RECOMENDACIONES

PARA EL CUMPLIMIENTO DEL

DEBER DE CONFIDENCIALIDAD

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Josefina Román Vergara
Comisionada

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

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530, Ciudad de México.

Edición, octubre de 2023

ÍNDICE

DEFINICIONES Y ABREVIATURAS

Las siguientes definiciones se retoman de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Diccionario de Protección de Datos Personales[1], la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales[2] y el Glosario de términos de ciberseguridad del Instituto Nacional de Ciberseguridad del Ministerio de España.[3]

Activo

Es cualquier información o sistema relacionado con el tratamiento de esta, que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.[4]

1 INAI, Coord. Davara F. de Marcos Isabel, Diccionario de Protección de Datos Personales. Primera Edición, diciembre 2019. México. Disponible en: http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf última fecha de consulta: 29 de agosto de 2023

2 INAI, (2015, junio), Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, Consulta realizada el 25/04/2022. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

3 INCIBE, Glosario de Términos de Ciberseguridad, una guía de aproximación para el empresario. Disponible para su consulta en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

4 Recomendaciones en materia de seguridad de datos personales, DOF, disponible en: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179 última fecha de consulta: 29 de agosto de 2023.

Amenaza	Se define como la circunstancia o evento con la capacidad de causar daño a una organización. Es aquella circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que exista una vulnerabilidad o debilidad de los sistemas aprovechando su existencia, puede derivar en un incidente de seguridad.
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Custodios	Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.
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.
Documento de seguridad	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
Encargado	La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LGPDPPSO o Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales o LGPDPSP	Lineamientos Generales de Protección de Datos Personales para el Sector Público.
Medidas de seguridad administrativas	De acuerdo con el artículo 3, fracción XXI de la LGPDPPSO, son políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.
Organización	Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.
Responsable	Los sujetos obligados a que se refiere el artículo 1° de la Ley General que deciden sobre el tratamiento de datos personales.
Riesgo	Combinación de la probabilidad de un evento y su consecuencia desfavorable.
Identificar el riesgo	Proceso para encontrar, enlistar y describir los elementos del riesgo.
Valorar el riesgo	Proceso para asignar valores a la probabilidad y consecuencias del riesgo (impacto).
Tratar el riesgo	Procesos que se realizan para modificar el nivel de riesgo.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.
Confidencialidad	Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.
Disponibilidad	Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.
Integridad	La propiedad de salvaguardar la exactitud y completitud de los activos.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP)	Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.
Sujeto Obligado	Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley General y los Lineamientos Generales, incluyendo al INAI y los organismos garantes.
Titular	La persona física a quien corresponden los datos personales.
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.
Trazabilidad	Cualidad que permite, a través de un sistema automatizado para la gestión documental y administración de archivos, identificar el acceso y la modificación de documentos electrónicos.

INTRODUCCIÓN

Las presentes recomendaciones buscan orientar a los sujetos obligados en el cumplimiento efectivo del deber de confidencialidad a que refiere el artículo 42 de la LGPDPPSO y el artículo 71 de los Lineamientos Generales, los cuales prevén que el responsable del tratamiento debe establecer controles o mecanismos que tengan por objeto que las personas que intervengan en cualquier fase del tratamiento de datos personales dentro de la entidad, guarden la confidencialidad respecto de éstos, obligación que debe subsistir aun después de finalizar la relación de las personas intervinientes con el sujeto obligado.

En ese sentido, en primera instancia se pretende que, los sujetos obligados comprendan qué es el deber de confidencialidad para posteriormente abordar algunas propuestas de medidas de seguridad que pueden ser aplicadas, de acuerdo con el contexto de cada Institución, para el cumplimiento de dicho deber.

Para abordar el deber de confidencialidad, se debe comprender qué es la confidencialidad. De acuerdo con la Real Academia Española de la lengua, la confidencialidad es la cualidad de confidencial,[5] por su parte la definición de confidencial es que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho.

De acuerdo con el Diccionario de Protección de Datos Personales, conceptos fundamentales, del INAI, al definir el deber de confidencialidad se indica:

> *"**La confidencialidad es la propiedad que posee un objeto, acción, pensamiento, idea, información o cualquier ente de no ser divulgado o expuesto a entidades no autorizadas**.*
>
> *En el caso de la información**, constituye una de las piedras angulares junto con la integridad y la disponibilidad de lo que es la seguridad de la información**, características conocidas como la triada de la seguridad.*
>
> *Por otro lado, **el deber de confidencialidad es la obligación que tiene una entidad de resguardar la confidencialidad de lo que tiene bajo responsabilidad***

5 Real Academia Española, Diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. https://dle.rae.es/confidencilidad Fecha de consulta 02/02/2023.

***o custodia**. En algunas profesiones como la medicina, el derecho, la psicología, el periodismo o la milicia, se considera un principio ético o de secreto profesional."* [6]

Es importante considerar que la confidencialidad la podemos ubicar como una de las tres propiedades o pilares de la información en materia de seguridad de la información.

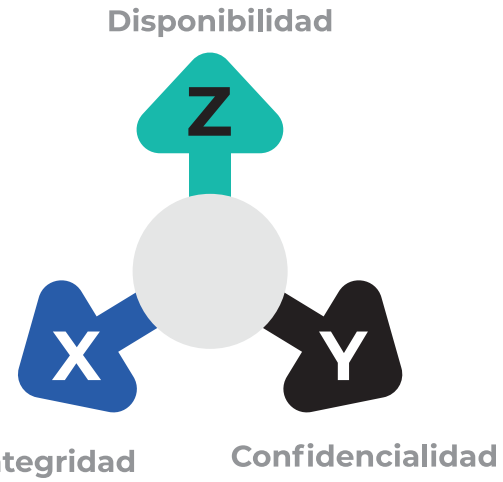

Ilustración 1. Dimensiones de la seguridad de la información.[7]

La confidencialidad entonces es aquella propiedad o característica que consiste en que terceros no autorizados accedan a información, ahora bien, existen supuestos donde por obligación legal, atribuciones, facultades o contratos de prestación de servicios, ciertas personas deben acceder a información personal, por lo que la confidencialidad recae en que dicha información se mantenga en secreto y no se divulgue a terceros.

