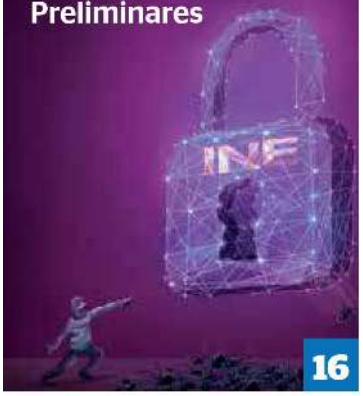
INE bajo ciberataque

El Instituto Nacional Electoral (INE) recibió más de 11 millones de ciberataques durante el periodo 2014-2021, aunque hasta ahora ninguno ha logrado vulnerar sus sistemas informáticos; los dos sistemas que ameritan mayor protección son el de Conteo Rápido y el Programa de Resultados Electorales Preliminares



16

#Elecciones

EL INE BAJO CIBERATAQUE

El Instituto Nacional Electoral (INE) recibió más de 11 millones de ciberataques durante el periodo 2014-2021, aunque hasta ahora ninguno ha logrado vulnerar sus sistemas informáticos; Lorenzo Córdova señala que los dos sistemas que ameritan mayor protección son el de Conteo Rápido y el Programa de Resultados Electorales Preliminares (PREP)

POR LUIS HERRERA
@Luis Herrera A

El Instituto Nacional Electoral (INE) enfrenta una tormenta de ciberataques con los que se ha intentado recurrentemente vulnerar sus sistemas informáticos, al grado de haber recibido más de 11 millones de estas embestidas durante los últimos años, de acuerdo con un informe del organismo.

A pesar de los millones de ciberataques que han estado siendo dirigidos contra la autoridad que está a cargo de las elecciones en México, la institución asegura que, hasta ahora, ninguna de esas ofensivas informáticas ha logrado su cometido de generar algún tipo de daño o robo de información.

Así lo señala la Unidad Técnica de Servicios de Informática del INE: "Sobre el presente cuestionamiento, esta Unidad informa que, dentro del periodo requerido por la persona requirente, comprendido del 1 de enero de 2014 al 19 de octubre de 2021, no se ha materializado ninguno de los intentos de ataques cibernéticos, ya que estos se han logrado contener a través de los distintos mecanismos de seguridad perimetral".

El reporte del INE obtenido vía transparencia (expediente: UT/21/02994), agrega: "Por lo que hace al número de ataques que causaron daño, esta unidad señala que el número es igual a cero. En este sentido, el número de ataques que no causaron daño es igual a 11 millones 126 mil 105".

Los datos de ataques cibernéticos que proporciona el INE comienzan en el año 2014 porque, según lo asevera, fue hasta ese año que tuvo posibilidades de generar un registro en la materia: "Es importante señalar que no se tiene el registro de los intentos de ataques cibernéticos realizados al Instituto desde el 1 de enero de 2007 al 31 de diciembre de 2013. Lo anterior, toda vez que no se contaba con las condiciones en la materia".

Y precisa que por "ataque" se entenderá un intento (deliberado o no) por vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos del INE.

"En este sentido, se señala que, en todos los casos, los intentos fueron detectados y contenidos por los distintos mecanismos de seguridad de la Red Nacional de Informática del INE (RedINE), por lo que ninguno de ellos fue exitoso".

Las amenazas

También se le cuestionó al INE si había recibido ataques con los virus conocidos como "ransomware", a través de los cuales los hackers pueden bloquear el acceso y la operación de los sistemas informáticos que fueron vulnerados, mientras a sus propietarios se les exige el pago de un "rescate" para liberarlos.

Sin embargo, el Instituto aseguró que ese tipo de virus no ha estado presente entre los millones de ataques cibernéticos que ha recibido: "Se informa a la persona solicitante que no se han registrado intentos de ataques en donde se involucre algún tipo de Ransomware".

Y de igual forma, el INE asevera que ninguno de los ciberataques que ha registrado ha logrado concretar algún robo de información: "Esta Unidad Técnica informa que el número de ataques cibernéticos, en donde hubo robo de información exitosa, es igual a cero, toda vez que no se ha materializado ninguno de los intentos de ataque".

El INE, sin embargo, clasificó una parte de la información solicitada como reservada, al considerar que su exposición podría poner en riesgo sus sistemas informáticos; por ello, evitó informar de qué países provinieron los ataques cibernéticos que ha tenido; en cuántos casos se identificó a sus autores y de qué autores se trata.

"La difusión de la información solicitada pone en riesgo evidente la estabilidad de los sistemas informáticos del Instituto, y con ello la operación institucional de este organismo, así como propiciar el delito de acceso ilícito a sistemas y equipos de informática", indicó.

"Para cumplir y salvaguardar los fines de este Instituto se considera necesario reservar la información con el objeto de contribuir a la vida democrática del país y asegurar a los ciudadanos el ejercicio de sus derechos políticos electorales", añadió.

Ciberescudos

El 11 de abril de 2018, durante su intervención en el Foro de Análisis y Discusión "Ciberseguridad en las Elecciones", el presidente del INE, Lorenzo Córdova Vianello, reconoció que el organismo se encontraba bajo constantes ciberataques.

