EL UNIVERSAL
EL GRAN DIARIO DE MÉXICO

PERIODISMO DE INVESTIGACIÓN Y DATOS

CRECEN LOS CIBERATAQUES CONTRA EL INE

En los primeros dos meses de 2024, **los dardos digitales que recibió el Instituto Nacional Electoral** ya superan el total de acumulados en la elección presidencial de 2018

> "En todos los casos, los intentos fueron detectados y contenidos por los distintos mecanismos de seguridad de la red"
>
> **INE**
> Respuesta vía transparencia

> "Por el poder computacional y por la naturaleza que tienen los sistemas... es muy fácil realizar ataques informáticos"
>
> **Vladimir Chorny**
> Investigador de R3D

EL UNIVERSAL
EL GRAN DIARIO DE MÉXICO

Texto: **ERNESTO AROCHE**
—nacion@eluniversal.com.mx
Ilustración: Liliana Pedraza

El Instituto Nacional Electoral (INE) está bajo ataque digital. En los primeros dos meses de 2024 ha recibido más golpes que durante todo 2018, cuando también hubo comicios.

"Durante la elección [de 2018], el INE sufrió el ataque cibernético de denegación de servicio más grande que haya tenido probablemente institución alguna del Estado mexicano en la historia", reconoció en 2019 el entonces presidente del INE, Lorenzo Córdova Vianello, durante una conferencia pública.

En 2018, el INE contabilizó un total de 1.8 millones de intentos de "vulnerar la integridad, disponibilidad o confidencialidad de sus sistemas informáticos", pero esta cifra quedó ya muy atrás. En los primeros 57 días de 2024 se registraron 2.6 millones: una lluvia de 32 ataques por minuto en promedio.

Estos datos fueron entregados por el INE en respuesta a una solicitud de información realizada por EL UNIVERSAL.

Especialistas consideran que las agresiones se intensificarán conforme avancen las campañas y durante la jornada electoral.

Aunque con vaivenes, los ataques o "intentos de ataques", como apunta el INE, han ido creciendo desde hace 10 años. En 2014 hubo 51; en 2015, 471; en 2016, 226; en 2017, mil 18; en 2018 se disparó a un millón 792 mil; en 2019, 2 millones 583 mil; en 2020, 3 millones 779 mil; en 2021, 2 millones 970 mil; en 2022, 2 millones 309 mil; en 2023, 3 millones 78 mil, y del 1 de enero al 26 de febrero suman ya 2 millones 616 mil impactos. En total, más de 19 millones en 10 años.

Si lo contamos según las manecillas del reloj de los últimos cinco años, entonces en 2020 fueron siete ataques por minuto; en 2021, seis; en 2022, cuatro; en 2023, seis, y en 2024, 32. Todo en números cerrados.

El 2020 fue atípico porque la pandemia disparó los crímenes digitales, coinciden especialistas.

El INE expone que, según el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés), un "ciberataque" se define como un intento de obtener acceso no autorizado a servicios, recursos o información del sistema, o un intento de comprometer la integridad, disponibilidad o confidencialidad del sistema, a través del ciberespacio, con el fin de interrumpir, deshabilitar, destruir o controlar un entorno/infraestructura informática, o destruir la integridad de los datos o robar información controlada.

Hasta el momento, también aclara el INE, ninguno de los millones de ataques que ha recibido el organismo en los últimos 10 años ha sido exitoso: "En todos los casos, los intentos fueron detectados y contenidos por los distintos mecanismos de seguridad de la Red Nacional de Informática del Instituto (RedINE)".

19.1
MILLONES
de ataques cibernéticos de "severidad alta" ha recibido el INE en 10 años.

3.8
MILLONES
de ataques recibió el INE en 2020, el año con más registros de la década.

32
ATAQUES
por minuto sucedieron en los dos primeros meses de 2024, el número más alto.

El escenario digital que enfrenta el organismo electoral de cara al proceso que se ha denominado como "los comicios más grandes de la historia" es complicado, pues las habilidades técnicas y de automatización para generar ataques/ciberataques se han incrementado en los últimos años, advierte Vladimir Chorny, investigador asociado de la Red en Defensa de los Derechos Digitales, conocida como R3D.