Se debe tener en cuenta que no toda la información es confidencial o debe gozar de dicha propiedad, particularmente en el sector público, ya que, la información generada por los sujetos obligados está regulada por las leyes de transparencia y acceso a la información; así como por las leyes de protección de datos personales. En ese sentido, los datos personales de particulares y en gran mayoría de los servidores públicos (aquellos datos que nada tienen que ver con su cargo y ejercicio de sus funciones), es considerada información confidencial.

Así, los datos personales son datos confidenciales por su naturaleza, salvo que exista alguna condición legal que señale lo contrario, por ello, se debe proteger el acceso, uso y divulgación por terceros no autorizados, y evitar el uso indebido, la difusión o divulgación no consentida por parte de aquellas personas autorizadas para tratarlos, es decir, se debe asegurar, que quienes están facultados para tratar los datos personales, lo hagan en apego a la normativa en la materia y cumpliendo los deberes y principios que esta contiene.

Una vez que se ha dicho que una de las dimensiones de la seguridad de la información es la confidencialidad, es importante tener en cuenta que la implementación de las medidas de seguridad de la información dentro de las que se abordan los mecanismos para guardar la confidencialidad, se deben dar

6 INAI, Coord. Davara F. de Marcos, Isabel; Diccionario de Protección de Datos Personales, Conceptos Fundamentales. Primera Edición, diciembre 2019. México. Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

7 Instituto Nacional de Ciberseguridad, (INCIBE), Protección de la información, Colección Protege tu empresa. Ministerio de Asuntos Económicos y Transformación Digital de España, p 6.

bajo un enfoque multidisciplinario, en el cual es necesaria la participación activa de personal del área o unidad administrativa de tecnologías de la información y comunicaciones, de sistemas o de seguridad de la información (u homóloga) particularmente para la adopción de medidas técnicas; aunado a ello, se requiere la colaboración de todas la áreas y personas servidoras públicas de la entidad que tengan atribuciones para tratar datos personales, a fin de que propongan, e instrumenten las medidas de seguridad para su efectivo cumplimiento.

Lo anterior es así, ya que en materia de seguridad de la información y particularmente en el derecho a la protección de datos personales, convergen múltiples materias, como la tecnología, el derecho, la ética, entre otras, y por ello se requiere que cada profesional colabore en la seguridad de los activos de información,[8] y en especial los que contienen datos personales, de acuerdo con su área de especialidad.

Sumado a lo anterior, se debe recordar que el cumplimiento de obligaciones corresponde al sujeto obligado como responsable de tratamiento, por supuesto con la guía y asesoría del Comité de Transparencia y de la Unidad de Transparencia.[9]

8 Recomendaciones en materia de seguridad de datos personales, DOF, disponible en: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179 última fecha de consulta: 29 de agosto de 2023.

9 Artículos 83, 84 y 85 de la LGPDPPSO.

DEBER DE CONFIDENCIALIDAD EN LA LEY GENERAL Y LOS LINEAMIENTOS GENERALES

La LGPDPPSO señala respecto al deber de confidencialidad:

Artículo 42.

> El responsable **deberá establecer controles o mecanismos** que tengan por objeto que **todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad** respecto de éstos, obligación que subsistirá **aún después de finalizar sus relaciones con el mismo**.
>
> **Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.**

En ese sentido, la confidencialidad es un deber a cargo del responsable del tratamiento que consiste en implementar medidas de seguridad para que cualquier persona que intervenga en el tratamiento de los datos personales en cualquiera de sus fases, los mantenga resguardados y se abstenga de divulgarlos.

Por su parte, los Lineamientos Generales, establecen:

> Deber de confidencialidad.
> Artículo 71. **El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo**.
>
> Cumplimiento de los deberes de seguridad y confidencialidad.
> Artículo 72. **La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente Capítulo, recaerá, en todo momento, en el responsable**.

En ese sentido, la Ley y los Lineamientos Generales obligan al responsable a cumplir con el deber de confidencialidad, teniendo en todo momento la carga de probar dicho cumplimiento.

Así, **el deber de confidencialidad** de acuerdo con una lectura armónica de la Ley General **busca combatir el escenario de vulneración en el que se realice un tratamiento indebido, particularmente, el uso y divulgación no autorizados de los datos personales, que puedan realizar los involucrados en el tratamiento de los datos personales, entiéndase de manera enunciativa más no limitativa, empleados, personas servidoras públicas, ya sea de estructura, de prestación de servicios profesionales o bien, que presenten algún servicio externo (encargados o terceros receptores de transferencias), del sujeto obligado, que tienen atribuciones para tratarlos, durante el tiempo que dure la relación que tengan estos con el sujeto obligado, y después de que esta finalice; en el entendido de que dichos escenarios conllevan la pérdida total de la confidencialidad, y pueden derivar en otros tratamientos indebidos y con grave impacto para las personas titulares de los datos personales, como pueden ser la suplantación de identidad, o el daño a su patrimonio o reputación.**

Ahora bien, este deber se consolida con las medidas de seguridad, controles o mecanismos que, en su caso, implemente el responsable del tratamiento y que sean acordes a los alcances establecidos, tanto temporales como subjetivos; es decir, dirigidos a todas las personas involucradas, incluidas sus relaciones con terceros y encargados, a fin de evitar la falta de discreción o deber de secrecía que deben tener estos en los tratamientos de datos durante y después de finalizar las relaciones jurídicas que tengan con el sujeto obligado.

