiente:*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- a) *Tomando en cuenta lo señalado en el punto 3 (página 1), ¿cuáles son, en general, los datos personales que se obtendrían?*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

- b) *En términos de lo contemplado en el punto 5 (página 2), precise si los responsables detallados aplican también en el caso del software en mención.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

- c) *De conformidad con lo establecido en el punto 7 (páginas 2 y 3), es necesario indique ¿qué unidades administrativas participan o pueden participar en el proceso de recolección de la información a partir de un posible uso del software denominado "PEGASUS"? y ¿cuál es el fundamento legal de su actuación?*

Respuesta: La Plataforma no contempla el software denominado "PEGASUS".

- d) *De acuerdo con lo señalado en el documento Plataforma ..., únicamente se investiga a partir de requerimientos y/o mandatos realizados por el ministerio público de la federación (sic), bajo esta premisa, resulta indispensable que:*

- *La forma en la que se lleva el registro de los requerimientos y/o mandatos.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

- *Descripción del tipo de registro que se lleva, rubros que lo integran, personal que tiene acceso, medidas de seguridad aplicadas a su resguardo.*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".

- *¿Qué tipo de personal realiza las ejecuciones de los requerimientos y/o mandatos? ¿Qué pasa con los registros una vez que se cumple con el requerimiento y/o mandato?*

Respuesta: La Plataforma ... no contempla el software denominado "PEGASUS".



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Adicionalmente, debe precisarse que una vez que se cumple con el requerimiento y/o el mandato, se estará a lo dispuesto por los artículos 15, 54, 106, 109, fracción XXVI y 347, fracción VII del Código Nacional de Procedimientos Penales, mismos que, en lo que interesa, a la letra disponen:

[...]

- *Forma en la que se transfiere la información recabada al área competente (área que realizó el requerimiento y/o mandato); así como, las medidas de seguridad establecidas para la transferencia.*

Respuesta: *La Plataforma ... no contempla el software denominado "PEGASUS".*

- *Criterios considerados para la cancelación, supresión o destrucción de los datos personales y mecanismos implementados en cada caso, precisando los servidores públicos que participan en la custodia de los datos durante la cancelación, supresión o destrucción.*

Respuesta: *La Plataforma ... no contempla el software denominado "PEGASUS".*

- e) *Tomando en cuenta lo dispuesto en el punto 8 (página 3), unidad que realiza la recolección y obtención de los datos personales, objeto de la recolección y obtención, área que los almacena, uso que les da y si se divulgan, proceso de bloqueo y de destrucción.*

Respuesta: *La Plataforma ... no contempla el software denominado "PEGASUS".*

Adicionalmente, debe precisarse que una vez que se cumple con el requerimiento y/o el mandato, se estará a lo dispuesto por los artículos 15, 54, 106, 109, fracción XXVI y 347, fracción VII del Código Nacional de Procedimientos Penales, mismos que, en lo que interesa, a la letra disponen:

[...]

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

[...](sic)



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

- a) Adjunto, se remitió la copia certificada del oficio número PGR/AIC/0302/2018 del uno de agosto de dos mil dieciocho emitido y signado por el director en jefe de la Agencia de Investigación Criminal, dirigido a la directora general de asuntos jurídicos, ambos de la entonces Procuraduría General de la República, a través del cual señaló lo siguiente:

[...]

*(...), en mi carácter de Director en Jefe de la Agencia de Investigación Criminal, me dirijo a Usted en relación a las solicitudes realizadas al suscrito mediante oficio número **DGAJ/02587/2018** de fecha **27 de julio de 2018**, con la finalidad de dar cabal contestación a cada una de ellas, en el mismo orden en el que fueron emitidas:*

[...]

Ahora bien, por lo que atañe a la solicitud consistente en:

"...Asimismo, en relación con la cláusula sexta del referido contrato (tomando como base la vigencia del mismo, es decir del 29 de octubre al 31 de diciembre de 2014), se especifique la temporalidad en que la Procuraduría General de la República dio uso a la referida tecnología o estuvo en condiciones de hacerlo, en razón de su licenciamiento, de acuerdo a los alcances y términos del contrato que nos ocupa..."

*Sobre el particular, **me permito comunicarle que esta Institución no utilizó la tecnología de referencia.***

[...]

121. El siete de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual tuvo por recibido el oficio **DGAJ/04317/2018** descrito en el **antecedente 120**.

122. Mediante el oficio número **INAI/SPDP/DGEIVSP/002/2019** del ocho de enero de dos mil diecinueve, a efecto de allegarse de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó al titular de la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión, en coadyuvancia institucional, lo siguiente:

[...]

*Me refiero al expediente de verificación **INAI.3S.07.01-007/2018**, sustanciado en la Dirección General de Evaluación, Investigación y Verificación del Sector Público del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.*

Al respecto se destaca que el treinta de junio de dos mil diecisiete, la entonces Dirección General de Investigación y Verificación de este Instituto dio inicio, de oficio, al procedimiento de investigación preliminar mixto, respecto a diversas entidades y dependencias que pudieran resultar con el carácter de responsables del tratamiento de los datos personales a través del software identificado como Pegasus.

*Ahora bien, la Dirección General de Evaluación, Investigación y Verificación del Sector Público tiene conocimiento del comunicado **986/17**, publicado el veintiuno de junio de dos mil diecisiete, mediante el cual la Procuraduría General de la República señaló que: "La FEADLE abrió una carpeta de investigación por los delitos de intervención de comunicaciones privadas y acceso ilícito a sistemas y equipos de informática, previstos en los artículos 177 y 211 bis 1 del Código Penal Federal, respectivamente".*

En este sentido, con fundamento en los artículos [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, se le requiere que gire sus apreciables instrucciones a quien corresponda, para que en estricta coadyuvancia institucional, se sirva proporcionar a este Instituto, la siguiente información en copia certificada por servidor público facultado para ello:

- 1. Informe el estado procesal de la carpeta de investigación a la que se hace referencia en el comunicado **986/17**.*
- 2. Proporcione el número o clave de identificación de la carpeta de investigación referida.*
- 3. Informe a esta autoridad si en la indagatoria de referencia se consideraron líneas de investigación respecto a la utilización o posible utilización del sistema adquirido por la Procuraduría General de la República denominado "PEGASUS", contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V.*
- 4. Precise, si los denunciantes y/o víctimas pusieron a disposición de esa representación social los equipos que según su dicho fueron infectados por el sistema multicitado, con el propósito de ser sometidos a alguna prueba pericial.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. *Señale si algún representante o apoderado de la organización denominada The Citizen Lab ha comparecido o rendido declaración dentro de la carpeta de investigación.*
6. *Si en la carpeta de investigación de mérito obra algún dictamen pericial respecto del uso o posible uso del sistema mencionado por parte de la Procuraduría General de la República, ya sea emitido por personal adscrito a la Coordinación General de Servicios Periciales de la dependencia o por algún otro perito autorizado.*

[...]

El requerimiento se notificó a la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión, el dieciséis de enero de dos mil diecinueve.

123. Mediante el oficio número **INAI/SPDP/DGEIVSP/015/2019** del once de enero de dos mil diecinueve, a efecto de allegarse de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, la Dirección General de Evaluación, Investigación y Verificación del Sector Público solicitó a la directora general de asuntos jurídicos de la entonces Procuraduría General de la República, lo siguiente:

[...]

Con fundamento en los [...], a efecto de que esta Dirección General de Evaluación, Investigación y Verificación del Sector Público se allegue de los elementos necesarios para resolver lo que en derecho corresponda, en relación con los hechos que se verifican, me permito solicitar su colaboración a efecto de que gire sus apreciables instrucciones a quien corresponda, a efecto de que se sirva proporcionar a este Instituto, la siguiente información con el soporte documental certificado que corresponda para cada caso:

1. *Informe el número de equipos (hardware) en el que se encuentra instalado y con los que funciona o funcionó el sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS", contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V.*
2. *Detalle las características del o de los equipos (hardware) en los que se encuentran alojadas las bases de datos del sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS".*
3. *Indique si se realizaron pruebas de operación del referido sistema e identifique las bases de datos que dan cuenta de la recopilación de los datos de prueba.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

4. *Informe si es factible el uso del sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS", para la recopilación de datos personales en la actualidad.*

[...]

El requerimiento se notificó a la Dirección General de Asuntos Jurídicos de la entonces Procuraduría General de la República, el dieciséis de enero de dos mil diecinueve.

124. El veintidós de enero de dos mil diecinueve, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/00127/2019** de la misma fecha, emitido y signado por la directora general de asuntos jurídicos de la ahora Fiscalía General de la República, antes Procuraduría General de la República, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/015/2019** descrito en el **antecedente 123**, indicando lo siguiente:

[...]

Con fundamento en lo dispuesto por el artículo Décimo Sexto transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en el Diario Oficial de la Federación el 10 de enero de 2014; y en términos de lo dispuesto por los artículos Tercero, Sexto y Décimo Segundo, fracción II, Transitorios del Decreto por el que se expide la Ley Orgánica de la Fiscalía General de la República, así como 3, inciso H), fracción II, y 49, fracción V, de su Reglamento, así como en el artículo PRIMERO, fracción II, numeral 2, del Acuerdo A/238/12 de la Procuradora General de la República, por el que se adscriben las unidades administrativas y órganos desconcentrados de la Procuraduría General de la República, publicado en el Diario Oficial de la Federación el 20 de septiembre de 2012, en mi carácter de Directora General de Asuntos Jurídicos, en representación jurídica del Titular de la Fiscalía General de la República, me refiero al requerimiento formulado mediante oficio INAI/SPDP/DGEIVSP/015/2019 de 11 de enero del año en curso, por el que solicita se informe y proporcione a ese órgano garante, el soporte documental certificado que corresponda en los casos que se transcriben:

1. *Informe el número de equipos (hardware) en el que se encuentra instalado y con los que funciona o funcionó el sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS",*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, SA. de C.V.

Sobre el particular, me permito informar que, en la actualidad, la Fiscalía General de la Republica -anteriormente denominada Procuraduría General de la República-, no cuenta con el sistema denominado "software pegasus".

Con base en lo anterior y toda vez que el sistema "software pegasus" en la actualidad no es utilizado por la Institución, no existe número o números de equipo en los que esté instalado.

En ese orden y en atención a la segunda parte de la información solicitada, esto es, "...el número de equipos (hardware) en el que se encuentra instalado y con los que funciona o funcionó el sistema para la realización de actividades sustantivas de la Procuraduría General de la Republica denominado "PEGASUS", contratado el veintinueve de octubre de dos mil catorce...", se estima pertinente puntualizar lo siguiente:

En atención a que la información relativa a este punto comprometería la Seguridad Nacional y la seguridad de la información con la que cuenta la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, se está en imposibilidad de proporcionarla; no obstante lo anterior, en la hora y fecha que ese órgano garante tenga a bien determinar, dará el acceso al equipo (hardware) con el que funcionó el sistema para la realización de actividades sustantivas de la anteriormente denominada Procuraduría General de la República.

El acceso indicado, de estimarlo procedente, se estaría realizando en las instalaciones que ocupa la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, [...].

- 2. Detalle las características del o de los equipos (hardware) en los que se encuentran alojadas las bases de datos del sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS".***

*En la documentación que obra en la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, **NO SE CUENTA** con alguna información que haga referencia a las "características del o de los equipos (hardware) en los que se encuentran alojadas las bases de datos del sistema para la realización de actividades sustantivas de la Procuraduría General de la República".*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

3. **Indique si se realizaron pruebas de operación del referido sistema e identifique las bases de datos que dan cuenta de la recopilación de los datos de prueba.**

*En la documentación que obra en la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, **NO SE CUENTA** con alguna información que haga referencia a pruebas de operación del sistema referido.*

4. **Informe si es factible el uso del sistema para la realización de actividades sustantivas de la Procuraduría General de la República denominado "PEGASUS", para la recopilación de datos personales en la actualidad.**

*Al día de hoy la Institución Fiscalía General de la República, anteriormente, Procuraduría General de la República, **NO CUENTA** con el "software Pegasus".*

[...] (sic)

125. El veintitrés de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibido el oficio **DGAJ/00127/2019** descrito en el **antecedente 124**; asimismo, señaló la hora y el día para que se llevara a cabo la diligencia de verificación al equipo (*hardware*) con el que funcionó el sistema para la realización de actividades sustantivas denominado "PEGASUS", en las instalaciones que ocupa la Agencia de Investigación Criminal.

126. El veintitrés de enero de dos mil diecinueve, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **AYD-FEADLE-046/2019** de la misma fecha, emitido y signado por la agente del ministerio público de la federación, adscrita a la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión, mediante el cual remitió el desahogo al requerimiento formulado a través del oficio **INAI/SPDP/DGEIVSP/002/2019** descrito en el **antecedente 122**.

127. El veinticuatro de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibido el oficio **AYD-FEADLE-046/2019** descrito en el **antecedente 126**, a petición del sujeto obligado ordenó su resguardo en sobre cerrado y que el análisis de su



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

contenido se realizara al momento de resolver; asimismo, señaló la hora y el día para que tuviera verificativo la diligencia con la finalidad de consultar la carpeta de investigación en las instalaciones que ocupa la Fiscalía Especial para la atención de Delitos cometidos contra la Libertad de Expresión.

128. Mediante el oficio número **INAI/SPDP/DGEIVSP/050/2019** del veinticuatro de enero de dos mil diecinueve, se solicitó al Secretario de Protección de Datos Personales de este Instituto, habilitar y comisionar a un especialista técnico en materia informática para que acuda en compañía de servidores públicos de la Dirección General de Evaluación, Investigación y Verificación del Sector Público, a la visita indicada en el acuerdo del veintitrés de enero de dos mil diecinueve (**antecedente 125**).

129. A través del oficio número **INAI/SPDP/DGEIVSP/051/2019** del veinticuatro de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, informó a diversos servidores públicos que se encontraban comisionados para acudir a la diligencia indicada en el acuerdo del veinticuatro de enero de dos mil diecinueve (**antecedente 127**).

El oficio se notificó a los servidores públicos comisionados adscritos a la Dirección General de Evaluación, Investigación y Verificación del Sector Público, el veinticinco de enero de dos mil diecinueve.

130. Por medio del oficio número **INAI/SPDP/DGEIVSP/057/2019** del veinticinco de enero de dos mil diecinueve, se informó al titular de la Fiscalía Especial para la atención de Delitos cometidos contra la Libertad de Expresión, el acuerdo emitido el veinticuatro de enero de dos mil diecinueve (**antecedente 127**).

El oficio se notificó a la Fiscalía Especial para la atención de Delitos cometidos contra la Libertad de Expresión, el veinticinco de enero de dos mil diecinueve.

131. Mediante el oficio número **INAI/SPDP/DGEIVSP/058/2019** del veinticinco de enero de dos mil diecinueve, se informó a la directora general de asuntos jurídicos de la Fiscalía General de la República, antes Procuraduría General de la República, el acuerdo emitido el veintitrés de enero de dos mil diecinueve (**antecedente 125**).



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

El oficio se notificó a la Dirección General de Asuntos Jurídicos de la Fiscalía General de la República, antes Procuraduría General de la República, en la misma fecha.

132. El veinticinco de enero de dos mil diecinueve, el Secretario de Protección de Datos Personales de este Instituto, emitió con fundamento en los artículos 2, fracciones IV, V y VI, 4, 89, fracciones I, VI y XIV, 146, 147, fracción I, 149, primero y cuarto transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 1, 2, 3, fracción VIII, 5, fracción VI, 25, fracción XXIII, 29, fracciones XXX y XXXVIII, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 182, 183, 184, 185, 200, 201, 202, 203, 204, fracción II, 205, 206 y 213 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; así como, el acuerdo de inicio de procedimiento verificación del veintitrés de noviembre de dos mil dieciocho, una **orden de verificación** para que se permitiera el acceso a los servidores públicos de este Instituto a las instalaciones que ocupa la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal de la Fiscalía General de la República, antes Procuraduría General de la República.

133. A través del oficio número **INAI/SPDP/064/19** del veinticinco de enero de dos mil diecinueve, el Secretario de Protección de Datos Personales de este Instituto, informó a diversos servidores públicos que se encontraban comisionados para acudir a la visita indicada en el acuerdo del veintitrés de enero de dos mil diecinueve (**antecedente 125**).

134. El veintinueve de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibida la minuta de la diligencia celebrada el veintiocho de enero de dos mil diecinueve en las instalaciones que ocupa la Fiscalía Especial para la atención de Delitos cometidos contra la Libertad de Expresión adscrita a la Fiscalía General de la República, ordenó su resguardo en sobre cerrado y que el análisis de su contenido se realizara al momento de resolver.

135. El treinta de enero de dos mil diecinueve, el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

por recibida la minuta de la diligencia celebrada el veintinueve de enero de dos mil diecinueve en las instalaciones que ocupa la Agencia de Investigación Criminal de la Fiscalía General de la República, ordenó su resguardo en sobre cerrado y que el análisis de su contenido se realizara al momento de resolver.

