PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo Cinco Días	1, 12 - 15	31/01/2024	LEGISLATIVO

BLANCO DE CIBERATAQUES Y ROBO DE INFORMACIÓN

El Gobierno de México enfrenta una creciente amenaza cibernética al ser blanco de cientos de miles de ataques al año. La crisis se agrava debido a la falta de inversión en programas tecnológicos y barreras digitales de protección para la información delicada que posee. Además la Ley de Ciberseguridad sigue sin encontrar consenso en el Congreso de la Unión

12

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo	1, 12 - 15	31/01/2024	LEGISLATIVO

#Ciberseguridad

BLANCO DE CIBERATAQUES Y ROBO DE INFORMACIÓN

El Gobierno de México enfrenta una creciente amenaza cibernética al ser blanco de cientos de miles de ataques al año. La crisis se agrava debido a la falta de inversión en programas tecnológicos y barreras digitales de protección para la información delicada que posee. Además la Ley de Ciberseguridad sigue sin encontrar consenso en el Congreso de la Unión

POR DANIEL FLORES

Las instituciones públicas del Gobierno de México son blanco de cientos de miles de ciberataques al año. La información pública que resguardan históricamente es buscada por hackers y sitios maliciosos que, de forma insistente, buscan vulnerabilidades en los sitios gubernamentales.

Datos oficiales proporcionados vía Transparencia revelan miles de ataques al mes a sitios de información como el Instituto Mexicano del Seguro Social (IMSS), la Secretaría de Gobernación (Segob), la Secretaría de Salud (Ssa) e incluso las Fuerzas Armadas, entre otras dependencias gubernamentales.

Por ejemplo, la Ssa federal informó que de 2019 a 2021 registró un promedio de 30 mil intentos de ataques cibernéticos por mes, es decir, más de un millón de agresiones de este tipo en este periodo.

Ante esta situación, la dependencia gubernamental se vio forzada a mejorar su seguridad digital al instalar un Firewall (sistema de seguridad que ayuda a bloquear accesos no autorizados). Tras la implementación de esta tecnología, la Secretaría de Salud dio a conocer que los ataques detectados ascendieron a 1.91 millones.

"Es importante destacar que, a pesar de la magnitud de los intentos de ataques, no se ha comprometido la funcionalidad de los sistemas y servicios operativos de la dependencia. Todos los ataques han sido mitigados de manera efectiva desde el Firewall mediante políticas de seguridad establecidas", respondió la Secretaría de Salud a una solicitud de información de la Plataforma Nacional de Transparencia.

EL DATO

En 2022, instituciones federales como la Secretaría de la Defensa Nacional (Sedena) fueron hackeadas. Se comprobó el robo de información clasificada de la institución castrense y de otras dependencias debido a un ataque masivo de hackers.

Ese año, el país registró más de 85 mil millones de intentos de ciberataques, según un estudio de la Asociación Mexicana de Ciberseguridad (IMECI).

Otra de las instituciones públicas que ha tenido que reforzar su ciberseguridad es la Secretaría de la Defensa Nacional (Sedena), que vio vulnerada su base de datos en esta gestión tras un hackeo masivo de los correos electrónicos que incluían información confidencial de su personal y de sus altos mandos, así como operativos y expedientes.

En 2022, cuando se dio a conocer este robo de información, la institución castrense trató de minimizar el hecho, aunque posteriormente anunció una inversión histórica para reforzar todas sus barreras de ciberseguridad. Hasta el momento, es la única dependencia que registra un alza en el presupuesto de tecnología y ciberseguridad.

Hasta el 80 por ciento se ha recortado el presupuesto destinado a rubros de ciberseguridad y tecnologías de la información en diversas dependencias gubernamentales en la presente administración

A esta extracción ilegal de información se sumaron otras dependencias como Petróleos Mexicanos, el IMSS, la Comisión Federal de Electricidad (CFE), entre otras instituciones públicas que trataron de minimizar el hackeo a sus portales y bases de datos.

No obstante, la vulneración digital puso en alerta máxima a la administración federal, que anunció tomar cartas en el asunto y al Poder Legislativo, cuyos diputados se pronunciaron por acelerar la aprobación de una Ley de Ciberseguridad.

Recortan gasto a ciberseguridad, pese a ataques

En los últimos cinco años, las bolsas presupuestales destinadas a tecnologías de la información y ciberseguridad se han reducido drásticamente para casi todas las dependencias de la administración federal.