En ese sentido, para implementar las medidas y controles idóneos que tengan el alcance requerido por el artículo 42 de la LGPDPSO, el responsable del tratamiento debe prever algunos escenarios de riesgo como pueden ser:

- **Que personal autorizado para el tratamiento (personal que intervenga) interno o externo, use o divulgue los datos personales mientras exista la relación con el sujeto obligado, o bien cuando esta finalice.**

- **Que, en el supuesto de transferencias o encargos del tratamiento, sean a esos terceros o encargados a quienes les vulneren los datos personales, o ellos mismos los vulneren, y dicha vulneración consista particularmente en el uso o divulgación indebida, bien mientras existe la relación jurídica o posterior a ella.**

DEBER DE CONFIDENCIALIDAD. RELACIÓN CON EL DEBER DE SEGURIDAD, EL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES Y EL DOCUMENTO DE SEGURIDAD

Previo a ahondar en la relación entre el deber de confidencialidad y el SGSDP, es importante comprender que el deber de confidencialidad y el deber de seguridad están directamente relacionados.

Para entender el conjunto de obligaciones que debe cumplir el sujeto obligado como responsable del tratamiento de datos, primero se tiene que comprender que todas las responsabilidades están relacionadas, por lo que se recomienda leer la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales[10] y las Recomendaciones para la elaboración de políticas internas de gestión y tratamiento de datos personales (Sector Público).[11]

El deber de seguridad de acuerdo con el artículo 31 de la LGPDPPSO, es la implementación y mantenimiento de controles, políticas y medidas de seguridad de carácter físico, técnico y administrativo por parte del responsable del tratamiento, que aseguren o garanticen la confidencialidad, integridad y disponibilidad de los datos personales, protegiéndolos contra daños, pérdidas, alteración, destrucción o su uso, tratamiento y acceso no autorizado.

El cumplimiento del deber de seguridad es fundamental para el cumplimiento del

10 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, junio 2015. https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf consultado el 09 de septiembre de 2023.

11 Recomendaciones para la elaboración de políticas internas de gestión y tratamiento de datos personales (Sector Público), RecomendacionesPolíticasPDP.pdf (inai.org.mx) consultado el 29 de agosto de 2023.

deber de confidencialidad, sin embargo, la Ley General particularizó un escenario de vulneración, es decir, la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, o tratamiento no autorizado, el daño, la alteración o modificación no autorizada,[12] en este caso **por terceros autorizados, es decir por personas que, están habilitadas o facultadas para tratarlos, ya que intervienen en alguna fase del tratamiento**,[13] a fin de que los sujetos obligados lo atendieran específicamente.

Ahora bien, un sistema de gestión de seguridad de datos personales *es el 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 Ley General y las demás disposiciones que le resulten aplicables en la materia*, de acuerdo con el artículo 34 de la LGPDPPSO.

Por su parte, el Documento de Seguridad es el *instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee* (artículo 3, fracción XIV de la LGPDPPSO).

Tanto el Sistema de Gestión de Seguridad de Datos Personales como el Documento de Seguridad son instrumentos obligatorios que debe tener el responsable para cumplir con el deber de seguridad. Su objetivo es realizar y documentar los análisis establecidos en el artículo 35 de la LGPDPPSO, implementar estándares nacionales e internacionales y metodologías para la gestión del riesgo, a fin de establecer las medidas de seguridad a implementar para la protección de los datos personales, y sistemas de tratamiento, lo que engloba proteger su confidencialidad.

Así, para el cumplimiento del deber de seguridad y por lo tanto también para el de confidencialidad, la LGPDPPSO impone la obligación a los responsables del tratamiento de implementar un Sistema de Gestión de Seguridad de Datos Personales, así como elaborar un documento de seguridad. Lo que buscan ambas obligaciones es garantizar que el responsable implemente y opere medidas de seguridad constantemente para proteger los datos personales y por lo tanto su confidencialidad, consolidando un sistema de mejora continua.

Sin embargo, la Ley General también impone la obligación de demostrar en lo particular el cumplimiento al deber de confidencialidad, por lo que se deberán identificar los controles o medidas de seguridad específicas que hayan resultado de los procesos para la implementación

12 Artículo 38 de la LGPDPPSO. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:
I. La pérdida o destrucción no autorizada.
II. El robo, extravío o copia no autorizada.
III. El uso, acceso o tratamiento no autorizado.
IV. El daño, la alteración o modificación no autorizada.

13 Artículo 42 de la LGPDPPSO. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas **personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos**, obligación que subsistirá aún después de finalizar sus relaciones con el mismo. **Se hace referencia particularmente a las personas que intervienen en cualquier fase del tratamiento.**

del Sistema de Gestión y del documento de seguridad,[14] (particularmente del análisis de brecha donde se analizarán los controles existentes y los que faltan por implementarse, y del plan de trabajo, en el que se proyectará la implementación de las medidas de seguridad faltantes) respecto a la confidencialidad y en particular respecto a las amenazas de tratamientos no autorizados, como daño, alteración o modificación, por terceros autorizados para el tratamiento.