136. El dieciocho de febrero de dos mil diecinueve, se recibió en la Dirección General de Evaluación, Investigación y Verificación del Sector Público el oficio número **DGAJ/00264/2019** del catorce de febrero de dos mil diecinueve, emitido y signado por la directora general de asuntos jurídicos de la Fiscalía General de la República, mediante el cual realizó diversas manifestaciones y remitió documentación en alcance al oficio número **DGAJ/03482/2018 (antecedente 96)**.

- Adjunto al oficio señalado, se remitieron los siguientes anexos:
 - a) Oficio número PGR/AIC/0473-BIS/2018 del tres de octubre de dos mil dieciocho.
 - b) Oficio número PGR/AIC/UICOT/1629/2018 del tres de octubre de dos mil dieciocho.
 - b1) Acta entrega recepción del seis de octubre de dos mil dieciocho.
 - c) Oficio número FGR/AIC/UICOT/0167/2019 del siete de febrero de dos mil diecinueve:
 - 1. Acta de visita de verificación del veintinueve de enero de dos mil diecinueve.
 - 2. Oficio número PGR/AIC/CENAPI/OT/5893/2018 del uno de junio de dos mil dieciocho.
 - 3. Contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V.
 - 4. Oficio número PGR/AIC/CENAPI/OT/15681/2018 sin fecha.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

5. Contrato de prestación de servicios de actualización de licenciamiento y de nuevos dispositivos del *software*, mantenimiento y mejoras en servicios, servidores y estaciones de trabajo de la Plataforma NSO Pegasus, número PGR/AIC/CENAPI/CN/GSN/SERV/001/2017 del siete de junio de dos mil diecisiete, celebrado entre la Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia y la empresa Air Cap, S.A. de C.V. como proveedor.
6. Contrato de los servicios de actualización de licenciamiento y nuevos dispositivos del *software*, instalación de un módulo de análisis y las estaciones de trabajo de la Plataforma NSO Pegasus, del cinco de agosto de dos mil dieciséis, celebrado entre la Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia como solicitante y la empresa Proyectos y Diseños VME S.A. de C.V. como proveedor.

137. El diecinueve de febrero de dos mil diecinueve el director general de evaluación, investigación y verificación del sector público, emitió un acuerdo a través del cual: tuvo por recibido el oficio **DGAJ/00264/2019** descrito en el **antecedente 136**; así como sus documentos anexos, a petición del sujeto obligado ordenó su resguardo en sobre cerrado y que el análisis de su contenido se realizara al momento de resolver.

En razón de los antecedentes expuestos y previo análisis de las documentales aportadas por las partes, se tienen los siguientes:

CONSIDERANDOS

PRIMERO. El Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es competente para conocer y resolver el presente procedimiento de verificación conforme a lo previsto en los artículos 6, apartado A,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

fracción VIII de la Constitución Política de los Estados Unidos Mexicanos¹⁹, 1, 2, fracciones I, IV y V, 3, fracción XVIII, 4, 89, fracciones I, II, VI y XIV, 146, 147, fracción I, 149 y 150, primero y cuarto transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados²⁰, 62 y 69 de la Ley Federal de Procedimiento Administrativo²¹, 5, fracción I, VI y X, letra q., 6, 7, 8, 9, 10, 12, fracciones I y VIII, 18, fracción VII, 28, fracciones XIII y XVI, 29, fracción XXX, 41 Bis, fracciones I, III, VIII, X y XI del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales²²; así como, 181, 183, 200, 212, 213 y 214 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público²³.

SEGUNDO. En primer término, debe señalarse que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es de aplicación y observancia directa para los sujetos obligados del ámbito federal, teniendo el carácter de responsables del tratamiento de los datos personales que posean, de conformidad con lo dispuesto por los siguientes preceptos:

[...]

Artículo 1. La presente Ley es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

Todas las disposiciones de esta Ley General, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

[...]

¹⁹ Publicada en el Diario Oficial de la Federación el cinco de febrero de mil novecientos diecisiete, última reforma publicada el veintisiete de agosto de dos mil dieciocho.

²⁰ Publicada en el Diario Oficial de la Federación el veintiséis de enero de dos mil diecisiete.

²¹ De aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en términos de lo dispuesto en su artículo 9 y 195, fracción I de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

²² Publicado en el Diario Oficial de la Federación el diecisiete de enero de dos mil diecisiete.

²³ Publicados en el Diario Oficial de la Federación el veintiséis de enero de dos mil dieciocho.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

*Son **sujetos obligados** por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.*

Artículo 3. *Para los efectos de la presente Ley se entenderá por:*

[...]

XXVIII. Responsable: *Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;*

[...]

De los artículos transcritos, se desprende además que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, es de orden público y de observancia general en materia de protección de datos personales en posesión de sujetos obligados y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales.

Asimismo, son sujetos obligados por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, que den tratamiento a datos personales.

En este sentido, no debe pasar desapercibido que el veintitrés de noviembre de dos mil dieciocho se determinó iniciar a la entonces Procuraduría General de la República, ahora Fiscalía General de la República, el procedimiento de verificación respectivo.

Lo anterior resulta relevante, puesto que el catorce de diciembre de dos mil dieciocho se publicó la Ley Orgánica de la Fiscalía General de la República.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Así, de acuerdo con lo establecido en el transitorio segundo de la Ley Orgánica de la Fiscalía General de la República, se abrogó la Ley Orgánica de la Procuraduría General de la República; no obstante, de conformidad con lo dispuesto en el tercero y sexto transitorios de la Ley Orgánica de la Fiscalía General de la República **todas las menciones a la entonces Procuraduría General de la República, deben entenderse referidas a la ahora Fiscalía General de la República**, aunado a que los casos que se encontraran en trámite, serán resueltos en las unidades a las que están adscritos, conforme a las normas vigentes al momento de su inicio.

Aunado a lo señalado, la **Fiscalía General de la República** es un órgano público autónomo, dotado de personalidad jurídica y patrimonio propio a cargo de las funciones otorgadas al Ministerio Público de la Federación, tal y como se desprende de lo dispuesto en la Ley Orgánica de la Fiscalía General de la República:

[...]

Artículo 1. Objeto de la ley

La presente Ley tiene por objeto reglamentar la organización, funcionamiento y ejercicio de las atribuciones de la Fiscalía General de la República como órgano público autónomo, dotado de personalidad jurídica y patrimonio propio a cargo de las funciones otorgadas al Ministerio Público de la Federación, de conformidad con la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado Mexicano sea parte y demás disposiciones aplicables.

[...]

Así, al ser la **Fiscalía General de la República** un órgano público autónomo, **debe considerarse sujeto obligado para el ámbito de aplicación de la Ley General Protección de Datos Personales en Posesión de Sujetos Obligados**; por lo que, se encuentra constreñida al cumplimiento de los principios, deberes y obligaciones que en ella se establecen.

En consecuencia, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales está en posibilidad de conocer el presente asunto y



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

determinar lo conducente de acuerdo a las disposiciones aplicables en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

TERCERO. La presente resolución se emite dentro del expediente de verificación **INAI.3S.07.01-007/2018** y corresponde al ejercicio de atribuciones del órgano máximo de dirección de este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que mediante acuerdo número ACT-PUB/23/11/2018.08 autorizó por unanimidad el inicio de oficio de una verificación a la entonces Procuraduría General de la República, hoy Fiscalía General de la República, en el ámbito de aplicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con motivo de los elementos derivados de la sustanciación del procedimiento de investigación previa de oficio, identificada con el número de expediente **INAI.3S.08.03-003/2017**.

En esta tesitura, con base en lo dispuesto en la facultad prevista en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en relación con los artículos 146, 147, 149 y 150, norma jurídica que otorga facultades a esta autoridad administrativa para regular la conducta de los sujetos obligados y cerciorarse de que la misma se ajusta a las normas de orden público aplicables, a través del procedimiento de verificación a fin de constatar que los responsables han cumplido con las disposiciones en materia de protección de datos personales, el Pleno de este Instituto autorizó mediante el acuerdo número ACT-PUB/23/11/2018.08 el inicio de una verificación a la entonces Procuraduría General de la República, hoy Fiscalía General de la República; así, a través del acuerdo de inicio de procedimiento de verificación emitido el veintitrés de noviembre de dos mil dieciocho, se precisó lo siguiente:

[...]

QUINTO. Ahora bien, respecto a la vinculación o participación de la **Procuraduría General de la República** en los hechos que se investigan, es preciso destacar que los hechos materia del presente estudio se refieren al posible tratamiento de los datos personales que, en su caso, dicho sujeto obligado pudo haber efectuado a través de la utilización del software identificado como Pegasus, por lo que resulta necesario traer a colación los hallazgos derivados de la investigación, en desahogo a los requerimientos de información que se le formularon a dicho sujeto obligado y lo que se advirtió durante la diligencia in situ que se realizó en sus oficinas.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

*De acuerdo con lo expuesto, dado que no se advierte que el sujeto obligado ante la posibilidad del tratamiento de datos personales mediante el uso del software contratado hubiere diseñado, desarrollado e implementado políticas públicas de conformidad con las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ni garantizó su cumplimiento, **se presume que incumplió con el principio de responsabilidad.***

[...]

Ahora bien, ante la posibilidad del tratamiento de datos personales a través de su recolección mediante el uso del software contratado por la Procuraduría General de la República, se estima que debió contar al menos, con un sistema de gestión y con un documento de seguridad, relacionado con su tratamiento.

*Así, puesto que durante la investigación la Procuraduría General de la República no acreditó contar con dichos elementos, **se presume que incumplió con el deber de seguridad.***

[...]

En términos de lo expuesto, resulta procedente que se inicie el procedimiento de verificación respectivo, a fin de vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, al considerarse que existen los elementos que motivan la causa legal para iniciar el mismo, en contra de la Procuraduría General de la República.

*Por lo expuesto, **el objeto y alcance** del procedimiento de verificación seguido en contra de la Procuraduría General de la República, está dirigido a corroborar que cumpla con los principios y deberes rectores de la protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con el posible tratamiento de datos personales que se relaciona con un eventual uso del software identificado como Pegasus, **pudiéndose requerir al responsable la documentación e información necesaria; así como, la realización de las diligencias conducentes in situ.***

[...]

Ahora bien, previo al análisis de los resultados de la sustanciación del procedimiento de verificación que nos ocupa, se estima necesario citar las disposiciones que regulan el procedimiento de verificación, establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; así como, lo dispuesto en los



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados, en los siguientes términos:

[...]

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Artículo 146. El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de esta.

Artículo 147. La verificación podrá iniciarse:

[...]

I. De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o

[...]

Previo a la verificación respectiva, el Instituto o los Organismos garantes podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

[...]

Artículo 149. La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.

Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[..]

Artículo 150. El procedimiento de verificación concluirá con la resolución que emita el Instituto o los Organismos garantes, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

[...]

[...]

Lineamientos Generales de Protección de Datos Personales para el Sector Público

Artículo 181. De conformidad con lo previsto en el artículo 146 de la Ley General, el Instituto a través de la unidad administrativa competente conforme a su Estatuto Orgánico vigente, tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en dicho ordenamiento y los presente Lineamientos generales.

[...]

Capítulo III Del procedimiento de verificación

Artículo 200. El procedimiento de verificación se podrá iniciar:

[...]

II. Derivado de una investigación previa.

Artículo 201. El procedimiento de verificación iniciará con la emisión del acuerdo de inicio a que hace referencia el artículo 198, fracción II de los Lineamientos generales, el cual constituye una orden escrita que funda y motiva la procedencia de la actuación por parte del Instituto, a través de la unidad administrativa competente conforme a su Estatuto Orgánico vigente, y tiene por objeto establecer las bases para requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.

El acuerdo de inicio del procedimiento de verificación podrá ser emitido por el Pleno del Instituto, o bien, por las unidades administrativas del Instituto competentes de conformidad con lo dispuesto en el Estatuto Orgánico vigente al momento de emitirse el acuerdo a que se refiere el presente artículo.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

Artículo 204. *El procedimiento de verificación se sustanciará de la siguiente manera:*

- I. **Requerimientos de información:** *el Instituto deberá emitir los oficios correspondientes dirigidos al responsable o a cualquier tercero para que, en un plazo máximo de cinco días, contados a partir del día siguiente a que surta efectos la notificación, realice lo siguiente:*
 - a) *Presente las pruebas que considere pertinentes sobre el tratamiento que brinda a los datos personales, y*
 - b) *Manifieste lo que a su derecho convenga respecto de los hechos materia de la verificación y el procedimiento instaurado en su contra, y/o*

- II. **Visitas de verificación:** *el Instituto deberá realizar aquéllas que sean necesarias en las oficinas o instalaciones del responsable o, en su caso, en el lugar donde estén ubicadas las bases de datos personales o se realice el tratamiento de los datos personales objeto del procedimiento de verificación, teniendo una duración máxima de cinco días hábiles cada una, con la finalidad de que se allegue de la documentación e información necesaria sobre el tratamiento que el responsable lleve a cabo.*

El responsable no podrá negar el acceso a la documentación solicitada con motivo de un procedimiento de verificación, a sus bases de datos personales o tratamientos de éstos, no podrá invocar la reserva o la confidencialidad de la información.

[...]

Artículo 212. *El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la cual se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.*

La resolución del procedimiento de verificación será notificada personalmente, mediante oficio, al responsable y al denunciante a través del medio que hubiera proporcionado para tal efecto.

Artículo 213. *El procedimiento de verificación deberá tener una duración máxima de cincuenta días hábiles, contados a partir de la fecha en que se haya dictado el acuerdo de inicio respectivo, en términos del artículo 149, párrafo tercero, de la Ley General, el cual no podrá ser prorrogable.*

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

De la normativa transcrita, se desprende que:

- El Instituto, tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- La verificación podrá iniciarse de oficio cuando se cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes.
- Previa a la verificación, podrán desarrollarse investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.
- La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación del Instituto.
- Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto.
- El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la cual se establecerán las medidas que deberá adoptar el responsable.
- El procedimiento de verificación deberá tener una duración máxima de cincuenta días hábiles, contados a partir de la fecha en que se haya dictado el acuerdo de inicio respectivo.

En esa tesitura, es preciso señalar que el procedimiento de verificación de oficio que nos ocupa, derivó de una investigación previa instruida con la finalidad de allegarse de elementos para determinar si resultaba factible iniciar un procedimiento de verificación, en su caso, que permitiera corroborar si efectivamente alguna instancia del gobierno federal incurrió en alguna situación que hubiere podido contravenir el marco jurídico aplicable, en el ámbito federal, en materia de protección de datos personales; específicamente, lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Así, el veintitrés de noviembre de dos mil dieciocho se determinó iniciar a la entonces Procuraduría General de la República, el procedimiento de verificación respectivo, como se ha señalado previamente.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En este sentido, en la presente resolución que concluye el procedimiento de verificación referido, se analizan los elementos puestos en conocimiento de este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, considerando cada una de las actuaciones y constancias que obran tanto en el expediente del procedimiento de investigación, como en el de verificación.

Tomando en cuenta lo señalado, se llevará a cabo un análisis exhaustivo de todas las constancias que obran en los expedientes, atendiendo a lo dispuesto por el artículo 3, fracción XVI de la Ley Federal de Procedimiento Administrativo²⁴.

Al respecto, de dicho artículo se desprende que todo acto de autoridad debe expedirse atendiendo todos los puntos establecidos por la ley que, en el caso concreto, se traduce en que la resolución emitida debe ser exhaustiva, contando con congruencia interna y externa.

Establecido lo anterior, resulta fundamental considerar las manifestaciones y los elementos aportados por la Fiscalía General de la República, antes Procuraduría General de la República, durante la investigación y el procedimiento de verificación, además de, aquellos que fueron constatados por la instancia sustanciadora durante el desarrollo de la verificación correspondiente, ya sea mediante el desahogo de requerimientos de información al responsable y a autoridades coadyuvantes; así como, aquellos resultado de la visita de verificación practicada al sujeto obligado.

Así, no debe pasar desapercibido que durante el desarrollo de la **investigación** la entonces Procuraduría General de la República, remitió a la Dirección General de Evaluación, Investigación y Verificación del Sector Público, la versión pública del contrato celebrado el veintinueve de octubre de dos mil catorce entre la antes Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V.; así como, de su anexo técnico, documentos a los que se tuvo acceso para consulta *in situ*, como se ha referido en los antecedentes de la presente resolución.

²⁴ De aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo con lo dispuesto en el artículo 9.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

De acuerdo con lo anterior, puesto que en el **ANEXO TÉCNICO. ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"**, obra un apartado denominado "Recolección de datos", de su revisión, se pudo advertir el tipo de datos personales que podrían ser recolectados a través de dicho sistema, la forma de la recolección de los mismos en términos generales; así como, la cronología derivada del contrato (instalación, período de prueba y de uso contratado).