De acuerdo con el Presupuesto de Egresos (PEF) de 2019, 2020, 2021, 2022 y 2023, las partidas presupuestales para estos rubros han registrado una disminución que va desde el 50 por ciento al 80 por ciento bajo razones de austeridad y para priorizar otros gastos "esenciales".

Esto, a pesar de las vulnerabilidades expuestas también en los sistemas registrados por entidades como el Banco de México, la Secretaría de Economía, del Trabajo y Previsión Social y el Consejo Nacional para Prevenir la Discriminación.

ILUSTRACIÓN: JESÚS MARTÍNEZ

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo	1, 12 - 15	31/01/2024	LEGISLATIVO

LA CIBERGUERRA Y LA FALTA DE PROTOCOLOS

Sitios especializados, colectivos y hackers lanzan ataques masivos contra dependencias de gobierno para extraer información sensible o incluso deshabilitar sitios. En los últimos años, la tendencia de agresiones digitales se ha disparado

A nivel mundial, México se ha posicionado como el país que más ciberataques recibe y el segundo en Latinoamérica, solo superado por Brasil, según informes de consultoras privadas especializadas en ciberseguridad.

Ante este escenario, especialistas en ciberseguridad advierten que es urgente analizar los mecanismos digitales actuales y elaborar una estrategia eficaz que permita responder de forma favorable ante los embates de hackers y otros entes en la Internet.

Carlos Piña, doctor en Ciencias de la Computación por la Universidad de Essex, Inglaterra, sostuvo en entrevista con Reporte Índigo que la disminución de presupuestos en seguridad informática no debería pasarse por alto, ya que descuidar este aspecto es común en todas las instancias, tanto públicas como privadas.

El especialista precisó que no se trata simplemente de actualizar softwares y licencias, es esencial capacitar al personal especializado y pagar salarios competitivos a los profesionales en ciberseguridad.

"No solo se trata de actualizar el software y las licencias de las dependencias públicas, se tiene que contratar a personal capacitado y pagar los sueldos que cobran estos profesionales, pues se siguen presentando casos de hackeos y filtración de datos personales provenientes desde el gobierno federal", sostuvo.

Carlos Piña puso como ejemplo los problemas que ha enfrentado el Servicio de Administración Tributaria (SAT) y otras dependencias, las cuales han experimentado filtraciones de seguridad y robo de información.

> **"Ha habido filtraciones de seguridad en el SAT y otras dependencias que han sufrido el robo de información y se sigue sin priorizar el gasto en ciberseguridad. Se ha descuidado a las instituciones en esta materia y ahí están las consecuencias"**
>
> **Carlos Piña**
> Doctor en Ciencias de la Computación por la Universidad de Essex

Por ello, insistió en la necesidad de priorizar la seguridad informática, no solo como una medida preventiva contra posibles filtraciones, sino también como una inversión en la protección de datos sensibles y en el mantenimiento de la integridad de las instituciones, tanto gubernamentales como privadas.

3 CASOS DE ATAQUES

Principales ciberataques a dependencias federales durante la actual administración del presidente Andrés Manuel López Obrador

2019
Se reveló que Pemex fue el objetivo de un ciberataque, aunque los detalles del incidente no fueron completamente divulgados

2020
La Secretaría de Economía detectó un ataque cibernético en algunos de sus servidores. A pesar de minimizar el incidente, la dependencia se vio obligada a tomar medidas drásticas

2022
La Secretaría de la Defensa Nacional sufrió un hackeo masivo de sus correos, en el que se lograron extraer miles de documentos oficiales y confidenciales, generando un escándalo en el Gobierno federal

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo	1, 12 - 15	31/01/2024	LEGISLATIVO