Lo anterior se fortalece si tomamos en cuenta que dentro de los estándares internacionales publicados por la Organización Internacional para la Estandarización (ISO), particularmente la familia de estándares publicados con la Comisión Electrotécnica Internacional (IEC), en particular la serie denominada ISO/IEC 27000 de estándares de seguridad, que contiene las mejores prácticas recomendadas en materia de seguridad de la información, el estándar ISO/IEC/27001 para gestionar la Seguridad de la Información, así como la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España en su versión 3.0,[15] entre otros documentos, consideran como amenaza el robo de documentación, el robo de equipos o soportes de información, así como el riesgo que representa el incumplimiento de las leyes aplicables a las Organizaciones, amenazas que se traducen en riesgos que pueden ser ocasionados por personas externas como hackers, crackers, ciberdelincuentes y terroristas, **pero que también pueden ser ocasionados por personal interno de las organizaciones**, debido a la falta de capacitación y sensibilización en la protección de datos personales o de la seguridad de la información en general, o por negligencia, por curiosidad, o bien intencionadamente, por venganza de empleados molestos, conflicto de intereses, entre otros supuestos.

En ese sentido, las mismas normas de estandarización, como la ISO/IEC/27005, y las distintas metodologías para la implementación de los Sistemas de Gestión de Seguridad de la Información incorporan en sus catálogos controles para mitigar o reducir el riesgo de las amenazas que atentan contra la confidencialidad causadas por los propios empleados de una organización, como lo son el control de acceso tanto físico como lógico, la seguridad de las comunicaciones, por ejemplo políticas para compartir información a través del correo electrónico, los acuerdos, cláusulas o cartas de confidencialidad y el cumplimiento de las leyes aplicables a las organizaciones, en este caso, las de protección de datos personales.

14 Se refiere al proceso de gestión de riesgos: análisis de riesgos donde se deben identificar las vulnerabilidades, amenazas a las que son susceptibles los datos personales, y cómo estas se conjuntan para generar escenarios de vulneración, así como la probabilidad de ocurrencia y su impacto en los titulares de los datos personales.

15 La metodología MAGERIT 3.0. de Análisis y Gestión de Riesgos de los Sistemas de Información, elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN), consta de 3 Libros, disponibles para su consulta, en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

RECOMENDACIONES PARA EL CUMPLIMIENTO DEL DEBER DE CONFIDENCIALIDAD

El sujeto obligado como responsable del tratamiento deberá establecer medidas de seguridad o controles específicos para el cumplimiento del deber de confidencialidad. En ese sentido, se propone que realicen protocolos o bien acciones para su cumplimiento y documentación.

Es importante precisar, que estas recomendaciones son propuestas que pueden realizar potestativamente los responsables del tratamiento, incluso aplicando o no, lo que de acuerdo a su contexto, objetivos, funciones, y capacidad en materia de recursos administrativos, económicos y humanos les sea conveniente; sin embargo, en caso de que el Órgano Garante realice verificaciones, deberán en todo momento, demostrar el cumplimiento del deber de confidencialidad, teniendo la carga probatoria como lo señala el artículo 72 de los Lineamientos Generales,[16] por lo que deberán documentarse las acciones que se generen para el cumplimiento de dicho deber.

Al respecto se realizan las siguientes recomendaciones para cumplir con el deber de confidencialidad:

I. Identificar dentro de los flujos de datos personales las funciones y obligaciones de las personas que los tratan

Como se puede observar, este paso también es parte del contenido del Documento de Seguridad, por lo que también es posible reutilizarlo; sin embargo, en este punto se recomienda ser exhaustivos en cuanto a identificar a todo el personal no solamente que participe en el flujo del dato personal, es decir que recabe, almacene, manipule o resguarde, sino que por alguna razón pueda tan solo acceder a él, incluso solo observarlos; esto es así, puesto que será indispensable para que en caso de vulneración, robo de información, o divulgación pueda documentarse de manera detallada, por donde transitaron los datos personales, quien tuvo acceso a ellos, quién los modificó, **esto es, que se pueda observar su trazabilidad.**

16 Artículo 72 de los LGPDPSP La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente Capitulo, recaerá, en todo momento, en el responsable.

De acuerdo con el diccionario de protección de datos, conceptos fundamentales, se entiende por trazabilidad: la cualidad que permite, a través de un sistema automatizado para la gestión documental y administración de archivos, identificar el acceso y la modificación de documentos electrónicos.[17]

En ese sentido el identificar los datos personales, así como el personal que tiene acceso a ellos, será una medida fundamental ya que es la base para combatir la amenaza de divulgación de datos personales por personal interno de la Organización, puesto que con ello se tendrá identificado al personal que los trata y al que opera los sistemas de tratamiento, por lo que, será importante que dicho documento contemple incluso a personal que presta servicios profesionales, proveedores de servicios, entre otros, que sin ser servidores públicos tengan acceso a ellos.

Una vez establecidas las funciones y obligaciones, será más fácil identificar las medidas de seguridad que se pueden incorporar incluso las enfocadas hacia dicho personal. Por ejemplo, establecer capacitación especializada al personal identificado como una medida de seguridad administrativa.

Aunado a lo anterior, debemos recordar que el artículo 57 de los LGPDPSP, establece la obligación de considerar roles y responsabilidades:

> *Artículo 57. Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*

A tal efecto, es importante que el sujeto obligado tome en consideración que para designar roles y responsabilidades en materia de seguridad y protección de datos personales, puede retomar su estructura organizacional a fin de establecer las funciones y obligaciones generales en materia de seguridad de los datos personales, y asignar los roles, perfiles y privilegios dependiendo del tratamiento, y del o los activos de información y de apoyo de que se traten, así como del nivel de responsabilidad particular en materia de seguridad de los datos personales que tienen sobre ellos, tomando en cuenta que entre mayor sea la jerarquía del puesto, mayores responsabilidades hacia el tratamiento de datos personales tendrán.