Con base en lo manifestado, resulta preciso señalar que la documental pública relativa al contrato y su anexo técnico, permitieron establecer un vínculo en materia de tratamiento de datos personales entre la entonces Procuraduría General de la República, debido a la factibilidad de uso de la tecnología referida, tras su adquisición por parte de dicha entidad pública y la facultad legal con la que cuenta para desarrollar actividades sustantivas de seguridad, investigación y prosecución de delitos, mismo que hizo viable el desarrollo de las facultades de verificación por parte de este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, con el objeto de corroborar el cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ordenamiento legal que tiene por objeto, establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, responsables de su tratamiento.

Derecho fundamental cuya tutela, por mandato del artículo 6o., apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos, ha sido encomendada a este Instituto como organismo autónomo, especializado, imparcial, colegiado, autoridad en la materia a que se refiere su denominación, sujeta como todas las demás del Estado, a la obligación impuesta en el artículo 1 de la ley fundamental, de promover, respetar, proteger y garantizar los derechos humanos, lo que se logra al interpretar el orden jurídico de su competencia a la luz y conforme a los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales en los que México es parte, favoreciendo en todo tiempo a las personas la protección



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

más amplia. Sobre el tema, el Poder Judicial de la Federación ha puesto énfasis en la siguiente tesis²⁵:

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. COMO AUTORIDAD DEL ESTADO, ESTÁ OBLIGADO A PROMOVER, RESPETAR, PROTEGER Y GARANTIZAR LOS DERECHOS HUMANOS, AL INTERPRETAR EL ORDEN JURÍDICO DE SU COMPETENCIA, FAVORECIENDO EN TODO TIEMPO A LAS PERSONAS LA PROTECCIÓN MÁS AMPLIA. Conforme al artículo 6o., apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento de los derechos de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados; se trata, por tanto, de una autoridad en la materia a que se refiere su denominación y, en consecuencia, sujeta, como todas las demás del Estado, a la obligación impuesta en el artículo 1o. de la Ley Fundamental, de promover, respetar, proteger y garantizar los derechos humanos, lo que se logra al interpretar el orden jurídico de su competencia a la luz y conforme a los derechos humanos reconocidos en la Constitución y en los tratados internacionales en los que México es Parte, favoreciendo en todo tiempo a las personas la protección más amplia.

En esa tesitura, si bien la investigación previa tuvo como origen ciertos hechos relacionados con "intentos de infección" presuntivamente realizados mediante el sistema denominado Pegasus del dos mil quince al dos mil dieciocho, los cuales se hicieron del dominio público a través de medios de comunicación; no menos cierto es, que las facultades con las que cuenta este Instituto se encaminan a garantizar la protección de los datos personales de los mexicanos, buscando que en todo momento se provea a las personas, como titulares de datos personales, la protección más amplia de dicho derecho fundamental.

Así, resulta importante destacar que no es la finalidad del presente procedimiento de verificación acreditar o tener por acreditados los referidos "intentos de infección" respecto al sujeto obligado verificado, lo que se busca es tutelar que el manejo de dicha tecnología

²⁵ Décima época, registro: 2015432, Tribunales Colegiados de Circuito, tipo de tesis: aislada, fuente: Gaceta del Semanario Judicial de la Federación, libro 47, octubre de 2017, tomo IV, materia(s): constitucional, tesis: I.7o.A.3 CS (10a.), página: 2444.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

en relación con el tratamiento de datos personales que permite la misma y estuvo latente desde su adquisición por parte de la entonces Procuraduría General de la República, haya sido acorde al mandato legal previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo a los principios y deberes que establece para los responsables frente a los titulares de datos personales, cualquiera que éstos sean.

Así, en desahogo a los requerimientos que se le formularon a la entonces Procuraduría General de la República, destacan las manifestaciones, que medularmente se hicieron consistir en lo siguiente:

- Está impedida para pronunciarse respecto a la posibilidad de recabar datos personales a través de la tecnología que adquirió, puesto que la tecnología **no fue utilizada**.
- Del dos mil quince a julio de dos mil dieciocho no recabó datos personales a través del uso de la tecnología adquirida. La tecnología, no fue utilizada en los diversos períodos respecto de los cuales se plantearon diversos hechos a partir de indicios de los que tomó conocimiento el Instituto.
- La temporalidad en que estuvo en condiciones de hacer uso de la tecnología adquirida fue la vigencia del contrato (del veintinueve de octubre al treinta y uno de diciembre de dos mil catorce), precisando que no fue utilizada la tecnología referida.
- No ha cedido por cualquier medio la licencia del uso del *software* Pegasus a algún tercero.
- No se ha realizado adquisición diversa, ni actualización alguna del *software*. La vigencia del contrato de adquisición de la tecnología fue del veintinueve de octubre al treinta y uno de diciembre de dos mil catorce.
- No cuenta con una bitácora de uso o registro del referido *software*.

Asimismo, durante el procedimiento de verificación que nos ocupa, la entonces Procuraduría General de la República precisó que ofrecía como pruebas para acreditar el principio de responsabilidad y el deber de seguridad que presuntivamente habría incumplido, dos documentos que conforman la estrategia de seguridad de la información con la que cuenta la Agencia de Investigación Criminal.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Al respecto, con la finalidad determinar si los documentos remitidos por la entonces Procuraduría General de la República, se relacionaban directamente con el objeto y alcance del presente procedimiento de verificación²⁶, se le formuló un requerimiento de información, en atención al cual, manifestó esencialmente lo siguiente:

- Cualquier cuestión ajena al periodo comprendido del veintinueve de octubre a treinta y uno de diciembre de dos mil catorce relacionado con la tecnología adquirida, resulta inatendible.
- La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas fue creada mediante acuerdo A/076/17 publicado el cinco de septiembre de dos mil diecisiete. Sólo investiga y labora a requerimiento de y/o mandatos que realiza el Ministerio Público de la Federación.
- La contratación de la tecnología adquirida es anterior a la entrada en vigor de las disposiciones contenidas en la ley que tutela la protección de datos personales, por lo que los documentos contemplados en la estrategia de seguridad de la información no contemplan el sistema de gestión y/o el documento de seguridad en el caso del sistema para la realización de actividades sustantivas denominado Pegasus, contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V. La estrategia referida es posterior a la adquisición de la tecnología indicada.
- **En el caso que nos ocupa, respecto de la adquisición de la tecnología materia del contrato indicado, es de señalar que dicha tecnología nunca fue utilizada.**
- Estando dentro del plazo fijado por el artículo séptimo transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esto es durante el periodo de 18 meses con que contaba en su calidad de sujeto obligado para tramitar, expedir o modificar su normatividad interna en la materia, elaboró el documento de seguridad relativo a la tecnología que en la actualidad se encuentra vigente, **sin que se cuente con documento de seguridad diverso al señalado, que contemple el software denominado "PEGASUS"**.

²⁶ **El objeto y alcance** del procedimiento de verificación seguido en contra de la Procuraduría General de la República, está dirigido a corroborar que cumpla con los principios y deberes rectores de la protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con el posible tratamiento de datos personales que se relaciona con un eventual uso del software identificado como Pegasus.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Aunado a lo anterior, cabe destacar que como parte de las constancias que integran el expediente de verificación que nos ocupa, se contempló requerir a la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión, con el objeto de que en coadyuvancia institucional, de acuerdo al contenido de la carpeta de investigación que informó públicamente tiene abierta en relación con los "intentos de infección" a través del sistema Pegasus, informara lo siguiente:

1. El estado procesal de la carpeta de investigación a la que se hace referencia en el comunicado **986/17**.
2. El número o clave de identificación de la carpeta de investigación referida.
3. Si en la indagatoria de referencia se consideraron líneas de investigación respecto a la utilización o posible utilización del sistema adquirido por la entonces Procuraduría General de la República denominado "PEGASUS", contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V.
4. Si los denunciantes y/o víctimas pusieron a disposición de esa representación social los equipos que según su dicho fueron infectados por el sistema multicitado, con el propósito de ser sometidos a alguna prueba pericial.
5. Si algún representante o apoderado de la organización denominada *The Citizen Lab* ha comparecido o rendido declaración dentro de la carpeta de investigación.
6. Si en la carpeta de investigación de mérito obra algún dictamen pericial respecto del uso o posible uso del sistema mencionado por parte de la entonces Procuraduría General de la República, ya sea emitido por personal adscrito a la Coordinación General de Servicios Periciales de la dependencia o por algún otro perito autorizado.

Atento a lo anterior, se destaca que la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión proporcionó la información solicitada, además de poner a disposición de este Instituto los registros que sustentan sus respuestas, mediante la consulta a la carpeta de investigación en sus instalaciones. Diligencia que tuvo verificativo el veintiocho de enero de dos mil diecinueve.

Al respecto, en atención al principio de secrecía que debe imperar en toda investigación penal en curso, se acordó que el contenido de la atención al requerimiento por parte de la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión y la minuta que da cuenta de la consulta a la carpeta de investigación debían mantenerse en sobre cerrado, el cual no sería glosado al expediente sino que permanecería bajo el resguardo de la Dirección General de Evaluación, Investigación y Verificación del Sector Público, precisando que su contenido sería analizado al resolver el presente asunto; por lo que, al momento de emitir la presente resolución se ha considerado en todos sus términos, destacando lo siguiente:

- La carpeta de investigación a la que se hace referencia en el comunicado **986/17**, publicado el veintiuno de junio de dos mil diecisiete, se encuentra en trámite e integración.
- El seis de octubre de dos mil diecisiete se realizó acta administrativa en la que se hizo constar la entrega de los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República, como bienes activos de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal, por parte del titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia.
- Se localizaron y revisaron los escritos de comparecencia de las personas que podrían haber sido objeto de los "intentos de infección" (víctimas); así como, su respuesta ante la solicitud de poner a disposición de la autoridad ministerial los equipos que supuestamente habrían sufrido los referidos "intentos de infección".
- Se localizaron y revisaron diversas diligencias, que mediante mecanismos de cooperación internacional, permitieron a *The Citizen Lab* desahogar requerimientos de información respecto al informe que publicó relativo a los intentos de infección a través del *malware* Pegasus, en el que se da cuenta sobre si practicó análisis a los equipos que presuntamente habrían recibido los referidos ataques, sobre si tenía pruebas para acreditar que alguna agencia gubernamental mexicana hubiera sido la que realizó las presuntas intervenciones; así como, la base probatoria de sus hallazgos.
- Se localizaron y revisaron diversos dictámenes emitidos por peritos en materia de fotografía forense, informática, electrónica y telecomunicaciones; así como,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

traducción, emitidos por profesionales de esas materias, adscritos a la Dirección General de Servicios Periciales de la entonces Procuraduría General de la República, que se relacionan con la búsqueda de evidencias sobre el posible uso de la tecnología Pegasus en el equipo (*hardware*) a cargo de la Agencia de Investigación Criminal.

Por otra parte, cabe destacar que se realizó un requerimiento de información a la entonces Procuraduría General de la República, con el objeto de que precisara:

1. El número de equipos (*hardware*) en el que se encuentra instalado y con los que funciona o funcionó el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V.
2. Las características del o de los equipos (*hardware*) en los que se encuentran alojadas las bases de datos del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS".
3. Si se realizaron pruebas de operación del referido sistema e identifique las bases de datos que dan cuenta de la recopilación de los datos de prueba.
4. Si es factible el uso del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", para la recopilación de datos personales en la actualidad.

En atención al requerimiento descrito, la Fiscalía General de la República, antes Procuraduría General de la República, señaló que:

- En la actualidad **no cuenta con el sistema** denominado "*software* pegasus".
- En la hora y fecha que el Instituto tenga a bien determinar, daría el acceso al equipo (*hardware*) con el que funcionó el sistema para la realización de actividades sustantivas de la anteriormente denominada Procuraduría General de la República.

Así, tras la emisión de la orden de verificación y el oficio de comisión por parte del Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Acceso a la Información y Protección de Datos Personales, servidores públicos de la Dirección General de Evaluación, Investigación y Verificación del Sector Público con apoyo de un servidor público especializado en informática, el veintinueve de enero de dos mil diecinueve llevaron a cabo la visita de verificación, constituyéndose en las oficinas que ocupa la Agencia de Investigación Criminal para revisar el equipo (*hardware*) relacionado con el funcionamiento del sistema para la realización de actividades sustantivas denominado Pegasus, adquirido por la entonces Procuraduría General de la República.

De acuerdo con lo anterior, de la diligencia derivó el acceso a los equipos (*hardware*) en los que refirió el sujeto obligado habría estado instalado el sistema para la realización de actividades sustantivas denominado Pegasus, teniendo a la vista el contrato de adquisición del veintinueve de octubre de dos mil catorce y su anexo técnico; así como, el acta administrativa del seis de octubre de dos mil diecisiete en la que se hizo constar la entrega de los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República, por parte del titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, al encargado de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, elementos con los que se contrastó que se trataba del equipo a verificar.

Cabe destacar, que con los requisitos previstos en los artículos 205 y 206 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público se hizo constar en el acta respectiva el desarrollo de la visita de verificación que nos ocupa, de la que se destaca medularmente lo siguiente:

- El seis de octubre de dos mil diecisiete la **Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas** recibió del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia el *hardware* objeto de la visita de verificación, incluyéndose como anexo al acta administrativa que da cuenta de este hecho; así como, copia del contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V., a través del cual el sujeto



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

obligado adquirió la tecnología que nos ocupa.

- El sistema para la realización de actividades sustantivas denominado Pegasus, **no está instalado ni registrado actualmente en el hardware de mérito.**
- De conformidad con lo establecido en el contrato y su anexo técnico, la instalación del sistema para la realización de actividades sustantivas denominado Pegasus, ocurrió dentro de la vigencia del mismo.
- No se localizan registros ni documentos que den cuenta de la desinstalación del sistema para la realización de actividades sustantivas denominado Pegasus, aclarando que, con base en el contrato, la vigencia del mismo fue al treinta y uno de diciembre de dos mil catorce.

En relación con lo expuesto, en cumplimiento a lo referido en el antepenúltimo párrafo del artículo 205 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se concedió a la Fiscalía General de la República su derecho a realizar manifestaciones con relación a la visita de verificación, mismo que hizo consistir en ese momento al tenor de lo siguiente:

- En la actualidad, no existe la posibilidad de que el sistema para la realización de actividades sustantivas denominado Pegasus, sea utilizado para la recopilación de datos personales.
- Las medidas de seguridad con las que actualmente se cuenta para el *hardware* que detenta, corresponden a **sistemas diversos** que emplea en el ejercicio de sus atribuciones.

Sobre las diligencias practicadas por parte del personal adscrito a la Secretaría de Protección de Datos Personales de este Instituto es preciso señalar, que de conformidad con lo dispuesto en el artículo 182 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en el ejercicio de las funciones de investigación y verificación, el personal del Instituto se encuentra dotado de fe pública para hacer constar la veracidad de los hechos con relación a las actuaciones practicadas.

Finalmente, a través de un alcance la Fiscalía General de la República realizó diversas manifestaciones y remitió documentación, alegando que de una nueva revisión y en atención a la diligencia de verificación *in situ*, había localizado nuevos datos relacionados



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

con el procedimiento de verificación que nos ocupa, cuyo contenido es analizado al resolver el presente asunto, destacando de la documentación remitida la siguiente:

- Acta entrega recepción del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República que hace el titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia al encargado de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, adscrita a la Agencia de Investigación Criminal, del seis de octubre de dos mil diecisiete.
- Contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V.
- Contrato de prestación de servicios de actualización de licenciamiento y de nuevos dispositivos del *software*, mantenimiento y mejoras en servicios, servidores y estaciones de trabajo de la Plataforma NSO Pegasus, número PGR/AIC/CENAPI/CN/GSN/SERV/001/2017 del siete de junio de dos mil diecisiete, celebrado entre la entonces Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia y la empresa Air Cap, S.A. de C.V. como proveedor.
- Contrato de los servicios de actualización de licenciamiento y nuevos dispositivos del *software*, instalación de un módulo de análisis y las estaciones de trabajo de la Plataforma NSO Pegasus, del cinco de agosto de dos mil dieciséis, celebrado entre la entonces Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia como solicitante y la empresa Proyectos y Diseños VME S.A. de C.V. como proveedor.

Ahora bien, por lo que respecta al alcance y valor probatorio de los documentos que obran en copia certificada en el expediente de verificación en que se actúa, es preciso considerar la siguiente jurisprudencia²⁷:

CERTIFICACIÓN DE COPIAS FOTOSTÁTICAS. ALCANCE DE LA EXPRESIÓN "QUE CORRESPONDEN A LO REPRESENTADO EN ELLAS", CONTENIDA EN EL ARTÍCULO 217 DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES, TRATÁNDOSE DE LA

²⁷ Tesis 2a./J. 2/2016 (10a.), Tribunales Colegiados de Circuito, página 873, Semanario Judicial de la Federación y su Gaceta, tomo I, febrero 2016, décima época.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

EMITIDA POR AUTORIDADES ADMINISTRATIVAS EN EJERCICIO DE SUS FUNCIONES.

