

EMPRESAS

Grupo Lala invirtió 900 millones de pesos en innovación en el primer semestre

Con el fin de consolidar su modelo de sostenibilidad y reafirmar su compromiso con los ODS, la productora de lácteos informó amplió su capacidad instalada en planta, equipos y vehículos de alta tecnología.

Editora: Karla Rodríguez Coeditora: Anasztazi Rizo Coeditora Gráfica: Ana Luisa González Diseñadora: Anreza Clavelina

SE REGISTRAN 32 ATAQUES POR MINUTO

Elecciones en México, bajo amenaza de cibercriminales

En el último año, los intentos de ciberataques contra el INE aumentaron más de 500 por ciento

En 2023, México fue el país con más intentos de ciberataques a nivel global

CHRISTOPHER CALDERÓN
calderonc@elfinanciero.com.mx

En medio del proceso electoral en México, que se llevará a cabo este 2 de junio y donde estarán en juego más de 20 mil cargos de elección popular, la preocupación entre los expertos de ciberseguridad se mantiene muy alta, debido al gran riesgo que existe de que el Instituto Nacional Electoral (INE) sea víctima de un hackeo que ponga en tela de juicio los resultados de la elección.

"La probabilidad de un ciberataque durante el proceso electoral está entre medio y alto pues el INE, desde que inició 2024, ha sido blanco de un mayor número de intentos de ciberataques", advirtió Verónica Becerra, integrante del Consejo de Seguridad de Información y Ciberseguridad (ConsejoCiaC).

De acuerdo con datos del propio órgano electoral, desde que inició el 2024 han registrado un aumento superior al 500 por ciento, en intentos de ciberataques, ya que, mientras en 2023 se reportaban seis por minuto, este año ha registrado 32 intentos de ciberataques en promedio por minuto.

De esta manera, en lo que va del año, el órgano encargado de organizar las elecciones en el país ha sido blanco de por lo menos 8.2 millones de intentos de ciberataques, lo que debería ser considerado, según expertos, como un 'foco rojo' de lo que podría suceder durante la jornada electoral de este domingo.

En riesgo

Sólo en 2023, los ataques registrados alcanzaron los 290 mil millones, 55.7% más que en el 2022.

■ Millones de intentos de ataques en México



Fuente: Q&A / Consejo Calcelec

"Es necesario que tanto las autoridades gubernamentales, como los organismos electorales y los proveedores de servicios en línea trabajen en estrecha colaboración, para mitigar los riesgos de ataques durante la elección", alertó Víctor Ruiz, fundador de la empresa de ciberseguridad Silikn.

De acuerdo con el experto, el principal riesgo que corre el INE es ser víctima de un ataque de denegación de servicio DDoS, el cual busca sobrecargar los servidores con un flujo masivo de tráfico malicioso, dejando los servicios inaccesibles a los usuarios.

Tan sólo en el segundo semestre de 2023, según datos del Reporte sobre ataques DDoS, elaborado por Netscout Systems, México fue blanco de un total de 16 mil 711 ataques en línea de este tipo, colocando esta amenaza sólo por debajo del ransomware y el phishing.

ALERTA

Preocupa la intervención de grupos criminales de países como Rusia, China, Corea del Sur.

AFECTA LINEA REDUCCIÓN DE PRESUPUESTO
La principal preocupación que tienen tanto expertos como empresas de ciberseguridad es la reducción en el presupuesto que ha tenido el INE a lo largo del sexenio de Andrés Manuel López Obrador, lo que

ha aumentado las alertas de un posible hackeo a los servidores del organismo electoral.

Para 2024, con la elección en puerta más grande en la historia de México, el Congreso aprobó al INE un presupuesto por 8 mil 808 millones de pesos, que significaron una reducción de 552 millones de pesos respecto a los 9 mil 355 millones de pesos que le fueron aprobados para sus operaciones en 2023, un periodo en el que sólo hubo elecciones en tres estados del país (Tamaulipas, Coahuila y Estado de México).

"El recorte de presupuesto al INE es uno de los principales riesgos que vemos, porque puede afectar

la prevención y respuesta ante un ciberataque; sin embargo, mientras existan políticas y tecnología implementadas de manera correcta, se puede minimizar el riesgo de un posible ciberataque", añadió Becerra, quien también es cofundadora de la empresa de ciberseguridad Offhack.

Por su parte, Víctor Ruiz aseguró que este recorte, puede abrir la puerta a que el INE sea blanco de hackers de diferentes países que quieran interferir con el proceso electoral de México, ya sea con fines políticos para robar la información de los ciudadanos y cometer delitos financieros con ellos.

"Preocupa este reporte porque son detalles que atraen a grupos de cibercriminales de Rusia, Corea del Norte, China, Estados Unidos, Reino Unido e Israel", dijo el directivo, quien afirmó que el mayor riesgo está en un ciberataque a nivel local, que tendrá como objetivo afectar la elección de este año con fines políticos.

En la mira

Con las elecciones en puerta, el INE podría ser víctima de un ataque y denegación de servicio DDoS.

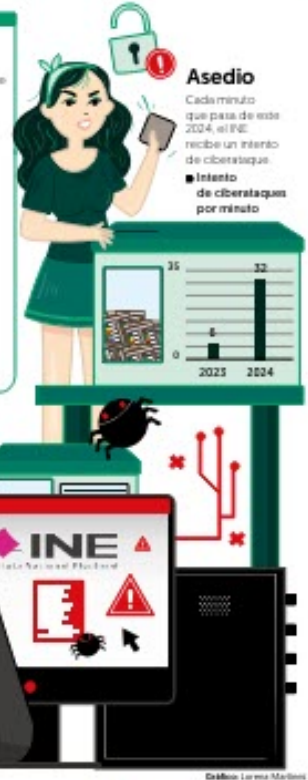
■ % Sectores más afectados por ciberataques en 2023



Asedio

Cada minuto que pasa de este 2024, el INE recibe un intento de ciberataque.

■ Intento de ciberataque por minuto



552

MILLONES DE PESOS

Menos recibió el INE de presupuesto este año respecto al 2023, a pesar de las elecciones.

REPUTACIÓN DEL INE EN JEGO

Según expertos en ciberseguridad, el proceso electoral del 2 de junio será clave para definir la reputación y la permanencia del INE como encargado de organizar las elecciones.

"Hay que recordar que en este gobierno se ha querido desaparecer al INE y si en este proceso falla y no garantiza la democracia, justificará el discurso del presidente", dijo el CEO de Silikn.

La integrante del ConsejoCiaC afirmó que el daño reputacional para el INE en caso de una vulnerabilidad sería irreparable y derivaría en una apatía de la gente.