Los roles que decida designar serán acordes a las necesidades del tratamiento del sujeto obligado, es decir, puede que les sea posible contratar nuevos perfiles considerados como especialistas en materia de seguridad de la información y de datos personales; sin embargo, se debe recordar que la propia LGPDPPSO obliga a los responsables del tratamiento a destinar recursos para instrumentar políticas y programas de protección de

17 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI, coord. Davara F. de Marcos, Isabel. Diccionario de Protección de Datos Personales, Conceptos Fundamentales. Página 76.

datos personales,[18] asimismo, recomienda a los responsables que realicen tratamientos de datos intensivos o relevantes, designar a un Oficial de Protección de Datos Personales, a fin de que asesore al sujeto obligado en la materia.

II. Medidas de Seguridad para cumplir con el deber de confidencialidad

A. Medidas de seguridad administrativas

A.1 Integrar el deber de confidencialidad en la Política General de Gestión y Tratamiento de Datos Personales y crear políticas respecto de los controles que se vayan a implementar que tengan relación con el deber de confidencialidad

Es importante que el deber de confidencialidad se incluya en la Política General de Gestión y Tratamiento de Datos Personales. Se debe recordar que el artículo 33 de la LGPDPPSO señala:

> *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;*
> *(...)*

Por su parte los Lineamientos Generales establecen al respecto:

> *Contenido de las políticas internas de gestión y tratamiento de los datos personales*
> *Artículo 56. Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable* ***deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente****:*
>
> *I.. El* ***cumplimiento de todos los principios, deberes****, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales.*
> *II. os roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen.*
> *III.* ***Las sanciones en caso de incumplimiento****.*
> *IV. La identificación del ciclo de vida de los datos personales respecto de cada*

18 Artículo 30 fracción I de la LGPDPPSO.

tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

V. *El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.*
VI. *El proceso general de atención de los derechos ARCO.*

En relación con lo anterior, se debe tener claro que la política debe contener **el cumplimiento del deber de confidencialidad, así como la sanción correspondiente en caso de incumplimiento, aunado a esto, se recomienda que también establezca las medidas de seguridad que se aplican dentro del sujeto obligado para el cumplimiento de dicho deber, en un sentido general**, (véase el apartado V. donde se recomienda la implementación de algunas medidas respecto al deber de confidencialidad).

Asimismo, es muy importante señalar dentro de la misma, **que el deber de confidencialidad, no culmina con la terminación del puesto, cargo o comisión, es decir que una vez que la persona deja de ser empleada, el deber de confidencialidad se mantiene** por obligación legal conforme al párrafo primero del artículo 42 de la Ley General.

Se debe precisar que la o las Políticas deben centrarse en el qué y no en el cómo, esto es, que deben centrarse en qué se debe proteger (los datos personales y sistemas del tratamiento), quién debe protegerlos, qué puede realizarse y que está prohibido, así como las sanciones o responsabilidades en caso de incumplimientos; no así en el cómo, ya que esto puede traducirse en procedimientos internos específicos por cada unidad administrativa.

Respecto a las sanciones por incumplimiento del deber de confidencialidad, debe tenerse en cuenta que la LGPDPPSO establece en su artículo 163:

Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
II. *Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.*
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.

V. *No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia.*

VI. *Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.*

VII. ***Incumplir el deber de confidencialidad establecido en el artículo 42 de 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.*

IX *Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley.*

X. *Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley.*

XI. *Obstruir los actos de verificación de la autoridad.*

XII. *Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley.*

XIII. *No acatar las resoluciones emitidas por el Instituto y los Organismos garantes.*

XIV. *Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.*

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.

Se debe considerar que, ante un incumplimiento a la Ley General, que tenga como consecuencia una vulneración a la seguridad de los datos y que dañe significativamente a personas titulares, existen tres supuestos en los que el Instituto tiene facultades para iniciar una verificación al responsable del tratamiento; el primero, que el propio sujeto obligado conforme al artículo 40 de la LGPDPPSO y 67 de los Lineamientos Generales, informe al Instituto sobre el incidente de seguridad, la segunda; por denuncia de la persona o personas titulares que se consideren afectadas por la vulneración, o bien, de

oficio, cuando el propio Instituto cuente con indicios que hagan presumir fundada y motivadamente la existencia de violaciones a las leyes correspondientes.

Dicho procedimiento se realiza a fin de observar si el sujeto obligado cuenta con medidas o mecanismos suficientes para cumplir con principios y deberes. En ese sentido, de observarse durante la verificación que la vulneración puede atribuirse al sujeto obligado, el propio Instituto da vista al Órgano Interno de Control a fin de que inicie las acciones conducentes, de estimarlo pertinente.

Lo anterior no obsta para que, el propio sujeto obligado pueda llevar a cabo las acciones que crea correspondientes en el caso de tener identificada a la persona que haya incumplido la legislación en la materia así como las políticas de seguridad de la entidad (donde se incluye el deber de confidencialidad).

Asimismo, debe precisarse que los incumplimientos de la Ley General pueden derivar en faltas administrativas, delitos y responsabilidades civiles, 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.

Ahora bien, para que las políticas de gestión y tratamiento de datos personales, así como las de seguridad de la información sean útiles, deben hacerse del conocimiento de todos los servidores públicos y personal que por algún motivo trate datos personales a cargo del sujeto obligado, por lo que **se recomienda que, a su ingreso en el puesto o encargo, o la firma del contrato de prestación de servicios se les brinde copia de estas, donde se firme su recepción, lectura y entendimiento**.

De igual manera, será importante que se comuniquen a las personas servidoras públicas que actualmente laboran en la entidad, y se sugiere solicitar firma de recepción y entendimiento.

A.2 Políticas y procedimientos de controles que integren el deber de confidencialidad

Además de incorporarse el deber de confidencialidad a la política general, tiene que considerarse que será importante que se creen políticas y procedimientos técnicos complementarios a la o las políticas generales, los cuales describen a fondo y de manera técnica algunos controles como por ejemplo podría ser una política de control de accesos físicos y técnicos, la política de escritorios limpios y el manual o política de uso aceptable de soportes.