*De la interpretación de los artículos 129 y 217 del Código Federal de Procedimientos Civiles se advierte que, por regla general, las copias certificadas **tienen valor probatorio pleno siempre que su expedición se realice con base en un documento original**, o de otra diversa copia certificada expedida por fedatario o funcionario público en el ejercicio de su encargo y, por el contrario, la certificación carece de ese valor probatorio pleno cuando no exista certeza si el cotejo deriva de documentos originales, de diversas copias certificadas, de copias autógrafas o de copias simples. En estas condiciones, cuando la copia es compulsada por un funcionario público, ello significa que es una reproducción del original y, por tanto, hace igual fe que el documento original, siempre y cuando en la certificación se incluya esa mención para crear convicción de que efectivamente las copias corresponden a lo representado en el cotejo; pues, en caso contrario, su valoración quedará al prudente arbitrio judicial. Bajo ese orden de ideas, la expresión "que corresponden a lo representado en ellas", contenida en el artículo 217 del Código Federal de Procedimientos Civiles implica que en la certificación, como acto jurídico material, se contenga la mención expresa de que las copias certificadas concuerdan de forma fiel y exacta con el original que se tuvo a la vista, a fin de que pueda otorgársele valor probatorio pleno, en términos del citado artículo 129; pues esa exigencia se justifica por la obligación de la autoridad administrativa de generar certeza y seguridad jurídica en los actos que emite. (sic)*

Así como, lo que establece la jurisprudencia²⁸:

COPIAS FOTOSTÁTICAS CERTIFICADAS DE OTRAS DE IGUAL ÍNDOLE, CUYO COTEJO O COMPULSA ORDENÓ LA JUNTA. HACEN FE EN EL JUICIO LABORAL, YA QUE PRODUCEN CERTEZA DE QUE SU CONTENIDO COINCIDE PLENAMENTE CON SU ORIGINAL, PUES ESA CONFIABILIDAD SE LA OTORGA LA CERTIFICACIÓN, SALVO PRUEBA EN CONTRARIO. *Las copias fotostáticas certificadas expedidas por la autoridad laboral **tienen pleno valor probatorio** no sólo cuando su expedición se realiza sustentándose en un documento original, sino también cuando se efectúa con apoyo en una copia certificada extendida por un funcionario público con fe pública que manifieste haber tenido el original a la vista y que ambos documentos concuerdan en todas sus partes. Ello es así, tomando en consideración, por una parte, el principio general para la valoración de pruebas contenido en el artículo 841 de la Ley Federal del Trabajo, que consiste en que las Juntas gozan de facultades para dictar sus laudos a verdad sabida y buena fe guardada, sin necesidad de sujetarse a reglas sobre la estimación de pruebas, apreciando los hechos según sus miembros lo crean debido en conciencia, pero siempre expresando las razones, motivos y fundamentaciones lógicas, esto es, sin llegar a conclusiones dogmáticas; y, por la otra, que la referencia que hace el artículo 798 de la ley de la materia en el sentido de que*

²⁸ Tesis 2a./J.16/2001, página 447, Seminario Judicial de la Federación y su Gaceta, tomo XIII, abril 2001, noven época.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

*cuando se ofrezca como medio de prueba un documento privado consistente en copia simple o fotostática se podrá solicitar, en caso de ser objetado, la compulsión o cotejo con el original, de modo alguno constituye un obstáculo para que dicha compulsión pueda realizarse con apoyo en una copia certificada, puesto que tal señalamiento únicamente tiene el propósito de precisar que aquel documento sirve de prueba idónea para el cotejo, pero de ninguna manera el de impedir que la compulsión se lleve a cabo con una copia certificada, **ya que no debe pasar inadvertido que ésta produce certeza de que su contenido coincide plenamente con su original, pues esa confiabilidad se la otorga la certificación, salvo prueba en contrario. En estas condiciones, cuando la copia simple o fotostática sea una reproducción del original y esté autenticada por un funcionario con fe pública hacen igual fe que el original, lo que encuentra apoyo, en lo esencial, en la jurisprudencia de la anterior Cuarta Sala de la Suprema Corte de Justicia de la Nación, publicada en el Semanario Judicial de la Federación, Séptima Época, Volúmenes 181-186, Quinta Parte, página 69, de rubro: "COPIAS FOTOSTÁTICAS, VALOR PROBATORIO DE LAS. REQUISITO DE FORMA.", que establece que: "No se le puede conceder valor probatorio alguno a las pruebas documentales fotostáticas cuando son objetadas según lo ordena el artículo 798 de la Ley Federal del Trabajo vigente, si al ofrecerlas no se cumple con los requisitos de forma, como son el que se acompañen de su original; a falta de este último, el que se ofrezca su cotejo con su original; a falta del citado cotejo, el que la propia documental fotostática se encuentre certificada por un funcionario con fe pública que manifieste haber tenido el original a la vista y que ambos concuerdan en todas sus partes. (sic)***

De los criterios anteriores, se tiene que las copias certificadas tienen valor probatorio pleno siempre que su expedición se realice con base en un documento original, o de otra copia certificada expedida por un fedatario o funcionario público en el ejercicio de su encargo, con fe pública que manifieste haber tenido el original a la vista y que ambos documentos concuerden en todas sus partes.

De acuerdo con lo señalado, resulta procedente conceder pleno valor probatorio sobre su contenido, a los documentos que, en copia certificada fueron agregados a los autos del expediente en que se actúa, mismos que serán considerados en todas sus partes para resolver lo que en derecho corresponda en el presente caso.

Así, respecto a los oficios remitidos por la Fiscalía General de la República, antes Procuraduría General de la República, agregados al expediente, se resalta que los mismos se toman en consideración como documentales públicas al ser emitidos por servidores públicos en ejercicio de sus atribuciones y que se entienden emitidos bajo los



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

principios de legalidad y buena fe que establece el artículo 13 de la Ley Federal de Procedimiento Administrativo²⁹ y, por tanto, corresponden a la instrumental de actuaciones, al formar parte de las constancias que obran dentro del presente expediente.

Asimismo, se destaca que la instrumental de actuaciones se desahoga por su propia y especial naturaleza, tal y como se señala en el criterio intitulado **PRUEBAS INSTRUMENTAL DE ACTUACIONES Y PRESUNCIONAL LEGAL Y HUMANA. NO TIENEN VIDA PROPIA LAS**³⁰, que refiere que las pruebas instrumental de actuaciones y la presuncional legal y humana, no tienen desahogo; es decir, que no tienen vida propia, pues no es más que el nombre que en la práctica se ha dado a la totalidad de las pruebas recabadas, por lo que respecta a la primera y por lo que corresponde a la segunda, éstas se derivan de las mismas pruebas que existen en las constancias de autos.

En términos de lo manifestado, se tiene que la instrumental de actuaciones se tiene por desahogada por su propia y especial naturaleza, toda vez que hace prueba plena.

Ahora bien, por cuanto hace a las notas periodísticas que se consideraron en el procedimiento de investigación previa, no debe pasar desapercibido que son únicamente indicios que se someten a la valoración de la autoridad, como un elemento contenido en la instrumental de actuaciones.

Al respecto, resultan orientadores los siguientes criterios:

NOTAS PERIODÍSTICAS, EL CONOCIMIENTO QUE DE ELLAS SE OBTIENE NO CONSTITUYE "UN HECHO PÚBLICO Y NOTORIO"³¹. *La circunstancia de que el público lector adquiera conocimiento de algún hecho consignado en periódicos o revistas, no convierte por esa sola circunstancia en "hecho público y notorio" la noticia consiguiente, toda vez que*

²⁹ De aplicación supletoria a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo a su artículo 9.

³⁰ Tesis: XX. 305 K, *Semanario Judicial de la Federación*, octava época, tribunales colegiados de circuito, tomo XV, enero de 1995, pág. 291, tesis aislada (común).

³¹ Tesis: I.4o.T.4 K, *Semanario Judicial de la Federación* y su gaceta, novena época 203622, Tribunales Colegiados de Circuito, tomo II, diciembre de 1995, pág. 541, tesis aislada común.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

es notorio lo que es público y sabido de todos, o el hecho cuyo conocimiento forma parte de la cultura normal propia de un determinado círculo social en el tiempo de su realización.

NOTAS PERIODÍSTICAS. ELEMENTOS PARA DETERMINAR SU FUERZA INDICIARIA³².

Los medios probatorios que se hacen consistir en notas periodísticas, sólo pueden arrojar indicios sobre los hechos a que se refieren, pero para calificar si se trata de indicios simples o de indicios de mayor grado convictivo, el juzgador debe ponderar las circunstancias existentes en cada caso concreto. Así, si se aportaron varias notas, provenientes de distintos órganos de información, atribuidas a diferentes autores y coincidentes en lo sustancial, y si además no obra constancia de que el afectado con su contenido haya ofrecido algún mentís sobre lo que en las noticias se le atribuye, y en el juicio donde se presenten se concreta a manifestar que esos medios informativos carecen de valor probatorio, pero omite pronunciarse sobre la certeza o falsedad de los hechos consignados en ellos, al sopesar todas esas circunstancias con la aplicación de las reglas de la lógica, la sana crítica y las máximas de experiencia, en términos del artículo 16, apartado 1, de la Ley General del Sistema de Medios de Impugnación en Materia Electoral, o de la ley que sea aplicable, esto permite otorgar mayor calidad indiciaria a los citados medios de prueba, y por tanto, a que los elementos faltantes para alcanzar la fuerza probatoria plena sean menores que en los casos en que no medien tales circunstancias.

De conformidad con lo anterior, los medios probatorios que se hacen consistir en notas periodísticas sólo pueden arrojar indicios sobre los hechos a que se refieren.

Es decir, las notas periodísticas no constituyen prueba plena, sino que únicamente constituyen elementos indiciarios sobre los que en ellas refiere y no son aptas para acreditar por sí mismas que la información que contienen se encuentra apegada a la realidad.

Así, las notas periodísticas que obran en el presente expediente únicamente pueden ser consideradas como indicios los cuales, en términos de lo que se ha señalado, no constituyen prueba plena.

De acuerdo a los elementos probatorios y diligencias descritas en el presente considerando, se realiza a continuación el análisis de cumplimiento de principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos

³² 920,903, jurisprudencia, materia(s): electoral, tercera época, Sala Superior del Tribunal Electoral, fuente: apéndice (actualización 2001), tomo VIII, P.R. Electoral, tesis: 134, página: 165.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Obligados, de acuerdo al objeto y alcance del procedimiento de verificación que autorizó el Pleno de este Instituto mediante acuerdo número ACT-PUB/23/11/2018.08, aprobado por unanimidad el veintitrés de noviembre de dos mil dieciocho en sesión pública, a la instancia de seguridad pública y nacional antes denominada Procuraduría General de la República, actualmente Fiscalía General de la República, con fundamento en los artículos 146, 147, 149 y 159 de la ley general en cita.

CUARTO. En relación con lo que se ha expuesto, es importante considerar que de conformidad con lo señalado en el acuerdo de inicio del procedimiento de verificación, emitido el veintitrés de noviembre de dos mil dieciocho, el **objeto y alcance** del procedimiento de verificación seguido en contra del sujeto obligado se dirigió a verificar que el responsable cumpla con los principios y deberes rectores de la protección de datos personales, previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativos al principio de responsabilidad y al deber de seguridad, respecto al posible tratamiento de datos personales a través de su recolección por medio del uso del sistema para la realización de actividades sustantivas denominado Pegasus, que adquirió la entonces Procuraduría General de la República en octubre de dos mil catorce.

Ahora bien, es preciso señalar que una cuestión previa y de especial pronunciamiento a considerarse en el presente caso, corresponde a la aplicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para resolver el fondo del asunto.

Ello, debido a que como se definió en el acuerdo de inicio respectivo, la norma adjetiva o procesal aplicable al caso concreto es sin duda la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados la cual entró en vigor el veintisiete de enero de dos mil diecisiete y, por ende, si el conocimiento del caso concreto se estableció a partir del inicio de la investigación previa de oficio, ello sucedió una vez que la referida ley general vigente definía el procedimiento para desarrollar las facultades de investigación y verificación de este organismo garante.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Sobre el particular, se reitera lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por cuanto hace a las facultades de investigación y verificación de este Instituto:

Artículo 146. *El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.*

En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los Organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.

Artículo 147. *La verificación podrá iniciarse:*

I. De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o

[...]

La verificación no procederá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente Ley.

La verificación no se admitirá en los supuestos de procedencia del recurso de revisión o inconformidad, previstos en la presente Ley.

Previo a la verificación respectiva, el Instituto o los Organismos garantes podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

Artículo 149. *La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.*

Artículo 150. *El procedimiento de verificación concluirá con la resolución que emita el Instituto o los Organismos garantes, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

No obstante lo anterior, refirió la entonces Procuraduría General de la República como parte de sus manifestaciones que la adquisición del sistema Pegasus se realizó de manera previa a la vigencia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y que los hechos investigados en un primer momento, se ceñían al dos mil quince y dos mil dieciséis; por lo que, de acuerdo a su consideración la ley general referida no le aplicaba al tratamiento de datos personales que hubiese merecido el posible uso de la tecnología adquirida.

Al respecto, es preciso señalar que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados contempla la posibilidad de que el Instituto inicie de oficio una verificación cuando cuente con indicios que hagan presumir de forma fundada y motivada, la existencia de violaciones a las leyes. Presunción que se definió con claridad en el acuerdo de inicio, considerando que con apoyo en la tecnología Pegasus podían recopilarse datos personales, lo que implicaba que en tanto la tuviera en su posesión la entonces Procuraduría General de la República, era factible su uso y, por ende, debía ceñirse al cumplimiento de las obligaciones previstas en la ley general de mérito.

Ahora bien, a mayor abundamiento, es preciso recordar que la investigación previa de este Instituto se amplió en su momento al dos mil diecisiete y dos mil dieciocho, ante la posibilidad de que diversos hechos relacionados con "intentos de infección" hubieran sucedido también durante dicho período; ante la posibilidad de recopilar datos personales con apoyo de la tecnología adquirida por parte de la entonces Procuraduría General de la República durante estos nuevos períodos.

Por otra parte, y sobre la aplicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para atender el fondo del asunto, es preciso señalar que el tratamiento de datos personales puede entenderse como:

[...]

Artículo 3. Para los efectos de la presente Ley se entenderá por:



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

IX. Datos personales: *Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;*

[...]

XXXIII. Tratamiento: *Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la **obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.***

[...]

Así, de los artículos transcritos, se desprende que:

- Serán datos personales, cualquier información concerniente a una persona física identificada o identificable.
- Se considera que una persona es identificable, cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- El tratamiento de datos personales, se refiere a cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados, relacionadas, entre otros, con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

De esta manera, el tratamiento de datos personales implica, entre otras, una serie de actividades y operaciones desarrolladas por parte de los sujetos obligados desde el momento en el que obtiene, almacena, posee, accede, transfiere o maneja datos concernientes a una persona física que la identifica o la hace identificable, las cuales no necesariamente se agotan en un único acto, lo que implica la posibilidad de estar frente actos de tracto sucesivo, lo que implica *per se*, la necesidad de observar el cúmulo de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

obligaciones que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados impone a los responsables de ese tratamiento.

Al respecto, como se definió en el considerando **TERCERO** de la presente resolución, el objeto del procedimiento de verificación que nos ocupa, en atención a las atribuciones con las que cuenta este Instituto, es tutelar que el manejo de esa tecnología en relación con el tratamiento de datos personales que permite la misma ante su adquisición por parte de la entonces Procuraduría General de la República, haya sido acorde al derecho de protección de datos personales, incluido el mandato legal previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo a los principios y deberes que establece para los responsables, frente a los titulares de datos personales.

En este sentido, no pasa inadvertido para este Instituto que el **siete de junio de dos mil diecisiete**, la entonces Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, formalizó el contrato PGR/AIC/CENAPI/CN/GSN/SERV/001/2017 (**antecedente 136, inciso c), numeral 5**), con objeto de contratar un servicio de actualización del licenciamiento, mantenimiento y mejoras en servicios, servidores y estaciones de trabajo de la plataforma NSO Pegasus; esto es, que durante la vigencia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el uso de la tecnología para la recolección de datos era evidente y, por lo tanto, debía sujetarse al cumplimiento de los principios y deberes que enarbola dicho ordenamiento legal.

Asimismo, destaca que como parte de las diligencias de verificación, este Instituto pudo corroborar que el último acto documentado en el que intervino el posible manejo de datos personales recabados a partir de la implementación del *software* adquirido por parte de la entonces Procuraduría General de la República tuvo lugar el seis de octubre de dos mil diecisiete, con la entrega-recepción (**antecedente 136, inciso b1**), mediante la cual el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia entregó a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, adscrita a la Agencia de Investigación Criminal, los recursos tecnológicos necesarios para la operación y desempeño; así como, **los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos**



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República, a fin de que la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas cumpliera con las funciones encomendadas, esto es, dentro de la vigencia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, máxime que a esa fecha, de acuerdo al contrato de licenciamiento referido en el párrafo anterior, sus efectos tenían una vigencia hasta el treinta y uno de diciembre de dos mil diecisiete.