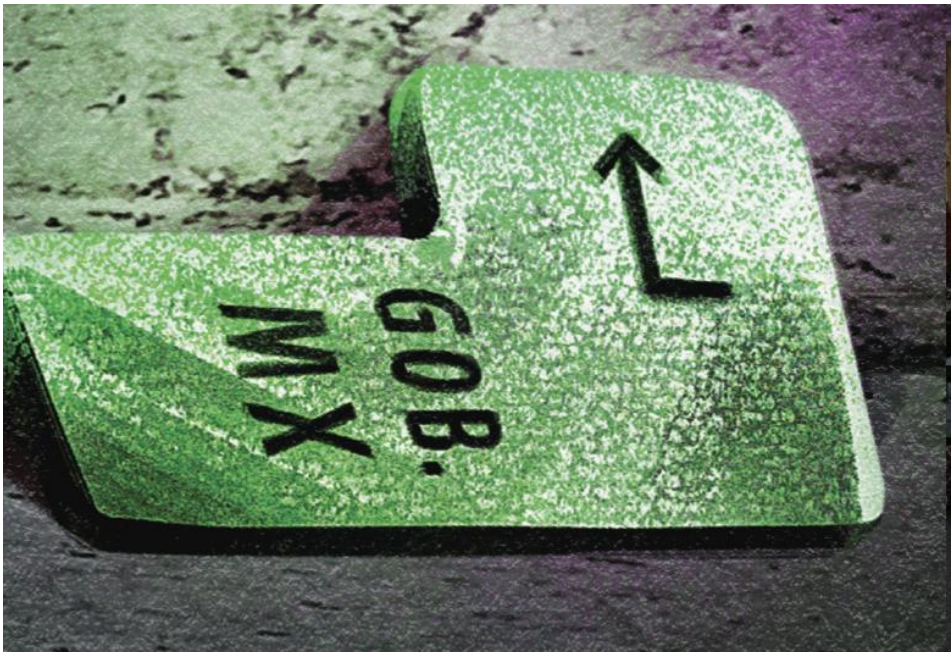

FOTO: CUARTOSCURO

El 26 de enero se filtró una base de datos del Sistema de Acreditación de Prensa de Presidencia a través de foros clandestinos en internet.

FILTRACIÓN DE DATOS DE PERIODISTAS

La filtración masiva de datos de casi 300 periodistas que cubren las conferencias matutinas del titular del Ejecutivo federal puso al descubierto las vulnerabilidades de los sitios que almacenan información personal del gobierno federal

El 26 de enero, Víctor Ruiz, fundador de la firma de ciberseguridad SILIKN, alertó en la red social X (antes Twitter) sobre la filtración de una base de datos del Sistema de Acreditación de Prensa de Presidencia a través de foros clandestinos en internet.

La información comprometida contenía los datos de más de 300 periodistas que tienen acreditación para asistir a la conferencia matutina que se registra en Palacio Nacional, lo que generó el reclamo inmediato de los comunicadores afectados.

El especialista en seguridad cibernética dio a conocer que la base de datos filtrada fue alojada en el sitio web oficial de la Presidencia (https://acreditacionprensa.alfa.gob.mx/) e incluyó información sensible como pasaportes, identificaciones, Registro Federal de Contribuyentes (RFC), nombres, correos electrónicos, números de teléfono, direcciones, fechas de nacimiento y Claves Únicas de Registro de Población (CURP).

La Coordinación General de Comunicación Social y Vocería del Gobierno federal confirmó el robo de información a un total de 263 periodistas que cubren la conferencia matutina del presidente Andrés Manuel López Obrador y en respuesta dijo que levantarían una denuncia penal contra quien resulte responsable.

Al respecto, Víctor Ruiz, fundador de SILIKN, precisó a este diario que es necesario contar con protocolos para este tipo de situaciones, pues quedó demostrado que no se contaban con medidas mínimas de seguridad para las bases de datos personales que almacenan.

"Es básico invertir en el desarrollo y ejecución de planes de respuesta a incidentes, planes de continuidad del negocio y de recuperación contra la pérdida de datos y planes de prevención, además de una gestión de crisis. Esto permite saber qué pasos seguir en caso de sufrir cualquier tipo de incidente", declaró el especialista.

> **"Este gobierno se ha caracterizado por su falta de interés en temas de ciencia y tecnología. No han sido una prioridad y esto afecta directamente al progreso del país, a las inversiones, a la generación de empresas, de empleos y emprendimientos"**
>
> **Víctor Ruiz**
> Fundador de SILIKN

Ley de Ciberseguridad, congelada

A pesar de los ataques perpetrados a dependencias gubernamentales y otras instituciones federales en los últimos años, el Congreso de la Unión sigue sin poder sacar adelante la Ley de Ciberseguridad nacional.

Javier López Casarín, legislador del Partido Verde y quien presidiera la Comisión de Ciencia, Tecnología e Innovación en la Cámara de Diputados, aseguró a este diario que la propuesta de ley aún se encuentra en análisis.

El ahora precandidato a una alcaldía de la Ciudad de México no proporcionó más detalles y se limitó a decir que espera que la propuesta sea llevada al Pleno para su discusión a la brevedad.