En ese sentido, es necesario que, todas las políticas y procedimientos se hagan del conocimiento o se comuniquen al personal adecuado para su cumplimiento; por ejemplo,

las generales a todas las personas que integran el sujeto obligado, incluidos prestadores de servicios y proveedores, y las políticas técnicas a quienes operen el tratamiento específico.

A.3 Capacitación especializada a los servidores públicos y personal externo como proveedores de servicios que por algún motivo tengan acceso a datos personales

La capacitación del personal en las organizaciones constituye una medida de seguridad fundamental si no es que la más importante, ya que de nada sirve contratar o enfocar recursos a medidas de seguridad sumamente complejas y técnicas para la protección de los datos personales, si quienes las operan no están capacitados en seguridad de la información y protección de datos personales; muchas veces las amenazas se encuentran dentro de la entidad, donde los propios empleados por errores, negligencia o pueden divulgar y realizar un mal tratamiento de datos personales.

Al respecto el especialista en seguridad de la información, y uno de los hackers más famosos del mundo, Kevin Mitnick ha señalado que "*Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores*".[19]

En virtud de lo anterior, la capacitación y sensibilización del personal en materia de protección de datos personales y seguridad de la información, constituye una medida de seguridad administrativa fundamental, conforme al artículo 3, fracción XXI de la LGPDPPSO.

De acuerdo con el artículo 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el sujeto obligado debe diseñar y aplicar distintos niveles de capacitación, de acuerdo con los roles y responsabilidades del personal a su cargo que trate los datos personales; esto quiere decir que el propio responsable del tratamiento debe impartir los cursos necesarios de acuerdo con las necesidades de capacitación de su personal, la cual en algunos casos y de acuerdo a los sistemas de tratamiento que utilicen deberán ser más o menos técnicos y especializados.

Debe comprenderse que no todo el personal requerirá todas las capacitaciones, por eso la ley establece la obligación de implementar cursos a corto, mediano y largo plazo y a distintos niveles, ya que no será la misma necesidad de capacitación que requiera un ingeniero en sistemas que es administrador de una base de datos, a la que requiera

19 El 2 de marzo de 2000, el Comité de Asuntos Gubernamentales del Senado de Estados Unidos de América, celebró una audiencia sobre la seguridad de los sistemas de información federales. Kevin Mitnick, quien ha sido llamado el hacker más notorio de todos los tiempos, habló ante el comité, y expresó la frase. Síntesis del testimonio disponible en idioma original: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/mitnick.pdf, Testimonio completo disponible en: https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

personal administrativo que solo trata datos personales en formato físico obteniéndolos y almacenándolos.

Bajo ese contexto, se recomienda establecer capacitaciones generales para sensibilizar al personal sobre la importancia de garantizar el derecho a la protección de datos personales, los conceptos de la LGPDPPSO, así como los cursos que imparte el INAI, pero también se recomienda impartir otros cursos especializados como pueden ser de ciberseguridad, seguridad de la información, e incluso se podrían crear cursos prácticos sobre la utilización particular de un sistema propio del sujeto obligado, donde se explique el manual del usuario, así como lo que se tiene permitido hacer y lo que no en dicho sistema, las medidas de seguridad implementadas, etcétera.

A.4 Firma de contratos o cláusulas de confidencialidad

Se recomienda que como medida para cumplir con el deber de confidencialidad se suscriban con los servidores públicos acuerdos o cláusulas de confidencialidad y no divulgación, así como con personal externo que preste servicios profesionales dentro de la entidad o preste cualquier servicio; por ejemplo el personal de limpieza que tenga acceso a las oficinas donde se traten datos personales, o personal técnico que acuda a arreglar equipos o servidores que contengan información correspondiente a datos personales. (se anexa ejemplo).

El objetivo de estos instrumentos es que los empleados o personas servidoras públicas se comprometan a cumplir con el deber de confidencialidad, se recomienda que estas cláusulas establezcan que el alcance será la información relativa a datos personales de los propios empleados, como de cualquier titular de datos personales, o cualquier dato personal que conozcan derivado de su empleo, cargo o comisión.

Se sugiere que dichos acuerdos o cláusulas, contengan como mínimo:

- El objeto de la firma de dicha cláusula.
- El compromiso de mantener el deber de confidencialidad, donde se establezcan como deben tratar los datos personales, a su vez se recomienda que haga referencia genérica a las medidas de seguridad correspondientes al deber de confidencialidad establecidas por el sujeto obligado, se recomienda conminar a cumplir la política de gestión y tratamiento de datos personales, la cual es conveniente entregar en ese momento para que el servidor público reconozca que se le ha entregado, la ha leído y comprendido.
- **La duración del acuerdo, el cual como señala la Ley General, no tiene plazo de prescripción ni caducidad, por lo que no finalizará con la culminación del empleo, cargo o comisión.**
- El derecho del responsable de auditar los sistemas, soportes e información que maneje el servidor público, así como el deber que tiene este para atender

requerimientos en caso de que el Instituto inicie sus facultades de verificación.
- Las sanciones y responsabilidades en caso de incumplimientos.
- Firma del empleado.

Estas son unas de las medidas de seguridad idóneas para el cumplimiento del deber de confidencialidad, puesto que buscan obligar a las personas involucradas en el tratamiento de datos personales a mantener la debida probidad y secrecía de los datos personales de los que conoce mientras dure la relación jurídica con el sujeto obligado, pero que perdura en el tiempo incluso después de que esta finalice.