Entonces, la aplicación de las bases, principios, deberes y obligaciones establecidas para la hoy Fiscalía General de la República, como sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados le son exigibles a dicho responsable, en tanto que el tratamiento de datos personales que sugiere la instalación del *software* en el equipo a cargo de la entonces dependencia del Ejecutivo, trascendió al transferirse los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República, del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, **en una fecha en la que se encontraba vigente la ley para todos los sujetos obligados y durante la vigencia de la actualización del licenciamiento de que se ha dado cuenta.**

Tomando en cuenta lo anterior, aún y cuando el sujeto obligado señaló no haber utilizado el sistema para la realización de actividades sustantivas denominado Pegasus, es preciso señalar que al realizar, mediante acta administrativa del seis de octubre de dos mil diecisiete, la entrega de los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República, como bienes activos a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal, por parte del titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, ante la posibilidad de utilización del sistema, debió atender lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al encontrarse vigentes los efectos



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

de la actualización del licenciamiento correspondiente a la tecnología adquirida por el sujeto obligado hasta el treinta y uno de diciembre de dos mil diecisiete.

En este sentido, lo que cobra relevancia para el caso concreto, es que la entonces Procuraduría General de la República afirmó no haber localizado documentos para acreditar los supuestos de incumplimiento que originaron la verificación que nos ocupa, como se asentó en el **antecedente 120** de la presente resolución.

Así, se estima que para que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se considere aplicada de manera retroactiva en perjuicio de la Fiscalía General de la República, se requeriría que obrara sobre el pasado previo a la vigencia de la ley en comento y que se lesionaran derechos adquiridos bajo el amparo de leyes anteriores, **lo que no sucede en el presente caso.**

En relación con lo manifestado, resulta importante destacar lo resuelto por el Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito en el Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito el veintidós de marzo de dos mil dieciocho³³, en la jurisprudencia intitulada **RETROACTIVIDAD DE LA LEY Y APLICACIÓN RETROACTIVA. SUS DIFERENCIAS**³⁴, de acuerdo con la cual:

- El **análisis de retroactividad de las leyes** implica estudiar si una determinada norma tiene vigencia o aplicación **respecto de derechos adquiridos o situaciones jurídicas acaecidas con anterioridad a su entrada en vigor.**

33

http://www.dgepij.cjf.gob.mx/internet/expedientes/ExpedienteTipo.asp?TipoAsunto=11&TipoProcedimiento=979&Expediente=425%2F2017&q-recaptcha-response=03AMGVjXhadmP12jUldkAkBGT7dUpS62DsnvAtXOEyvWgo8DqoiW13o4o4aXHNxeJm5gm699CSHn3dh3O2cQ5IUevqrOvXXzOouXLoB1nLzEzkpqZY3AcB24L_nqlgdERxlwtkVKbUvo4MLe-9OI7NldUQwaQnVZ_ZOCmt94Sryk3I4buTGa98bsj6Af6jfGIFryxsykOqBZn7DtSPS7jKA_nOhqldkYOWPbcfZtqBubaxa7fdq17fgcMWWK-niAxVAwMfO8nilkJjfdxMSAOrcY0CTySUrwRGxA&Buscar=Buscar&Circuito=1&CircuitoName=PRIMER+CIRCUITO&Organismo=79&OrgName=D%E9cimo+Tribunal+Colegiado+en+Materia+Administrativa+del+Primer+Circuito&TipoOrganismo=0&Accion=1 vínculo consultado el diez de octubre de dos mil dieciocho.

³⁴ 162299, 1a./J. 78/2010, primera sala, novena época, Semanario Judicial de la Federación y su Gaceta, tomo XXXIII, abril de 2011, pág. 285. Cfr. <https://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/162/162299.pdf>

235



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- **El análisis sobre la aplicación retroactiva de una ley** supone la verificación de que los actos materialmente administrativos o jurisdiccionales estén fundados en normas vigentes, y que **en caso de un conflicto de normas en el tiempo se aplique la que genere un mayor beneficio al particular.**

Lo señalado resulta relevante puesto que, en el presente caso, no se lesionan derechos adquiridos bajo el amparo de leyes anteriores, cabe recordar que tanto la Constitución Política de los Estados Unidos Mexicanos y la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental reconocían a los ciudadanos la protección de sus datos personales y a este Instituto como el organismo encargado de garantizar ese derecho fundamental, cuya facultad de vigilancia y emisión de recomendaciones fue ampliada con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, más no diseñada o concretada a partir de la misma.

Tal y como se ha señalado, es en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en la que se **establece el procedimiento para que el Instituto lleve a cabo las investigaciones previas y verificaciones, por presuntos incumplimientos a las normativas aplicables.**

Tomando en cuenta lo expuesto, se considera que la norma aplicable en lo procesal y en lo sustantivo dada la naturaleza de la verificación practicada por este Instituto es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, siendo este organismo autónomo competente para resolver lo que en derecho corresponde en términos de lo dispuesto en dicha ley.

Así, en relación con la obligación a cargo del sujeto obligado entonces Procuraduría General de la República respecto a la observancia de los principios y el cumplimiento de los deberes que prevé la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, debe confrontarse en el presente caso con el contenido de las actuaciones y constancias que obran tanto en el expediente del procedimiento de investigación previa **INAI.3S.08.03-003/2017**, como en el expediente de la verificación **INAI.3S.07.01-007/2018**, en relación con el posible tratamiento de datos personales a través de su recolección por medio del uso del sistema para la realización de actividades sustantivas denominado Pegasus.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Lo anterior, con el objeto de determinar si el sujeto obligado cumplió con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, observando lo dispuesto sus artículos:

[...]

Artículo 1. *La presente Ley es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.*

Todas las disposiciones de esta Ley General, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

El Instituto ejercerá las atribuciones y facultades que le otorga esta Ley, independientemente de las otorgadas en las demás disposiciones aplicables.

Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Artículo 4. *La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.*

[...]

Artículo 6. *El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.*

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[...]

Artículo 8. *La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia.*

Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

[...]

De los artículos transcritos se advierte que:

- Todas las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.
- El Instituto ejercerá las atribuciones y facultades que le otorga la ley, independientemente de las otorgadas en las demás disposiciones aplicables.
- La ley tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados y será aplicable a cualquier



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

- La aplicación e interpretación de la ley, se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales; así como, las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia.

Ahora bien, en el presente como en todos aquellos casos en los que está involucrado el tratamiento de datos personales, no debe perderse de vista la obligación a cargo de los sujetos obligados y/o responsables de observar los principios y deberes previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el caso concreto, se destacan el principio de responsabilidad; así como, el deber de seguridad que fueron referidos en el acuerdo de inicio que originó el procedimiento de verificación en que se actúa.

En este sentido, previo análisis del principio de responsabilidad y del deber de seguridad, resulta relevante referir que todo tratamiento de datos personales debe sujetarse a las facultades o atribuciones que la normativa aplicable le confiera al responsable.

En el caso que nos ocupa y entendiendo que la legalidad de los actos inmersos en el tratamiento de los datos personales se basa en las referencias normativas que facultan a los sujetos obligados a realizar el mismo, es importante traer a colación lo dispuesto en el artículo 291 del Código Nacional de Procedimientos Penales; así como, lo dispuesto en los artículos primero, segundo, tercero, cuarto, sexto y octavo del acuerdo A/018/15 por el que se delega en los servidores públicos que se indican, diversas facultades previstas en el Código Nacional de Procedimientos Penales, disposiciones de las cuales se desprende que el titular de la entonces Procuraduría General de la República o servidores públicos en quienes se delegue esta facultad contaban con la atribución para intervenir comunicaciones privadas cuando en una investigación se considere necesario; para lo cual, tanto el titular de la entonces Procuraduría General de la República o servidores públicos en quienes se delegue esta facultad se encontraban obligados a



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

solicitar al juez federal de control competente la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

También se requería autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como, la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.

En esta lógica, el tratamiento de datos personales consecuente con el posible uso de una herramienta tecnológica como la que nos ocupa, para los fines que fue adquirida según refirió el sujeto obligado tanto en los procedimientos de investigación como en el de verificación, estaría relacionado con atribuciones como las previstas en el artículo 291 del Código Nacional de Procedimientos Penales y en el acuerdo A/018/15 por el que se delega en los servidores públicos que se indican, diversas facultades previstas en el Código Nacional de Procedimientos Penales, a través del cual se confieren atribuciones a la entonces Procuraduría General de la República de intervenir y extraer información de las comunicaciones privadas bajo ciertos requisitos.

Requisitos que se prevén fundamentalmente, en una autorización emitida por un juez de control de la Federación, mediante una solicitud a través de la cual exprese el objeto y necesidad de su actuación y su vinculación con una investigación en trámite.

En este sentido y no obstante las declaraciones de la entonces Procuraduría General de la República respecto a la no utilización del sistema denominado Pegasus, es preciso señalar que con las actuaciones que obran en el expediente que nos ocupa no se permite confirmar tales aseveraciones, considerando ante todo que el sistema de mérito fue desinstalado y que la entonces Procuraduría General de la República no acreditó contar con una bitácora o con algún registro de su uso; además, de no contar con un registro de las bases de datos que debían generarse en la operación del propio sistema, según su anexo técnico, circunstancia que sostuvo el sujeto obligado desde las diligencias de investigación previa y que ratificó en la visita de verificación *in situ*, considerando los



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

archivos de las unidades administrativas que detentaron el sistema y que intervinieron en el acta de entrega-recepción del seis de octubre de dos mil diecisiete.

Así, precisamente, aun y cuando con base en sus atribuciones podría estar facultado el sujeto obligado para emplear este tipo de tecnología para el desarrollo de su función investigadora ministerial, ante la referida capacidad para realizar tratamiento de datos personales con base en la tecnología adquirida; es decir, recabar, procesar y llevar a cabo ciertas operaciones con los datos personales obtenidos a través de la misma, así como, la obligación de registro de esas operaciones al tratarse de una potestad en la que debe mediar autorización judicial previa para su desarrollo, existe la imperiosa necesidad de analizar si el sujeto obligado cumplió con los extremos atinentes al principio de responsabilidad y al deber de seguridad que se establecen en la Ley General de Protección de datos Personales en Posesión de Sujetos Obligados, en los siguientes términos:

[...]

Artículo 16. *El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y **responsabilidad** en el tratamiento de datos personales.*

[...]

Artículo 30. *Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:*

[...]

VII. *Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y*

VIII. *Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Artículo 31. *Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*

Artículo 32. *Las medidas de seguridad adoptadas por el responsable deberán considerar:*

- I. El riesgo inherente a los datos personales tratados;*
- II. La sensibilidad de los datos personales tratados;*
- III. El desarrollo tecnológico;*
- IV. Las posibles consecuencias de una vulneración para los titulares;*
- V. Las transferencias de datos personales que se realicen;*
- VI. El número de titulares;*
- VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*
- VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.*

Artículo 33. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

- I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
- II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
- III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
- IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
- V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
- VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
- VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Artículo 34. *Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.*

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Artículo 35. *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

- I. El inventario de datos personales y de los sistemas de tratamiento;*
- II. Las funciones y obligaciones de las personas que traten datos personales;*
- III. El análisis de riesgos;*
- IV. El análisis de brecha;*
- V. El plan de trabajo;*
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*
- VII. El programa general de capacitación.*

[...]

De los artículos transcritos se advierte que:

- El principio de responsabilidad consiste en que el sujeto obligado debe adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y obligaciones establecidos en la ley y rendir cuentas sobre dicho tratamiento. Encontrándose entre dichos mecanismos, los siguientes:
 - Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, **de conformidad con las disposiciones previstas en la ley** y en la demás normativa aplicable.
 - Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

que implique el tratamiento de datos personales, **cumplan con las obligaciones previstas en la presente ley** y en la demás normativa aplicable.

Asimismo, se destaca que los responsables deberán:

- Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Al adoptar medidas de seguridad, deberá considerarse: el riesgo inherente a los datos personales tratados, el desarrollo tecnológico, la sensibilidad de los datos personales tratados, las posibles consecuencias de una vulneración para los titulares, el número de titulares.

De acuerdo con lo anterior, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá:

- Crear políticas internas para la gestión y tratamiento de los datos personales, tomando en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales: obtención, uso y supresión.
- Definir las funciones y obligaciones del personal involucrado en el tratamiento.
- Elaborar un inventario de datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes; así como, las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.
- Monitorear y revisar de manera periódica las medidas de seguridad implementadas; así como, las amenazas y vulneraciones a las que están sujetos los datos personales.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Ahora bien, las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un **sistema de gestión**, el cual se entenderá como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Asimismo, en cumplimiento al deber de seguridad, el responsable deberá elaborar un **documento de seguridad** que contenga:

- El inventario de datos personales y de los sistemas de tratamiento.
- Las funciones y obligaciones de las personas que traten datos personales.
- El análisis de riesgos.
- El análisis de brecha.
- El plan de trabajo.
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.
- El programa general de capacitación.

Lo descrito anteriormente, cobra relación con el presente asunto, puesto que tal y como se señaló en el acuerdo de inicio de procedimiento de verificación emitido el veintitrés de noviembre de dos mil dieciocho, se presumió el incumplimiento por parte de la entonces Procuraduría General de la República del principio de responsabilidad y del deber de seguridad, de acuerdo con lo siguiente:

[...]

QUINTO. Ahora bien, respecto a la vinculación o participación de la **Procuraduría General de la República** en los hechos que se investigan, es preciso destacar que los hechos materia del presente estudio se refieren al posible tratamiento de los datos personales que, en su caso, dicho sujeto obligado pudo haber efectuado a través de la utilización del software identificado como **Pegasus**, por lo que resulta necesario traer a colación los hallazgos derivados de la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

investigación, en desahogo a los requerimientos de información que se le formularon a dicho sujeto obligado y lo que se advirtió durante la diligencia in situ que se realizó en sus oficinas.

[...]

*De acuerdo con lo expuesto, dado que no se advierte que el sujeto obligado ante la posibilidad del tratamiento de datos personales mediante el uso del software contratado hubiere diseñado, desarrollado e implementado políticas públicas de conformidad con las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ni garantizó su cumplimiento, **se presume que incumplió con el principio de responsabilidad.***

[...]

Ahora bien, ante la posibilidad del tratamiento de datos personales a través de su recolección mediante el uso del software contratado por la Procuraduría General de la República, se estima que debió contar al menos, con un sistema de gestión y con un documento de seguridad, relacionado con su tratamiento.

*Así, puesto que durante la investigación la Procuraduría General de la República no acreditó contar con dichos elementos, **se presume que incumplió con el deber de seguridad.***

[...]

En términos de lo expuesto, resulta procedente que se inicie el procedimiento de verificación respectivo, a fin de vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, al considerarse que existen los elementos que motivan la causa legal para iniciar el mismo, en contra de la Procuraduría General de la República.

*Por lo expuesto, **el objeto y alcance** del procedimiento de verificación seguido en contra de la Procuraduría General de la República, está dirigido a corroborar que cumpla con los principios y deberes rectores de la protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con el posible tratamiento de datos personales que se relaciona con un eventual uso del software identificado como Pegasus, **pudiéndose requerir al responsable la documentación e información necesaria; así como, la realización de las diligencias conducentes in situ.***

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora bien, como punto de partida del análisis de estos posibles incumplimientos, se destaca que, de acuerdo al contenido de las diligencias y constancias que obran en el expediente citado al rubro, se tiene acreditada la **adquisición** del sistema para la realización de actividades sustantivas denominado Pegasus, por parte de la entonces Procuraduría General de la República, con el contrato de adquisición que celebró dicho ente público el veintinueve de octubre de dos mil catorce.

En relación directa con lo manifestado, se destaca que la **instalación** de dicho sistema ocurrió de acuerdo a los términos y condiciones de instalación descritos en el contrato, corroborándose, con la existencia del *hardware* en el que se encontraba el sistema y la manifestación de la representante de la ahora Fiscalía General de la República durante la visita de verificación, en el sentido de que la misma habría ocurrido dentro de la vigencia del contrato, esto es, entre el veintinueve de octubre de dos mil catorce y el treinta y uno de diciembre del mismo año.

Lo señalado resulta relevante en el presente asunto, puesto que con base en el contenido del **ANEXO TÉCNICO. ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"**, del contrato celebrado el veintinueve de octubre de dos mil catorce en el que se describe en un apartado específico la recolección de los datos a los que se podían acceder a través del uso del sistema en comento, que el tratamiento de datos personales era completamente factible, inclusive respecto al período de pruebas que para su instalación de acuerdo al propio contrato, tuvieron que realizarse.