"Los sistemas informáticos, privados y públicos, están sometidos a un intento permanente de intromisión o de hackeo. Eso no es novedoso y el INE, no es que estemos ahora enfrentando el proceso más grande de la historia desde una perspectiva naif (ingenua o de manera espontánea), pero esos sistemas y el INE, también han sido objetos de ataques cibernéticos a lo largo de su historia en innumerables ocasiones".

"Sin dar las cifras precisas sí comentó que al mes nuestros sistemas reciben intentos de hackeo de más de cientos de miles de intentos al mes. (...) en su mayoría provienen de sistemas de computadoras mexicanas, es normal, y después de computadoras de Estados Unidos, no de Rusia", expuso.

Para protegerse, dijo, "el INE tiene una división de ciberseguridad interna muy relevante y todos los sistemas hoy además están siendo auditados por una compañía externa, que está vigilando la integridad del sistema desde afuera, pero también los protocolos con los que se opera desde adentro. (...) estamos protegiéndonos de hackeos que vengan desde afuera y por supuesto de vulneraciones que algún operador que dentro del propio INE pudiera hacer".

Expuso también cuáles eran los sistemas que ameritaban mayor protección: "Tenemos 35 sistemas vinculados al proceso electoral, entre ellos, lo más probable, lo más relevante, al menos desde el punto de vista político y los que más cuidamos, son los que tienen que ver con la información preliminar de resultados, el sistema del Conteo Rápido y el Sistema del Programa de Resultados Electorales Prelimi-

nares".

El consejero presidente advirtió que ambos sistemas arrojan información "no legalmente válida porque los votos, los resultados electorales no dependen de esa información, sino que serán contados tres días después en los cómputos distritales"

Y añadió que "si tuviéramos una vulneración en esto sistemas, insisto, la legalidad de la elección no se pone en riesgo, pero sin duda sí la certeza y el blindaje político que se requiere".

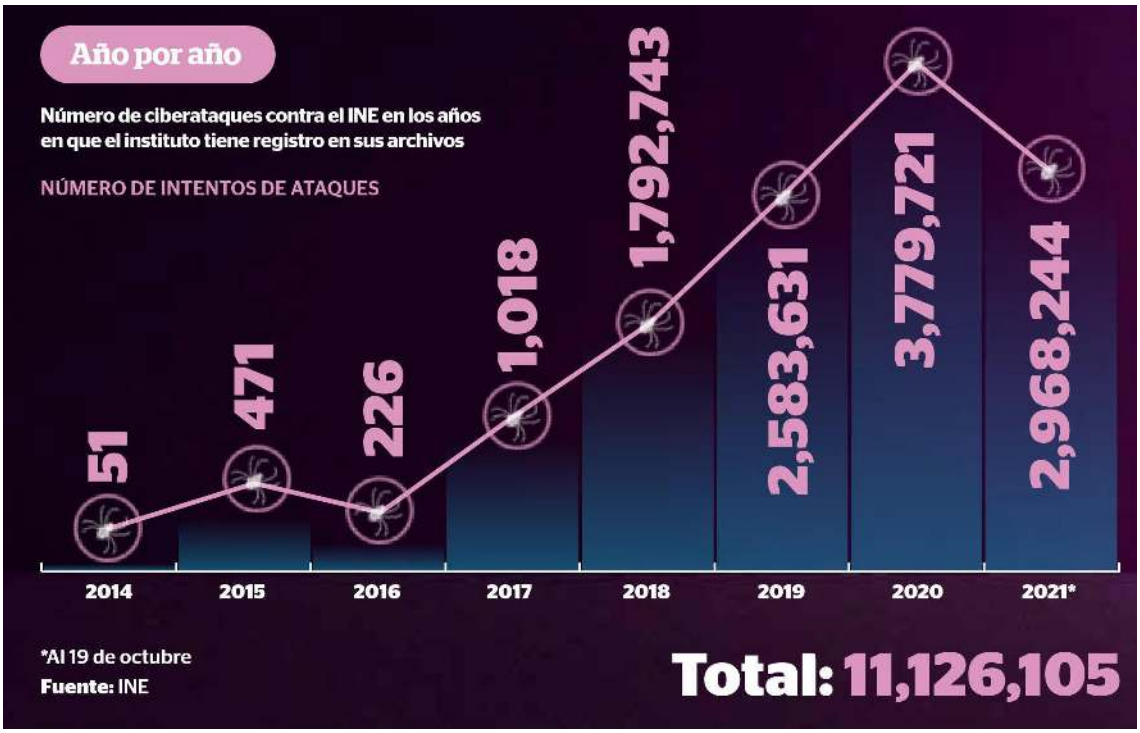
11.1
millones
de intentos
de ataque ha
detectado el INE
del 1 de enero
de 2014 al 19 de
octubre de 2021

"No se ha materializado ninguno de los intentos de ataques cibernéticos, ya que estos se han logrado contener a través de los distintos mecanismos de seguridad perimetral"

Informe del INE

FOTO: CUARTOSCURO

El consejero presidente, Lorenzo Córdova, confirmó que el Conteo Rápido y el PREP son los sistemas que más se resguardan, aunque no son vinculantes en una elección, sino otra vía para la certeza de los ciudadanos.



Fuente: INE

Blindado
Ninguno de los ataques cibernéticos contra el Instituto ha logrado hacer daño a los sistemas computacionales