A.5 Requisitos de seguridad en los contratos con proveedores de servicios-encargados del tratamiento y proveedores de cómputo en la nube, así como cláusula de confidencialidad en el contrato respectivo

Se recomienda que se suscriban con proveedores de servicios, incluyendo a proveedores de cómputo en la nube, acuerdos o cláusulas de confidencialidad y no divulgación, los cuales se pueden incluir en el respectivo contrato de encargo del tratamiento o bien constar en un instrumento jurídico distinto.

A.6 Inventario de datos personales y sistemas del tratamiento

El inventario de activos es el listado de soportes, equipos, sistemas y bienes en general que son propiedad del sujeto obligado, pero que están a cargo de los empleados. Este es un contenido obligatorio del Documento de Seguridad, de acuerdo con el artículo 33, fracción III y 35 fracción I, de la LGPDPPSO, sus requisitos mínimos se encuentran desarrollados en los artículos 58 y 59 de los LGPDPSP, donde es posible observar que no solo deben identificarse los datos personales que se tratan en la entidad, sino los activos que los soportan como pueden ser bases de datos, sistemas, computadoras, discos y memorias extraíbles, archiveros y en general bienes que contengan dichos datos personales, su tipo de almacenamiento, ubicación, entre otros supuestos. El inventario además de ser un requisito obligatorio debe considerarse una medida de seguridad administrativa en sí misma, ya que es fundamental para tener un control de la información incluida la que contiene datos personales, quien la resguarda, y para la elaboración del análisis de riesgos.

B. Medidas de seguridad físicas

B.1 Control de accesos físicos

Esta medida consiste en restringir el acceso a las personas en general, para el caso del deber de confidencialidad debe restringirse incluso a aquellas personas servidoras públicas del sujeto obligado que por atribuciones expresas deban tratar datos personales,

bajo el principio de mínimos privilegios, es decir que puedan tratarlos solo para aquello que es indispensable conforme a sus funciones y atribuciones. En el caso de información que se encuentre soportada en archivos físicos se recomienda mantener los siguientes controles:

B.1.1 Restringir los accesos a las áreas de trabajo mediante identificación constante del personal autorizado a través de políticas y procedimientos de gestión y tratamientos de datos personales la obligatoriedad de portar la credencial de trabajo para identificarse en cualquier momento, y así evitar en la medida de lo posible accesos no autorizados a las instalaciones, y a lugares de trabajo restringidos.

B.1.2 Elaborar un listado de personal autorizado para su acceso a lugares de trabajo restringidos donde se encuentren archivos que contengan datos personales mediante un control de quienes están autorizados y quienes dejan de estarlo puesto que si no se le da seguimiento de nada serviría el control.

B.1.3 Elaborar y mantener una bitácora de acceso a expedientes o archivos físicos que contengan datos personales e información sensible. En relación con el punto anterior, además de un listado de autorizados, se sugiere elaborar una bitácora de accesos, a efectos de que se mantenga un control respecto a quién ha accedido a los datos personales, durante cuánto tiempo, la fecha en que accedió y el motivo, para el caso de que exista una fuga de información o una vulneración a la seguridad se tenga un registro de quienes han tratado los datos vulnerados.

B.1.4 Seguridad en las áreas donde se traten datos personales. Como se mencionó con antelación, las áreas sensibles de trabajo deben restringirse mediante controles físicos, como pueden ser desde seguridad perimetral, hasta la utilización de candados de seguridad en archiveros y gavetas.

C. Medidas de seguridad técnicas

Al igual que en el control de accesos físicos, debe restringirse el acceso a sistemas y bases de datos electrónicas que contengan datos personales, al personal estrictamente necesario y que tenga facultades para ello; asimismo los técnicos que tengan que ingresar a bases de datos o sistemas donde se traten datos personales, se les otorguen permisos temporales y no puedan tener acceso continuado de no ser necesario.

C.1 Alta y baja de usuarios y provisión y revocación de permisos

Al igual que en el acceso físico, es importante tener un **registro de usuarios**, esto es que al momento de dar de alta a un nuevo empleado que requiera de autorización para

ingresar y operar sistemas de tratamiento de datos personales, se registre como usuario y se determine su nivel de privilegio (por ejemplo, si tendrá acceso como administrador o solo como usuario) asimismo, cuando el empleado finalice su encargo, se deberá dar de baja del registro y por lo tanto se deberá dar de baja como usuario. Será muy importante que estos registros **se revisen constantemente y se actualicen cada que se den altas y bajas de servidores públicos.**

C.2 Gestión de autenticación secreta de usuarios

Se sugiere que este control tenga su propia política, en la que se establezca que las personas servidoras públicas deben mantener en secreto los nombres de usuario y contraseñas que se generen para el uso de sistemas y bases de datos (prohibir que se escriban en agendas y/o *notas adhesivas,* y que se compartan por toda la unidad administrativa), asimismo, se sugiere que se imponga la obligación de cambiar la contraseña que se brinda por defecto al primer acceso, y que estas se tengan que cambiar en periodos bimestrales, por ejemplo; así como la generación obligatoria de contraseñas robustas. Finalmente, es muy recomendable el uso de doble factor de autenticación para el control de accesos.

C.3 Seguridad de las comunicaciones

Implementar controles técnicos (así como su correspondiente control administrativo mediante una política o procedimiento) para mantener la seguridad en las comunicaciones, respecto del intercambio de información que contenga datos personales dentro del sujeto obligado y con cualquier otra entidad, o, por ejemplo, los datos personales que traten los encargados del tratamiento a nombre y cuenta del sujeto obligado. Es recomendable que se analice si es oportuno restringir el acceso a ciertas páginas web, y plataformas por las que es posible compartir información mediante dispositivos móviles, sistemas y el correo electrónico institucional, así como regular la posibilidad o no de utilizar los correos electrónicos personales, aplicaciones de mensajería instantánea y redes sociales mediante los dispositivos institucionales.