Lo anterior, basados en el hecho de que en el apartado denominado "Recolección de datos" del **ANEXO TÉCNICO. ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"**, se precisan los tipos de datos personales que podrían ser recolectados, tras la instalación del sistema; así como, que los datos recogidos serían enviados hacia un centro de control en tiempo real, viajando de forma segura y cifrada.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

De acuerdo con lo descrito, el hecho de que se haya previsto, de conformidad al referido anexo técnico, que los datos personales que pudieron haberse recolectado a través del sistema contratado por la entonces Procuraduría General de la República durante el periodo de pruebas y el periodo de uso, se enviarían a un centro de control (servidor), da cuenta de la necesaria **generación por parte de dicho sistema** de repositorios de dicha información; esto es, **de bases electrónicas en las que debían resguardarse los datos personales recolectados a través del sistema, para ser empleados en las tareas de investigación, seguridad y prosecución de delitos (actividades sustantivas) de la entonces Procuraduría General de la República.**

Asimismo, no pasa inadvertido que de acuerdo con lo señalado en el contrato PGR/AIC/CENAPI/CN/GSN/SERV/001/2017 (**antecedente 136, inciso c), numeral 5**), el administrador del contrato y el responsable técnico (ambos servidores públicos de la entonces Procuraduría General de la República), en coordinación con el personal técnico del proveedor, procederían a realizar las pruebas a la versión actualizada del sistema y equipos a los que se les otorgó mantenimiento, los cuales tendrían que mostrar todas las funcionalidades que se solicitaron, por parte del sujeto obligado, mismas que **deberían registrarse en un formato con protocolos de prueba que serían firmados por las áreas mencionadas.**

Ahora, en relación directa con lo manifestado, destaca que si bien la entonces Procuraduría General de la República manifestó durante la sustanciación de la verificación que nos ocupa que el sistema en mención no fue utilizado, los extremos de esa afirmación no fueron acreditados, pues si bien se tuvo acceso al *hardware* en el que habría estado instalado el *software* Pegasus, ya no se cuenta con el sistema, máxime que la hoy Fiscalía General de la República indicó no tener con documentos que dieran cuenta de su desinstalación y de las medidas adoptadas para el borrado de la información que se habría generado con dichas operaciones (bases electrónicas en las que debían resguardarse los datos personales recolectados a través del sistema, incluso durante los periodos de prueba estipulados tanto en el anexo técnico del contrato de adquisición como en los contratos de actualización de licenciamiento mencionados; así como, la bitácora de uso o registro y el formato con protocolos de prueba firmados por los responsables, según se indicó en los instrumentos jurídicos remitidos en alcance por el sujeto obligado).



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora bien, no escapa al análisis de este Instituto que la **Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas** de la Agencia de Investigación Criminal fue creada mediante acuerdo A/076/17 publicado el cinco de septiembre de dos mil diecisiete, con el objeto de ser una unidad de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyan las investigaciones relacionadas con medios electrónicos y tecnológicos, con la finalidad de combatir tácticamente el fenómeno delictivo y la delincuencia.

Así, el seis de octubre de dos mil diecisiete se realizó acta administrativa en la que se hizo constar la entrega de los recursos tecnológicos necesarios para la operación y desempeño; así como, **los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República**, como bienes activos de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal, por parte del titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia.

En relación con lo anterior, respecto del estado actual del sistema para la realización de actividades sustantivas denominado Pegasus, no pasa por alto que, durante la visita de verificación llevada a cabo en la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal, se pusieron a la vista los equipos (*hardware*) en los que estaba instalado el sistema y que el sujeto obligado informó que dicho sistema **no está instalado** en el *hardware* que obra en dicha unidad ni obra registro o bitácora de uso.

En este sentido, durante la visita de verificación respecto a la desinstalación del sistema para la realización de actividades sustantivas denominado Pegasus, en el *hardware* revisado, la Fiscalía General de la República señaló que de conformidad con lo establecido en el contrato y su anexo técnico, la instalación del sistema para la realización de actividades sustantivas denominado Pegasus, debió ocurrir dentro de la vigencia del mismo, mientras que no se habían localizado registros ni documentos que den cuenta de



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

la desinstalación de dicho sistema, aclarando que con base en el contrato, la vigencia del mismo fue al treinta y uno de diciembre de dos mil catorce.

Al respecto, si bien se consideró una vigencia que se agotaba treinta y uno de diciembre de dos mil catorce, gracias a las diligencias de verificación realizadas por este organismo garante y al alcance remitido por la Fiscalía General de la República, se pudo advertir que dicho *software* estuvo licenciado y con posibilidad de uso durante dos mil dieciséis y dos mil diecisiete, tal y como se advierte de los dos contratos de licenciamiento relacionados con el sistema (**antecedentes 136, inciso c), numerales 5 y 6**), que facultaban a la dependencia a utilizar la referida tecnología durante la vigencia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Respecto a lo anterior, si bien el acta administrativa de entrega-recepción del seis de octubre de dos mil diecisiete actualiza la posesión de los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema, al transferirlos como un bien activo del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, no menos cierto es, que en la misma no se da cuenta sobre la remisión de los documentos que contengan el sistema de gestión de datos personales asociados a dicho sistema, ni la constancia de desinstalación del *software* que habría estado instalado en el *hardware* transferido, máxime que la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas recibió dicho activo cuando el contrato de licenciamiento respectivo aún se encontraba vigente.

Así, tomando en cuenta lo señalado, la afirmación del sujeto obligado en el sentido de que no se localizaron aquellos documentos que den cuenta del tratamiento, seguridad y medidas a considerar para la operación del equipo transferido y que cubrirían los extremos sujetos a verificación notificados en el acuerdo de inicio, relativos al principio de responsabilidad y al deber de seguridad, opera en su contra, en tanto que el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, también formaba parte de la estructura de la entonces Procuraduría General de la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

República³⁵; por lo que, la sujeción de cubrir las obligaciones del sujeto obligado que se presumieron incumplidas en el acuerdo de inicio subsiste y le es exigible, puesto que no se acreditó la desinstalación del sistema, ni las medidas adoptadas para el borrado de la información que se habría generado con dichas operaciones (bases electrónicas en las que debían resguardarse los datos personales recolectados a través del sistema, incluso durante los periodos de prueba estipulados tanto en el anexo técnico del contrato como en los contratos de actualización de licenciamiento mencionados; así como, la bitácora de uso o registro y el formato con protocolos de prueba firmados por los responsables).

Tomando en cuenta lo expuesto, a continuación se determinará si el sujeto obligado incumplió lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de acuerdo a la presunción fundada y motivada que originó el inicio del procedimiento.

QUINTO. Ahora bien, entre los deberes que como sujeto obligado la ahora Fiscalía General de la República está obligada a cumplir, se encuentra el referido **deber de seguridad**, el cual en términos de lo expuesto implica:

- Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Al adoptar medidas de seguridad, deberá considerarse: el riesgo inherente a los datos personales tratados, el desarrollo tecnológico, la sensibilidad de los datos personales tratados, las posibles consecuencias de una vulneración para los titulares, el número de titulares.
- Contar con un **sistema de gestión**, en el que se documenten y contengan las medidas de seguridad para el tratamiento de los datos personales.
- Elaborar un **documento de seguridad** que contenga:
 - El análisis de riesgos.

³⁵ Artículos 3, inciso I), fracción 1, 93 y 94 del Reglamento de la Ley Orgánica de la Procuraduría General de la República.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- El análisis de brecha.
- El plan de trabajo.
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.
- El programa general de capacitación.

Lo anterior resulta relevante en el presente caso, puesto que, si bien la entonces Procuraduría General de la República durante el procedimiento de verificación ofreció en principio, como pruebas para acreditar el cumplimiento al deber de seguridad, dos documentos, después del desahogo de los requerimientos formulados, la actual Fiscalía General de la República precisó que:

- La contratación de la tecnología adquirida es anterior a la entrada en vigor de las disposiciones contenidas en la ley que tutela la protección de datos personales, por lo que los documentos remitidos como pruebas de su parte **no contemplan** el sistema de gestión y/o el documento de seguridad en el caso del sistema para la realización de actividades sustantivas denominado Pegasus, contratado el veintinueve de octubre de dos mil catorce a la empresa Grupo Tech Bull, S.A. de C.V., puesto que se trata de documentos que se asocian a la gestión y seguridad de sistemas diversos al que es motivo de la presente investigación; por lo que los mismos no contemplan el *software* denominado "PEGASUS".
- Estando dentro del plazo fijado por el artículo séptimo transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esto es durante el periodo de 18 meses con que contaba en su calidad de sujeto obligado para tramitar, expedir o modificar su normatividad interna en la materia, **elaboró el documento de seguridad relativo a la tecnología que en la actualidad se encuentra vigente**, sin que se cuente con documento de seguridad diverso.

Así, tomando en cuenta lo manifestado por la Fiscalía General de la República, los documentos remitidos como pruebas a partir de los que pretendió acreditar el cumplimiento al deber de seguridad, **no resultan aplicables, ni guardan relación** con el sistema para la realización de actividades sustantivas denominado Pegasus; por lo que, no son idóneos para acreditar el cumplimiento de la obligación a cargo del sujeto obligado que se presumió incumplida, perdiendo cualquier eficacia probatoria a su favor.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora, si bien es cierto que la tecnología (sistema para la realización de actividades sustantivas denominado Pegasus), se adquirió con anterioridad a la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, no pasa desapercibido que se pudo advertir que dicho *software* estuvo licenciado y con posibilidad de uso también durante dos mil dieciséis y dos mil diecisiete, tal y como se advierte de los dos contratos de licenciamiento relacionados con el sistema (**antecedentes 136, inciso c), numerales 5 y 6**), que facultaban a la dependencia a utilizar la referida tecnología durante la vigencia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y que el **seis de octubre de dos mil diecisiete** la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas recibió los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República.

Así, a través del acta en mención se hizo constar la entrega-recepción del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", por parte del titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia al encargado de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas.

Lo anterior resulta relevante, toda vez que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se publicó en el Diario Oficial de la Federación el veintiséis de enero de dos mil diecisiete, entrando en vigor al día siguiente de su publicación; por lo que, si se considera que al **seis de octubre de dos mil diecisiete** la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas recibió a través de acta entrega el *hardware*; así como, la administración del contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V., como bienes activos de la dependencia, **aún contaba** con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", estando vigente la licencia de uso correspondiente hasta el treinta y uno de diciembre de dos mil diecisiete.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Tomando en cuenta lo anterior, estamos en presencia de actos de tracto sucesivo respecto al manejo de bienes relacionados con el sistema que nos ocupa, lo que asociado al indicio de posible uso, inclusive hasta el dos mil diecisiete como fue parte de la ampliación de investigación en su momento, implica que el manto de tutela respecto a la verificación del cumplimiento del deber de seguridad por parte de dicho sujeto obligado se amplíe en la medida que más favorezca a los intereses de las personas que pudieron haber resentido alguna afectación en sus datos personales.

De esta manera, como la facultad de verificación de este Instituto es de pleno derecho y se ejerce de manera amplia para tutelar la garantía del derecho de protección de datos personales de las personas que pudieron haber sufrido algún tratamiento de sus datos personales a través de la herramienta tecnológica, la falta de elementos por parte del sujeto obligado que permitan desvirtuar la presunción fundada y motivada contenida en el acuerdo de inicio respecto a los incumplimientos a la ley de la materia; así como, la inexistencia de una bitácora de uso, permite la exigencia del cumplimiento del deber de seguridad que nos ocupa, en tanto, que es el piso mínimo exigible para un sistema que recolecta datos como uno de sus fines específicos.

En términos de lo señalado, dado que a través del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", se preveía la recolección de datos personales; así como, la generación de bases electrónicas en las que debían resguardarse los datos personales recolectados a través del sistema, incluso durante los periodos de prueba estipulados tanto en el anexo técnico del contrato como en los contratos de actualización de licenciamiento mencionados; así como, detentar la bitácora de uso o registro y el formato con protocolos de prueba firmados por los responsables, la entonces Procuraduría General de la República debió contar, al menos, con un sistema de gestión y con un documento que contuviera las medidas de seguridad, relacionado con el tratamiento de datos personales a partir de dicha tecnología, máxime que el sujeto obligado refirió la desinstalación del *software* respectivo del *hardware* revisado en la visita de verificación, por lo que, debió salvaguardar la seguridad de los datos personales que se vieron inmersos con el proceso de desinstalación del sistema respectivo.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Sin que sea óbice alegar como lo refiere el sujeto obligado, que los documentos aportados como prueba en su descargo hayan sido generados dentro de los 18 meses posteriores a la entrada en vigor de la ley general, ya que el propio sujeto obligado fue enfático, en un requerimiento posterior a dicho ofrecimiento, en señalar que tales documentos de gestión y de seguridad no contemplaban al sistema Pegasus.

De conformidad con lo expuesto, dado que durante la verificación la Fiscalía General de la República no acreditó contar con dichos elementos (sistema de gestión y con un documento de seguridad asociado con el tratamiento de datos personales a partir de la instalación del sistema Pegasus en equipos bajo su resguardo), es dable concluir que dicho sujeto obligado **incumplió con el deber de seguridad que prevé la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.**

SEXTO. Ahora bien, por lo que respecta al **principio de responsabilidad** que se indicó en el acuerdo de inicio del procedimiento de verificación que nos ocupa, es preciso señalar que derivado del análisis de las constancias y de las diligencias practicadas durante la sustanciación del presente procedimiento, se obtuvieron las consideraciones y conclusiones que a continuación se plantean:

Así, al estar directamente relacionado con lo anterior, se destaca que dicho principio consiste en que el sujeto obligado debe adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y obligaciones establecidos en la ley y rendir cuentas sobre dicho tratamiento. Encontrándose entre dichos mecanismos, los siguientes:

- Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, **de conformidad con las disposiciones previstas en la ley** y en la demás normativa aplicable.
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, **cumplan con las obligaciones previstas en la presente ley** y en la demás normativa aplicable.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

De acuerdo con lo señalado, no pasa inadvertido para este Instituto que respecto del estado actual del sistema para la realización de actividades sustantivas denominado Pegasus, durante la visita de verificación llevada a cabo en la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal, se pusieron a la vista los equipos (*hardware*) en los que estaba instalado el sistema y el sujeto obligado informó que en la actualidad dicho sistema **no está instalado ni registrado** en el *hardware* que obra en dicha unidad.

Así, dado que a través del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", se preveía la recolección de datos personales; así como, la generación por parte de dicho sistema de bases en las que se resguardan dichos datos (incluso durante los periodos de prueba estipulados tanto en el anexo técnico del contrato como en los contratos de actualización de licenciamiento mencionados, así como la generación de protocolos que avalaban dichas pruebas), no debe perderse de vista lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, **respecto de la supresión de datos personales asociados a cualquier tratamiento:**

[...]

Artículo 23. [...]

[...]

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Artículo 24. *El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.*

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

[...]

En relación con lo anterior, en los Lineamientos Generales de Protección de Datos Personales para el Sector Público se establece lo siguiente:

[...]

Artículo 23. *En la supresión de los datos personales a que se refiere el artículo 23, párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de estos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.*

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

- I. Irreversibilidad:** *que el proceso utilizado no permita recuperar los datos personales;*
- II. Seguridad y confidencialidad:** *que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y*
- III. Favorable al medio ambiente:** *que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.*

[...]

De los artículos transcritos se observa que:

- Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento.
- El responsable deberá establecer y documentar los procedimientos para la supresión de los datos personales que lleve a cabo.
- En el establecimiento de las políticas, métodos y técnicas orientadas a la supresión definitiva, el responsable deberá considerar la **irreversibilidad**, la **seguridad y confidencialidad**; así como, que sea **favorable al ambiente**.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Ahora bien, tal y como se ha señalado, en el presente asunto durante la visita de verificación respecto a la desinstalación del sistema para la realización de actividades sustantivas denominado Pegasus, la Fiscalía General de la República destacó que:

- De conformidad con lo establecido en el contrato y su anexo técnico, la instalación del sistema para la realización de actividades sustantivas denominado Pegasus, debió ocurrir dentro de la vigencia del mismo.
- No se localizan registros ni documentos que den cuenta de la desinstalación del sistema para la realización de actividades sustantivas denominado Pegasus, aclarando que con base en el contrato la vigencia del mismo fue al treinta y uno de diciembre de dos mil catorce.

Ahora bien, en relación con lo anterior, de forma orientadora se destaca lo dispuesto en la Guía para el Borrado Seguro de Datos Personales³⁶, en la que se señala lo siguiente:

[...]

8. ¿Cómo borrar de manera segura los datos personales?

La destrucción y borrado de información es un tema de vital importancia para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales, por esta razón, los sujetos obligados deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren. Las técnicas de borrado seguro buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos. De acuerdo a estándares internacionales en la materia, las características para este tipo de destrucción son:

- **Irreversibilidad.** Se debe garantizar que no existe un proceso que permita recuperar la información.
- **Seguridad y confidencialidad.** Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.

³⁶ http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_Borrado_Seguro_DP.pdf#page30 vinculo consultado el veintitrés de enero de dos mil diecinueve.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

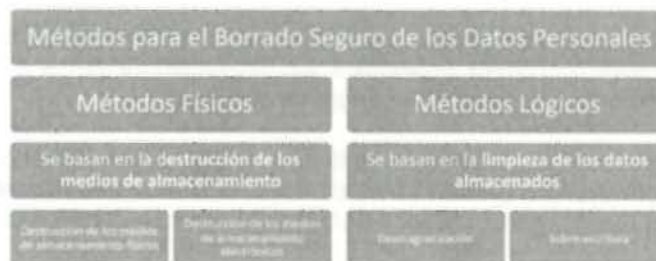
SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

- **Favorable al medio ambiente.** El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente.