"Hoy en día, por las herramientas tecnológicas, por el poder computacional y por la naturaleza que tienen los sistemas computacionales de hackeo, es muy fácil realizar ataques informáticos", reconoce.

El especialista menciona que es factible que grupos asociados a la criminalidad cibernética, actores de poder o incluso partidos políticos que busquen incidir en la contienda electoral contraten hackers que, a través de "redes zombies" de computadoras o "*botnets*", puedan dañar infraestructuras críticas o provocar el bloqueo al acceso a servicios del INE, como el Programa de Resultados Electorales Preliminares, conocido como PREP.

Este modelo técnico de agresión ya se ha intentado, según explicó Lorenzo Córdova en 2018, cuando habló de los ataques que se vivieron durante la jornada electoral donde resultó ganador el actual presidente Andrés Manuel López Obrador.

"Llegamos a tener solicitudes de

UNA TORMENTA DE ASALTOS

Los golpes digitales al INE han ido creciendo en la última década.

AÑO	ATAQUES
2014	51
2015	471
2016	226
2017	1,018
2018	1,792,743
2019	2,583,631
2020	3,779,721
2021	2,970,477
2022	2,309,631
2023	3,078,035
2024*	2,616,121
TOTAL	**19,132,125**

*Fuente: INE. *Datos de 2024 hasta el 26 de febrero.*

acceso a nuestros sistemas a través de robots para tratar de intentar bloquear el funcionamiento de nuestros sistemas, lo que se conoce como ataques de denegación de servicio muy intensos, y fuimos exitosos".

El coordinador de Seguridad de la Información de la UNAM, Carlos Raúl Tlahuel Pérez, explica que un ataque de denegación de servicio implica el envío de miles de solicitudes de acceso a páginas de internet con el objetivo de provocar el colapso de los servidores.

"No significa que se vaya a destruir la información, queda indisponible por un lapso... lo que más preocuparía sería un ataque en la reputación", considera.

El INE se negó a entregar algunos datos solicitados porque consideró que se "pondría en riesgo la seguridad nacional informática de los sistemas". Reservó hasta 2026 el número de ataques por día, el tipo de ataque recibido y la procedencia de éstos. El organismo se limitó a entregar información por año.

El problema de esta respuesta parcial, sostiene Vladimir Chorny, es que al ser tan general la información no se puede dimensionar: "Una cosa es que estén atacando la página para que no funcione, o algo así, y otra cosa es que estén atacando, por ejemplo, los servidores que se están utilizando para los servicios de voto electrónico o voto por internet... hay un montón de ámbitos en los que se pueden realizar ataques informáticos y va a variar la gravedad".

Los ciberataques y hackeos a diferentes entidades de gobiernos son una constante en la presente administración federal. En septiembre de 2022 se conoció de una filtración masiva de correos electrónicos de la Secretaría de la Defensa Nacional a manos del grupo *hacktivista* autodenominado *Guacamaya*.

En 2019, Petróleos Mexicanos fue víctima de un secuestro virtual de datos. En enero de 2024, extrajeron datos personales de periodistas y asistentes a la conferencia mañanera presidencial, y en las últimas semanas se han registrado ciberagresiones y robo de información a portales de gobiernos locales adjudicados a un grupo autodenominado *Mexican Mafia*.

Blindados contra los ataques

Yuri Adrián González Robles, director de seguridad y control informático del INE, manifiesta en entrevista que estos impactos han sido de "severidad alta"; sin embargo, el instituto ha logrado contenerlos.

Afirma que el repunte de los ataques tiene que ver con el incremento en los sistemas digitales del instituto expuestos a internet, entre ellos el PREP.

"A partir de 2019 lo que está reflejando la numeralia [obtenida por transparencia] tiene que ver con el gran incremento en el número de sistemas; actualmente para efecto del proceso electoral y, a reserva de que me equivoque, son 47 sistemas los que tenemos en operación, nada más para proceso electoral", dice.

Sobre las "redes zombies", puntualiza que ahora "se pueden rentar como si fuera un servidor" e incluir cualquier dispositivo conectado a internet, incluso un refrigerador.

Para reforzar la seguridad, añade, mantienen auditorías externas al PREP a cargo de la Universidad Autónoma de México unidad Iztapalapa, y al Sistema de Voto Electrónico por Internet vía Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional. El resto de los sistemas se audita de manera interna. ●