ANEXO ÚNICO: EJEMPLO DE CARTA DE CONFIDENCIALIDAD (SECTOR PÚBLICO)

CARTA COMPROMISO DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE GESTIÓN DE LA INFORMACIÓN Y DATOS PERSONALES QUE SE TRATAN EN (nombre del tratamiento de datos, sistema, aplicación, etcétera) DE (nombre de sujeto obligado y de la unidad administrativa responsable del tratamiento).

(ciudad), a xx de xx de xx

El/la que suscribe _____, con número de ____ (identificación que lo acredita como persona servidora pública del responsable o sujeto obligado), desempeñándome como _____ de la _____, adscrito/a a (Unidad administrativa) ___ de (nombre del responsable o sujeto obligado).

Se hace constar que se me otorgó por parte de la _____ (unidad administrativa responsable), la política general de gestión y tratamiento de datos personales del _____(sujeto Obligado), en la que consta que todas las personas servidoras públicas, así como personal externo, debemos cumplir estrictamente con dicha Política, y con la normativa en materia de protección de datos personales.

Para efectos de lo anterior, tomo conocimiento de que queda estrictamente prohibido, de manera enunciativa más no limitativa, acceder, robar, copiar sin autorización, alterar o modificar, divulgar, transferir, publicar, prestar la información para fines ajenos a mis atribuciones y facultades, atendiendo en todo momento y aún después de mi comisión o encargo para conocerlos, de conformidad con los principios y directrices que rigen la actuación de los Servidores Públicos. Lo anterior con fundamento en las fracciones I, II, V y VI del artículo 7 de la Ley General de Responsabilidades Administrativas:[20]

20 Decreto por el que se expide la Ley General del Sistema Nacional Anticorrupción; la Ley General de Responsabilidades Administrativas, y la Ley Orgánica del Tribunal Federal de Justicia Administrativa de fecha 18 de julio de 2016; https://www.dof.gob.mx/nota_detalle.php?codigo=5445048&fecha=18/07/2016#gsc.tab=0 consultada el 05 de septiembre de 2023.

"Artículo 7. Los Servidores Públicos observarán en el desempeño de su empleo, cargo o comisión, los principios de disciplina, legalidad, objetividad, profesionalismo, honradez, lealtad, imparcialidad, integridad, rendición de cuentas, eficacia y eficiencia que rigen el servicio público. Para la efectiva aplicación de dichos principios, los Servidores Públicos observarán las siguientes directrices:

I. Actuar conforme a lo que las leyes, reglamentos y demás disposiciones jurídicas les atribuyen a su empleo, cargo o comisión, por lo que deben conocer y cumplir las disposiciones que regulan el ejercicio de sus funciones, facultades y atribuciones;

...

II. Conducirse con rectitud sin utilizar su empleo, cargo o comisión para obtener o pretender obtener algún beneficio, provecho o ventaja personal o a favor de terceros, ni buscar o aceptar compensaciones, prestaciones, dádivas, obsequios o regalos de cualquier persona u organización;

...

V. Actuar conforme a una cultura de servicio orientada al logro de resultados, procurando en todo momento un mejor desempeño de sus funciones a fin de alcanzar las metas institucionales según sus responsabilidades;

...

VI. Administrar los recursos públicos que estén bajo su responsabilidad, sujetándose a los principios de eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a los que estén destinados;

VII. Promover, respetar, proteger y garantizar los derechos humanos establecidos en la Constitución;

..."

Por su parte, en cumplimiento a los principios y deberes en materia de protección de datos personales, me comprometo a:

1. Utilizar la documentación, información y datos personales en mi posesión que tenga bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos, adquiridos con motivo de mi encargo o comisión.

2. Garantizar, custodiar, salvaguardar y cuidar la documentación, información y datos personales en mi posesión que tenga bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos o adquiridos con motivo de mi encargo o comisión.

3. Impedir o evitar el mal uso, divulgación, transferencia, sustracción, destrucciones o inutilización, total o parcial, de la documentación, información y datos personales en mi posesión bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos o adquiridos con motivo de mi encargo o comisión.

4. Adquirir y actualizar los conocimientos necesarios en materia de protección de datos personales y seguridad de la información.

Notificar a quien corresponda de acuerdo con lo previsto en la política/protocolo correspondiente.

5. Actuar conforme a los principios y directrices que rigen la actuación de los Servidores Públicos establecidos en la Ley Genera de Responsabilidades Administrativas, el Código de Ética de _____, el Código de Conducta de _____, y demás leyes normativas aplicable.

Por último, me doy por enterada/o de que en caso de incurrir en alguna violación o incumplimiento de cualquiera de los supuestos establecidos en los párrafos anteriores se podrá iniciar un procedimiento correspondiente de conformidad con lo establecido en la política de protección de datos personales del _____(sujeto obligado).

Una vez leída la presente carta de confidencialidad y responsabilidad, y enterada/o de su contenido y alcances legales, firmo y acepto a su entera satisfacción y conformidad.

_____

(Nombre completo, cargo y firma)

REFERENCIAS

INAI, coord. Davara F. de Marcos, Isabel, Diccionario de Protección de datos personales, conceptos fundamentales.

INCIBE, Protección de la información, Colección Protege tu empresa. Ministerio de Asuntos Económicos y Transformación Digital de España. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf Última fecha de consulta: 29/08/2023.

INCIBE, (30 de noviembre de 2016) CEO, CIO, CISO... ¿Roles en Ciberseguridad? Disponible en https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad Última fecha de consulta: 30/08/2023.

ISO27002puntoporpunto(normaiso27001.es) última fecha de consulta 30/08/2023

Metodología MAGERIT del Ministerio de Asuntos Económicos y Transformación Digital de España. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html fecha de consulta 05/09/2023.


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