A continuación se detallan los diferentes métodos de Borrado Seguro, a fin de que las organizaciones puedan seleccionar aquéllos que mejor se ajusten a sus necesidades (Fig. 6).



8.2 Métodos lógicos de Borrado

Los métodos lógicos son aquellos que implican la sobre-escritura o modificación del contenido del medio de almacenamiento electrónico.

a) Desmagnetización

Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador. Debido a las fuerzas físicas del proceso, es posible que el hardware donde se encuentra la información se vuelva inoperable, por lo que se recomienda aplicar este método si no se volverá a utilizar el medio de almacenamiento.

La desmagnetización se considera más segura que algunos procesos de destrucción física, ya que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo.

La potencia requerida para borrar el dispositivo depende de su tamaño y forma, y para hacer efectivo el borrado, se requiere de una configuración particular para cada medio de almacenamiento. Por la naturaleza del equipo necesario para este proceso, suele utilizarse bajo un esquema de contratación del servicio.

b) Sobre-escritura

Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de **escribir información nueva en la superficie de**



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

El método más simple consiste en realizar una sola sobre-escritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobreescrituras o "pasadas" con variaciones en los caracteres grabados al medio de almacenamiento.

Una ventaja particular de la sobre-escritura es que las herramientas se pueden utilizar para borrar un archivo o carpeta específica, sin necesidad de alterar o detener la operación de todo un medio de almacenamiento o equipo de cómputo.

En la Tabla 3 siguiente se muestran distintos métodos de borrado utilizados por las herramientas de software que existen en el mercado, con su respectiva descripción y nivel de seguridad, donde a mayor grado, mayor nivel de seguridad en el borrado.

Método de borrado	Características de la sobre-escritura aplicada al medio de almacenamiento	Nivel de seguridad
Grado 1. Super Fast Zero Write	1. Valor fijo (0x00) una vez cada 3 sectores	Bajo
Grado 2. Fast Zero Write	1. Valor fijo (0x00) una vez todos los sectores	Bajo
Grado 3. Zero Write	1. Valor fijo (0x00) en todo el área	Bajo
Grado 4. Random Write	1. Valores aleatorios. La fiabilidad aumenta con la cantidad de pasadas	Medio
Grado 5. Random & Zero Write	1. Valores aleatorios 2. Valor fijo (0x00) 3. Valores aleatorios 4. Escritura de valor cero	Medio
Grado 6. US Navy, NAVSO P-5239-26 - MFM. Para discos codificados con MFM (Modified Frequency Modulation)	1. Valor fijo (0xffffffff) 2. Valor fijo (0xbfffffff) 3. Valores aleatorios 4. Se verifica la sobre-escritura	Medio
Grado 7. US Navy, NAVSO P-5239-26 - RLL. Para discos duros y soportes ópticos (CD, DVD, Blu Ray)	1. Valor fijo (0xffffffff) 2. Valor fijo (0x27ffffff) 3. Valores aleatorios 4. Se verifica la sobre-escritura	Medio



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Grado 8. Bit Toggle	<ol style="list-style-type: none"> 1. Valor (0x00) 2. Valor (0xff) 3. Valor (0x00) 4. Valor (0xff) Total de sobre-escrituras: 4	Medio
----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

Método de borrado	Características de la sobre-escritura aplicada al medio de almacenamiento	Nivel de Seguridad
Grado 9. Random Random Zero	<ol style="list-style-type: none"> 1. Dos veces con valores aleatorios 2. Valor fijo (0x00) 3. Dos veces con valores aleatorios 4. Con ceros 	Medio
Grado 10. US Department of Defense (DoD 5220.22-M)	<ol style="list-style-type: none"> 1. Valor fijo determinado 2. Valor complementario (0xff) 3. Valores aleatorios 4. Se verifica la sobre-escritura 	Medio
Grado 11. US Air Force, AFSSI5020	<ol style="list-style-type: none"> 1. Valor fijo (0x00) 2. Valor fijo (0xff) 3. Valor aleatorio constante 4. Se verifica sobre-escritura de un mínimo del 10% del disco 	Medio
Grado 12. North Atlantic Treaty Organization (OTAN) NATO standard	<ol style="list-style-type: none"> 1. Seis veces con valores fijos alternativos entre cada pasada (0x00) y (0xff) 2. Valor aleatorio Total de sobre-escrituras: 7	Alto
Grado 13. Peter Gutmann Secure Deletion	<ol style="list-style-type: none"> 1. Valores aleatorios 4 veces sobre cada sector 2. Valores pseudo aleatorios sobre cada sector por veintisiete pasadas 3. Valores aleatorios durante cuatro pasadas sobre cada sector Total de sobre-escrituras: 35	Alto
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Combina los grados 13 y 10 Total de sobre-escrituras: 35	Muy Alto

Algunos equipos de cómputo y medios de almacenamiento ya contemplan entre sus mecanismos de seguridad, funciones de borrado seguro integradas en su arquitectura.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Para conocer si estas funciones, o bien otras herramientas de software, tienen un nivel de seguridad aceptable, es necesario revisar con el fabricante o en Internet el método de borrado utilizado, así como las características de la sobre-escritura al medio de almacenamiento. Para ello, puede resultar de utilidad la tabla anterior.

c) Cifrado de medios

Cuando un archivo electrónico o medio de almacenamiento se encuentra cifrado, es posible aplicar el denominado "borrado criptográfico" (Cryptographic Erase o CE), para borrar únicamente las claves que se utilizaron para cifrar el medio de almacenamiento o archivo. Esto deja únicamente datos en un formato tal que es imposible obtener información de ellos sin dichas claves.

La efectividad de esta técnica depende:

- *Del tipo de cifrado utilizado en el medio de almacenamiento o archivo.*
- *Del nivel de seguridad del método de borrado aplicado a las claves.*

[...]

9. ¿Cuál es el método de Borrado Seguro más conveniente?

El método de borrado adecuado para cada organización depende de factores tales como su modelo de negocio, el volumen y tipo de datos personales que manejan y el presupuesto con el que cuentan para este procedimiento. A continuación se presentan tres tablas comparativas que pueden permitir decidir sobre el mejor método para su organización.

[...]

9.2 Comparación entre los Métodos Lógicos



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Técnica	Ventajas	Desventajas
Desmagnetización	<ul style="list-style-type: none"> Hace que los datos sean totalmente irrecuperables. Es un método rápido. Permite la eliminación de información aunque el soporte se encuentre dañado. 	<ul style="list-style-type: none"> Implica costos para transportar dispositivos a donde se encuentre el desmagnetizador. El dispositivo deja de ser utilizable. Dificultad para verificar borrado de datos. Dificultad para calcular la potencia requerida para borrar cada equipo. No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. Suele requerir un desmagnetizador por cada tipo de soporte. Se debe tener cuidado para evitar daños a equipos magnéticos cercanos. Personas con ciertas condiciones médicas o que tienen marcapasos deben permanecer alejados. Al ser generalmente una subcontratación, se debe gestionar la entrega de evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción.
Sobre-escritura	<ul style="list-style-type: none"> Facilidad para comprobar la eliminación de la información. Se puede hacer en las instalaciones de la organización. Permite la reutilización de dispositivos. Bajo costo. Prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. 	<ul style="list-style-type: none"> No se puede utilizar en dispositivos dañados. No se puede utilizar en dispositivos que no sean regrabables. No sirve en discos con funciones de gestión de almacenamiento avanzadas.

9.3 Medios de almacenamiento y sus respectivos métodos de borrado seguro



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

Medio de almacenamiento	Tipo de medio	Método de borrado seguro
Medio de almacenamiento físico	<ul style="list-style-type: none">• Archiveros• Gavetas• Bodegas• Estantes• Oficinas	<ul style="list-style-type: none">• Trituración• Incineración• Uso de químicos
Magnético	<ul style="list-style-type: none">• Disco duro• Disco duro externo o portátil• Cintas magnéticas	<ul style="list-style-type: none">• Sobre-escritura• Desmagnetización• Destrucción física
Óptico (dispositivos re-grabables)	<ul style="list-style-type: none">• CD-RW / DVD-RW• Blu-Ray re-gradable (BD-RE)	<ul style="list-style-type: none">• Sobre-escritura• Destrucción física
Magneto-óptico	<ul style="list-style-type: none">• Disco magneto-óptico• MiniDisc• HI-MD	<ul style="list-style-type: none">• Sobre-escritura• Destrucción física
Estado sólido	<ul style="list-style-type: none">• Pendrive / USB• Tarjetas de memoria (Flash drive)• Dispositivo de estado sólido	<ul style="list-style-type: none">• Sobre-escritura• Destrucción física

[...]

De acuerdo con lo anterior, en la guía en comento se establecieron criterios orientadores, a partir de los cuales los sujetos obligados pueden implementar el borrado de datos personales que obran en su posesión, entre los que se destacan los siguientes:

- Los sujetos obligados deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren.
- Las técnicas de borrado seguro buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos.
- Dentro de los métodos lógicos de borrado, los cuales implican la sobre escritura o



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

modificación del contenido del medio de almacenamiento electrónico, se encuentran: la desmagnetización, la sobre escritura y el cifrado de medios.

Así, puesto que durante la verificación la Fiscalía General de la República no acreditó que hubiere diseñado, desarrollado e implementado políticas públicas de conformidad con las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ni garantizó su cumplimiento, al no demostrar, ni acreditar el borrado del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", el cual preveía la recolección de datos personales; así como, de las bases electrónicas generadas por el sistema y los protocolos de prueba en los que debían resguardarse los datos personales recolectados, **incumplió con el principio de responsabilidad**.

SÉPTIMO. Cabe destacar en el presente asunto que no se advirtieron elementos para acreditar que personas específicas u organizaciones hayan sido objetivos de "intentos de infección" del *software* identificado como Pegasus, atribuibles a la entonces Procuraduría General de la República.

Al respecto, tal y como se ha señalado, las notas periodísticas al ser producto de la investigación e interpretación personal de su autor, **únicamente pueden ser consideradas como indicios simples**.

Así, de acuerdo con los criterios intitulados **NOTAS PERIODÍSTICAS, EL CONOCIMIENTO QUE DE ELLAS SE OBTIENE NO CONSTITUYE "UN HECHO PÚBLICO Y NOTORIO"** y **NOTAS PERIODÍSTICAS. ELEMENTOS PARA DETERMINAR SU FUERZA INDICIARIA**, los medios probatorios que se hacen consistir en notas periodísticas, sólo pueden arrojar indicios sobre los hechos a que se refieren; es decir, las notas periodísticas **no constituyen prueba plena**, sino que únicamente constituyen elementos indiciarios sobre los que en ellas refiere y **no son aptas para acreditar por sí mismas que la información que contienen se encuentra apegada a la realidad**.

Lo señalado resulta relevante, puesto aún y cuando se publicaron edictos en el Diario Oficial de la Federación el diecisiete, dieciocho y diecinueve de octubre de dos mil



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

diecisiete; así como, en los diarios de circulación nacional el diecisiete, diecinueve y veinte de octubre de dos mil diecisiete, a efecto de que en el término de 30 días hábiles, contados a partir del día siguiente a la última ubicación, los titulares que habrían resentido alguna presunta afectación comparecieran en el domicilio del Instituto para presentar formalmente su denuncia, manifestar lo que a su derecho convenga, aportar pruebas y señalar un domicilio cierto y determinado para recibir notificaciones, **no se recibieron en este Instituto escritos o manifestaciones de los titulares que tuvieron alguna presunta afectación.**

Así, aún y cuando no se recibieron escritos o manifestaciones de los titulares que tuvieron alguna presunta afectación durante la investigación previa, no puede obviarse la coadyuvancia a este Instituto, recibida por parte de la Red en Defensa de los Derechos Digitales A.C., que compareció durante las diligencias de investigación previa y cuyas manifestaciones y aportaciones fueron consideradas como parte de los elementos que permitieron fundar y motivar el acuerdo de inicio de verificación que originó el presente procedimiento de verificación; sin embargo, no aportó mayores elementos que pudieran acreditar que la entonces Procuraduría General de la República, a través de la Agencia de investigación Criminal habría sido la autora o responsable de los "intentos de infección" descritos en el informe de *The Citizen Lab*.

No obstante lo anterior, a fin de agotar este extremo de los hechos que originaron en su momento la actuación de oficio por parte de este Instituto, como lo fue la posible invasión a la esfera jurídica de protección de datos personales de periodistas y defensores de derechos humanos que se señalaron en el informe de mérito; es preciso indicar que, durante la diligencia del veintiocho de enero de dos mil diecinueve (**antecedente 134**), se localizaron diversas diligencias de cooperación internacional que permitieron recabar el desahogo a un requerimiento realizado a *The Citizen Lab* respecto al informe que publicó, documental de la que no fue posible advertir que se hayan realizado análisis de equipos celulares específicos para su investigación, pues se enfocó únicamente a intentos de infección.

En relación directa con lo descrito, *The Citizen Lab* en desahogo a dicho requerimiento indicó medularmente que tampoco se pudo localizar evidencia de que una agencia gubernamental mexicana instalara el *malware* Pegasus en algún dispositivo, puesto que



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

únicamente advirtió evidencia circunstancial que apoya la hipótesis que sostiene el informe publicado.

De lo anterior, se advierte que no existen elementos que permitan a este Instituto pronunciarse de manera categórica sobre la afectación de personas específicas u organizaciones que hayan sido objetivos por parte del *software* identificado como Pegasus, que adquirió la entonces Procuraduría General de la República.

No obstante, la factibilidad y eficacia del desarrollo de las facultades de verificación por parte de este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el presente caso, con el objeto de corroborar el cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la maximización de los alcances y vigencia de las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, responsables de su tratamiento, cuya vigilancia le está encomendada como organismo autónomo, especializado, imparcial, colegiado, favorece en todo tiempo a las personas la protección más amplia³⁷.

Al respecto, si bien la acreditación de la referida afectación en la esfera particular de cada una de las víctimas de los señalados "intentos de infección" será tarea de la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión; así como, la determinación del responsable de esas intrusiones, este Instituto tiene el deber de tutelar que el manejo de los datos personales que habría sido posible a través del sistema adquirido, en este caso, por la entonces Procuraduría General de la República al poseer tal tecnología para el ejercicio de sus atribuciones, haya sido acorde al mandato legal previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo a los principios y deberes que establece para los responsables frente a los titulares de datos personales cualquiera que éstos sean, más allá de acreditar

³⁷ Décima época, registro: 2015432, instancia: Tribunales Colegiados de Circuito, tipo de tesis: aislada, Gaceta del Semanario Judicial de la Federación, libro 47, octubre de 2017, tomo IV, materia(s): constitucional, tesis: I.7o.A.3 CS (10a.), página: 2444: INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. COMO AUTORIDAD DEL ESTADO, ESTÁ OBLIGADO A PROMOVER, RESPETAR, PROTEGER Y GARANTIZAR LOS DERECHOS HUMANOS, AL INTERPRETAR EL ORDEN JURÍDICO DE SU COMPETENCIA, FAVORECIENDO EN TODO TIEMPO A LAS PERSONAS LA PROTECCIÓN MÁS AMPLIA.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

o tener por acreditados los referidos "intentos de infección" respecto al sujeto obligado verificado.

Se afirma lo anterior, ya que tal y como ha quedado acreditado, el responsable al no contar con un sistema de gestión y con un documento de seguridad, respecto del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS"; así como, no demostrar, ni acreditar el borrado seguro del sistema en comento, el cual preveía la recolección de datos personales y la generación por parte de dicho sistema de bases en las que se resguardan dichos datos y al carecer de una bitácora de uso del sistema, incumplió con el **deber de seguridad** y con el **principio de responsabilidad** establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por lo que su conducta presuntamente actualiza las hipótesis señaladas en el artículo 163, fracciones III, IV, VIII y XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

OCTAVO. Ahora bien, dado que el responsable incumplió con el **deber de seguridad** y con el **principio de responsabilidad**, resulta necesario traer a colación lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de acuerdo con la cual:

[...]

Artículo 163. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

[...]

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, **destruir o inutilizar, total** o parcialmente y **de manera indebida datos personales**, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

[...]

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

XI. Obstruir los actos de verificación de la autoridad.

[...]

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 164. *Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.*

Artículo 165. *Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.*

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

[...]

Artículo 167. *En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un Expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.*

La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción al Instituto o al organismo garante, según corresponda.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto, o el organismo garante que corresponda, deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el Expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto o el organismo garante correspondiente tenga conocimiento de los hechos.

