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

DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL Y DIFUSIÓN

COMUNICADO • **INAI/249/21**

Ciudad de México.
18 de julio de 2021

www.inai.org.mx

- **La Comisionada del INAI, Josefina Román alertó a cibernautas a proteger sus datos personales**
- **Participó en las conferencias de ciberseguridad 2021 del IFT**

CRIMEN ORGANIZADO, INVOLUCRADO EN VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES

La obtención ilegal de dinero sigue siendo la causa principal de los ataques cibernéticos para robar datos personales en Internet; el crimen organizado es uno de los actores principales de estos ilícitos que atentan contra el derecho humano a la privacidad, alertó Josefina Román Vergara, Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Al impartir la conferencia magistral "Vulneración de datos personales en Internet y plataformas digitales", la integrante del Pleno del organismo garante nacional refirió que "los actores maliciosos continúan siendo la fuerza impulsora del número de vulneraciones que se producen mientras que las bases de datos y los servicios (estén) mal configurados, siendo la principal causa del número de registros (de datos personales) expuestos".

"La motivación financiera sigue siendo la causa más común de ataques, y los principales actores continúan siendo actores externos, es decir, el crimen organizado, y también actores internos; la técnica más utilizada para las vulneraciones a la seguridad de datos personales son el *hacking*, errores, ataques de ingeniería social y *software* malicioso, principalmente", comentó en el evento digital convocado por el Instituto Federal de Telecomunicaciones (IFT) con la participación de la Guardia Nacional y la Secretaría de Seguridad y Protección Ciudadana.

El riesgo de que haya un mal uso de los datos personales, explicó la Comisionada Román, ha crecido notablemente desde el año pasado a causa de la pandemia por COVID-19, que a su vez derivó en un mayor y más intensivo uso de diversas plataformas digitales para trabajar, estudiar y divertirse. Actualmente, según el Instituto Nacional de Estadística y Geografía (INEGI), el 72 por ciento de la población mexicana de seis años en adelante, cuenta con Internet.

Consulta el video #INAIalMomento

La Comisionada del INAI refirió que en 2020 ocurrieron al menos 12 incidentes de seguridad que derivaron, en mayor o menor medida, en vulneraciones a datos personales; entre éstos destacaron los ocurridos entre el 5 y el 11 de julio de 2020, cuando la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el Banco de México (Banxico) y el Servicio de Administración Tributaria (SAT) sufrieron afectaciones en sus respectivas páginas de Internet. Mencionó que entre mayo y junio de 2020, la Secretaría de la Función Pública sufrió un incidente de seguridad que expuso las declaraciones patrimoniales de 830 mil personas servidoras públicas.

Román Vergara señaló que no sólo las instituciones públicas han sido objeto de ataques de la ciberdelincuencia organizada. En el ámbito privado se han padecido episodios de vulneración digital de datos personales en bancos, empresas financieras tecnológicas o *fintech*, además de *holdings* de microfinanzas.

Al citar el informe del monto de las vulneraciones de datos de 2020 de IBM, la Comisionada detalló que el costo promedio total de una vulneración de datos asciende a 3.86 millones de dólares; esto incluye una combinación de costos tanto directos como indirectos relacionados con el tiempo y el esfuerzo para hacer frente a una vulneración, la pérdida de clientes como resultado de la mala publicidad y las multas reglamentarias.

“Otro costo asociado con una vulneración se relaciona con el tiempo que transcurre entre su identificación y su contención, el cual, de acuerdo con el mismo informe, es de 280 días en promedio” dijo Román Vergara.

Recordó que la primera obligación que se tiene es la notificación al titular, que deberá realizarse incluyendo al menos, la naturaleza del incidente, los datos personales comprometidos, las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses, las acciones correctivas realizadas de forma inmediata y los medios donde puede el titular obtener más información al respecto.

Señaló que el INAI publicó recomendaciones para el manejo de incidentes de seguridad de datos personales, cuyo objetivo es “describir los procesos y controles recomendados por el INAI para generar un plan de respuesta a incidentes de seguridad, el participar para mitigar las vulneraciones a la seguridad; estas recomendaciones ayudarán y orientarán a los responsables para: reconocer las diferencias entre alertas e incidentes de seguridad; elaborar un plan para responder ante incidentes de seguridad, conforme estándares internacionales; utilizar formatos de referencia para documentar los incidentes de seguridad”.

Y acotó que “el INAI no está facultado para investigar el robo de identidad (…) corresponde a las autoridades que tienen esta facultad, pero desde el INAI sí podemos investigar el indebido tratamiento de datos personales que esté vinculado, por ejemplo, con el robo de identidad, o con un fraude por la falta de medidas de seguridad para la protección de los datos personales; en una vulneración de datos, una es la parte penal, que se investigue y se lleve a sus últimas consecuencias y otra es la parte que corresponde al INAI, que es la falta de medidas de seguridad que puede llevar a una vulneración de datos personales”.

El Comisario General Luis Rodríguez Bucio, Comandante de la Guardia Nacional, señaló que se está experimentando un cambio sin precedentes en la forma en la comunicación, donde el confinamiento y el distanciamiento social han traído como consecuencia un incremento en el uso del Internet en la educación, el trabajo de oficina y el comercio. Entre más personas y dispositivos se conecten al ciberespacio, más importancia adquiere la seguridad digital, señaló.

“En estas condiciones, el cibercrimen se ha convertido en una preocupación central, por lo que es necesario que los gobiernos incluyan en sus políticas públicas digitales la ciberseguridad, y que las empresas contemplen la gestión proactiva de los riesgos cibernéticos y la privacidad en su planificación y presupuesto de proyectos, así como incrementar la protección de los datos personales”, advirtió.

En la conferencia estuvo presente, vía remota, Adolfo Cuevas Teja, Comisionado Presidente del IFT.

-o0o-

VER VIDEO

VER FOTOGRAFÍA