Artículo 168. *En caso de que el incumplimiento de las determinaciones de los Organismos garantes implique la presunta comisión de un delito, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente.*

En términos de los artículos transcritos, serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las siguientes:

- Usar, sustraer, divulgar, ocultar, alterar, mutilar, **destruir o inutilizar**, total o parcialmente y **de manera indebida datos personales**, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

En relación con lo señalado, en el presente caso no debe pasar desapercibido que aún y cuando en junio de dos mil diecisiete la entonces Procuraduría General de la República manifestó a través del comunicado 986/17 que abrió una carpeta de investigación por delitos de intervención de comunicaciones privadas y acceso ilícito a sistemas y equipos de informática y que el seis de octubre de dos mil diecisiete existió una transferencia de los recursos tecnológicos necesarios para la operación y desempeño; así como, los instrumentos jurídicos concatenados con la adquisición, actualizaciones y demás documentos relacionados con el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

República, como bienes activos de la dependencia y con licencia de uso vigente, la ahora Fiscalía General de la República **no acreditó la desinstalación del sistema**, lo cual da cuenta de una destrucción o inutilización de la información que impide a este Instituto verificar y corroborar las afirmaciones de la Fiscalía General de la República.

Aunado a la inexistencia de bases electrónicas en las que debían resguardarse los datos personales recolectados a través del sistema, incluso durante los períodos de prueba estipulados tanto en el anexo técnico del contrato como en los contratos de actualización de licenciamiento mencionados; así como, de la bitácora de uso o registro y el formato con protocolos de prueba firmados por los responsables.

- Dar tratamiento, de manera intencional, a los datos personales **en contravención a los principios y deberes establecidos** en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **No establecer las medidas de seguridad** en los términos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Sobre ambos supuestos, deberá considerarse respectivamente y en lo que atañe a cada uno, que el responsable incumplió con el **deber de seguridad** y con el **principio de responsabilidad** por las consideraciones expuestas en la presente resolución, ya que sin justificación alguna no acreditó contar con un sistema de gestión y con un documento de seguridad, respecto del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS"; así como, no demostrar, ni acreditar el borrado seguro del sistema en comento, el cual preveía la recolección de datos personales y la generación por parte de dicho sistema de bases en las que se resguardan dichos datos, careciendo de una bitácora de uso del sistema.

- **Obstruir los actos de verificación de la autoridad.** Al respecto, considerando que el sujeto obligado manifestó reiteradamente no contar con bitácoras de uso o registros, bases de datos y aplicaciones que dieran cuenta de la utilización del sistema adquirido por la entonces Procuraduría General de la República, ni



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

constancia de su instalación o desinstalación de los equipos en su posesión; a pesar de que con base en los contratos de adquisición y licenciamiento que se describieron en el considerando anterior, debieron existir, se considera que se impidió el ejercicio pleno de las facultades de verificación de este Instituto.

Así, es preciso recordar que en aquellos casos en que el presunto infractor tenga la calidad de servidor público, se deberá remitir a la autoridad competente, junto con la denuncia correspondiente la cual debe estar **dirigida a la contraloría, órgano interno de control o equivalente**, un expediente que contenga todos los elementos que sustenten la presunta responsabilidad administrativa, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y que pudieran constituir una posible responsabilidad.

En razón de lo anterior, puesto que la conducta del responsable presuntamente actualiza las hipótesis contenidas en el artículo 163, fracciones III, IV, VIII y XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se estima procedente **dar vista al Órgano Interno de Control de la Fiscalía General de la República**, con copia certificada del expediente citado al rubro, para que determine las responsabilidades administrativas que pudieran haberse originado en el actuar de los servidores públicos de la entonces Procuraduría General de la República.

Ahora bien, cabe destacar que en el procedimiento de verificación que nos ocupa, se tuvieron a la vista diversos contratos celebrados por la entonces Procuraduría General de la República, que involucran el ejercicio de recursos públicos para la adquisición del sistema materia de investigación y verificación por parte de este Instituto, entre los que se destacan los siguientes:

- Contrato celebrado el veintinueve de octubre de dos mil catorce entre la entonces Procuraduría General de la República y la empresa Grupo Tech Bull, S.A. de C.V.
- Contrato de prestación de servicios de actualización de licenciamiento y de nuevos dispositivos del software, mantenimiento y mejoras en servicios, servidores y estaciones de trabajo de la Plataforma NSO Pegasus, número PGR/AIC/CENAPI/CN/GSN/SERV/001/2017 del siete de junio de dos mil diecisiete,



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

celebrado entre la Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia y la empresa Air Cap, S.A. de C.V. como proveedor.

- Contrato de los servicios de actualización de licenciamiento y nuevos dispositivos del *software*, instalación de un módulo de análisis y las estaciones de trabajo de la Plataforma NSO Pegasus, del cinco de agosto de dos mil dieciséis, celebrado entre la Procuraduría General de la República a través del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia como solicitante y la empresa Proyectos y Diseños VME S.A. de C.V. como proveedor.

En relación con los mismos, el sujeto obligado manifestó durante las diversas diligencias de investigación y verificación que el sistema de mérito no habría sido utilizado e incluso que no tenía documentación que diera cuenta de su instalación específica, razón por la cual se considera que, dadas las atribuciones con las que cuenta la **Auditoría Superior de la Federación**, este Instituto debe dar vista a dicha autoridad con las actuaciones tanto del procedimiento de investigación previa **INAI.3S.08.03-003/2017** como con el de verificación **INAI.3S.07.01-007/2018**, para que verifique los bienes adquiridos y los servicios contratados por la entonces Procuraduría General de la República relacionados con el presente procedimiento de verificación e investigue, en el ámbito de sus atribuciones, los actos u omisiones que impliquen alguna irregularidad, o presunta conducta ilícita o comisión de faltas administrativas, en términos de lo dispuesto en la Ley de Fiscalización y Rendición de Cuentas de la Federación y de la Ley General de Responsabilidades Administrativas, de acuerdo a lo que establece el primero de los ordenamientos en los siguientes artículos:

Ley de Fiscalización y Rendición de Cuentas de la Federación

[...]

Artículo 17.- Para la fiscalización de la Cuenta Pública, la Auditoría Superior de la Federación tendrá las atribuciones siguientes:

[...]

VIII. Verificar obras, bienes adquiridos y servicios contratados por las entidades fiscalizadas para comprobar si los recursos de las inversiones y los gastos autorizados a las entidades fiscalizadas se ejercieron en los términos de las disposiciones aplicables;



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

[...]

XIII. Investigar, en el ámbito de su competencia, los actos u omisiones que impliquen alguna irregularidad o presunta conducta ilícita, o comisión de faltas administrativas, en los términos establecidos en esta Ley y en la Ley General de Responsabilidades Administrativas

[...]

En razón de lo anterior, con fundamento en el artículo 164 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se estima procedente, de igual forma, **dar vista a la Auditoría Superior de la Federación**, con copia certificada de los expedientes referidos, para que determine lo que en derecho corresponda en el ámbito de sus atribuciones.

NOVENO. Por otra parte, considerando que durante la sustanciación del procedimiento de investigación previa **INAI.3S.08.03-003/2017** como en el de verificación **INAI.3S.07.01-007/2018**, el sujeto obligado manifestó reiteradamente no contar con bitácoras de uso o registros, bases de datos y aplicaciones que dieran cuenta de la utilización del sistema adquirido por la entonces Procuraduría General de la República, ni constancia de su instalación o desinstalación de los equipos en su posesión; a pesar de que con base en los contratos de adquisición y licenciamiento que se describieron en el considerando anterior, debieron existir, se considera que estos hechos podrían ser constitutivos del delito de ejercicio ilícito de servicio público, por parte de los servidores públicos del sujeto obligado, establecido en el artículo 214 fracciones IV, V del Código Penal Federal, sin menoscabo de aquellas que pueda determinar la autoridad ministerial:

Artículo 214.- Comete el delito de ejercicio ilícito de servicio público, el servidor público que:

[...]

IV.- Por sí o por interpósita persona, sustraiga, destruya, oculte, utilice, o inutilice ilícitamente información o documentación que se encuentre bajo su custodia o a la cual tenga acceso, o de la que tenga conocimiento en virtud de su empleo, cargo o comisión.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

V.- Por sí o por interpósita persona, cuando legalmente le sean requeridos, rinda informes en los que manifieste hechos o circunstancias falsos o niegue la verdad en todo o en parte sobre los mismos, y

[...]

De esta manera, se considera procedente que este Instituto presente denuncia formal ante el Ministerio Público para que determine lo que en derecho corresponda, de acuerdo a lo que establece el artículo 222 del Código Nacional de Procedimientos Penales, que a la letra dispone, lo siguiente:

[...]

Artículo 222. Deber de denunciar

Toda persona a quien le conste que se ha cometido un hecho probablemente constitutivo de un delito está obligada a denunciarlo ante el Ministerio Público y en caso de urgencia ante cualquier agente de la Policía.

Quien en ejercicio de funciones públicas tenga conocimiento de la probable existencia de un hecho que la ley señale como delito, está obligado a denunciarlo inmediatamente al Ministerio Público, proporcionándole todos los datos que tuviere, poniendo a su disposición a los imputados, si hubieren sido detenidos en flagrancia. Quien tenga el deber jurídico de denunciar y no lo haga, será acreedor a las sanciones correspondientes.

Cuando el ejercicio de las funciones públicas a que se refiere el párrafo anterior, correspondan a la coadyuvancia con las autoridades responsables de la seguridad pública, además de cumplir con lo previsto en dicho párrafo, la intervención de los servidores públicos respectivos deberá limitarse a preservar el lugar de los hechos hasta el arribo de las autoridades competentes y, en su caso, adoptar las medidas a su alcance para que se brinde atención médica de urgencia a los heridos si los hubiere, así como poner a disposición de la autoridad a los detenidos por conducto o en coordinación con la policía.

No estarán obligados a denunciar quienes al momento de la comisión del delito detenten el carácter de tutor, curador, pupilo, cónyuge, concubina o concubinario, conviviente del imputado, los parientes por consanguinidad o por afinidad en la línea recta ascendente o descendente hasta el cuarto grado y en la colateral por consanguinidad o afinidad, hasta el segundo grado inclusive.

[...]



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

En razón de lo anterior, con fundamento en el artículo 168 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se estima procedente, que por conducto de la Dirección General de Asuntos Jurídicos de este Instituto **presente denuncia ante el Ministerio Público Federal**, con copia certificada de los expedientes referidos, para que determine lo que en derecho corresponda en el ámbito de sus atribuciones.

En consecuencia, por lo expuesto y fundado, este Pleno emite las siguientes:

M E D I D A S

Respecto de las medidas resulta importante precisar que, si bien el sujeto obligado incumplió el deber de seguridad y el principio de responsabilidad, dado que en la actualidad el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS", no se encuentra instalado, las mismas deben dirigirse a acreditar dicha situación y documentar su proceso.

PRIMERA. Con fundamento en lo dispuesto en el artículo 150 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se instruye al sujeto obligado para que acredite de manera formal que se ha corroborado que el sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS" ha sido desinstalado del *hardware* en posesión de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal y que dicho *software* no se encuentra instalado en algún equipo en posesión de la ahora Fiscalía General de la República.

SEGUNDA. Con fundamento en lo dispuesto en el artículo 150 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se instruye al responsable para que precise las políticas, métodos y técnicas que dan cuenta de la desinstalación del sistema para la realización de actividades sustantivas de la entonces Procuraduría General de la República denominado "PEGASUS"; así como, que acredite fehacientemente que no es factible instalar nuevamente el *software* adquirido en dos mil



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

catorce y del que tuvo licenciamiento actualizado durante dos mil dieciséis y dos mil diecisiete, en algún equipo en posesión de la ahora Fiscalía General de la República, considerando la irreversibilidad, seguridad y confidencialidad.

En adición a las medidas que deberá adoptar el sujeto obligado respecto al tratamiento de datos personales que obran en su posesión o aquellos que recabe en ejercicio de sus atribuciones y que se identificaron como PRIMERA y SEGUNDA del presente apartado, resulta necesario que remita a este Instituto la expresión documental que acredite que comunicó a sus unidades administrativas que tiene adscritas y que desarrollan actividades sustantivas, la necesidad de adopción de las referidas medidas en el ámbito de su competencia respecto de la totalidad de los sistemas en que lleven a cabo tratamiento de datos personales, debiendo considerar en todos los casos el resguardo de las bases de datos generadas con motivo del uso de ese tipo de tecnología.

Concluido el análisis de los hechos y constancias correspondientes al presente asunto, este Pleno:

RESUELVE

PRIMERO. En razón del incumplimiento detectado al **deber de seguridad** y al **principio de responsabilidad**, en relación con lo previsto por el artículo 163, fracciones III, IV, VIII y XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con fundamento en lo dispuesto en el artículo 164 de la de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, **se da vista** al Órgano Interno de Control de la Fiscalía General de la República, a efecto de que en el ámbito de sus atribuciones determine lo que en derecho corresponda en relación con las responsabilidades administrativas en que pudieron haber incurrido servidores públicos a cargo del sistema Pegasus derivado de los incumplimientos a la ley general ya referidos.

SEGUNDO. Con fundamento en lo dispuesto en los artículos 3, fracción XIII y 28, fracción XVI del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, tórnese el expediente a la Secretaría Técnica del Pleno a efecto de que dé el seguimiento al cumplimiento de las medidas, el cual debe efectuar la **Fiscalía General de la República** en un término de **treinta días hábiles** a partir de la notificación de la presente resolución.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE EVALUACIÓN INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PÚBLICO

EXPEDIENTE: INAI.3S.07.01-007/2018

TERCERO. De conformidad con lo dispuesto en el artículo 12, fracción XXXVI del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la presente resolución se hará pública por lo cual se instruye a la Secretaría de Protección de Datos Personales, de este Instituto para que elabore la versión pública respectiva, eliminando aquella información clasificada por ser información que identifique o haga identificable a las personas físicas y la confidencialidad de las personas morales, en términos de los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública y 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública; y una vez hecho lo anterior, dicha resolución sea remitida a la Secretaría Técnica del Pleno para que, previa revisión, se publique en la página de internet del Instituto.

CUARTO. Se hace del conocimiento del responsable que, con fundamento en los artículos 152 y 168 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; así como, 217 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, este Instituto podrá imponer las medidas de apremio que correspondan en caso de incumplimiento a la presente resolución.

QUINTO. El presente expediente puede ser consultado en el domicilio del Instituto, ubicado en avenida insurgentes Sur, número 3211, colonia Insurgentes Cuicuilco, Coyoacán, Código Postal 04530, en la Ciudad de México, en la Dirección General de Evaluación, Investigación y Verificación del Sector Público.

SEXTO. Remítase copia certificada de la presente resolución y de los expedientes de investigación previa **INAI.3S.08.03-003/2017** y de verificación **INAI.3S.07.01-007/2018** a la Dirección General de Asuntos Jurídicos de este Instituto, para que en el ámbito de sus atribuciones presente la denuncia correspondiente al Ministerio Público referida en el considerando **NOVENO** de la presente resolución.

SÉPTIMO. Notifíquese la presente resolución por conducto de la Secretaría de Protección de Datos Personales al responsable; así como, al Órgano Interno de Control de la Fiscalía General de la República y a la Auditoría Superior de la Federación, para efectos de las vistas ordenadas.



Instituto Nacional de Transparencia,
Acceso a la Información y
Protección de Datos Personales

**INSTITUTO NACIONAL DE TRANSPARENCIA,
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE
DATOS PERSONALES**

**SECRETARÍA DE PROTECCIÓN DE DATOS
PERSONALES**

**DIRECCIÓN GENERAL DE EVALUACIÓN
INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR
PÚBLICO**

EXPEDIENTE: INAI.3S.07.01-007/2018

Así, por unanimidad, lo resolvieron y firman los comisionados presentes del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Francisco Javier Acuña Llamas, Oscar Mauricio Guerra Ford, Blanca Lilia Ibarra Cadena, María Patricia Kurczyn Villalobos, Rosendoevgueni Monterrey Chepov y Joel Salas Suárez, en sesión celebrada el veinte de febrero de dos mil diecinueve, ante el Secretario Técnico del Pleno y el Secretario de Protección de Datos Personales.



Francisco Javier Acuña Llamas
Comisionado presidente



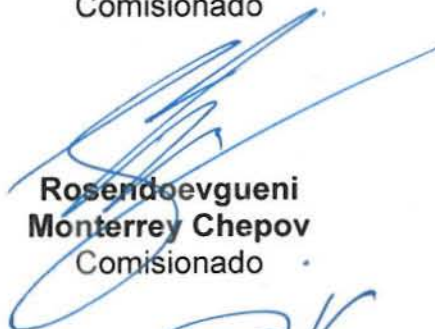
**Oscar Mauricio Guerra
Ford**
Comisionado



**Blanca Lilia Ibarra
Cadena**
Comisionada



**María Patricia Kurczyn
Villalobos**
Comisionada




**Rosendoevgueni
Monterrey Chepov**
Comisionado



Joel Salas Suárez
Comisionado



Hugo Alejandro Córdova Díaz
Secretario Técnico del Pleno



Jonathan Mendoza Iserte
Secretario de Protección de Datos
Personales

