EDITOR:
Héctor Molina

COEDITOR:
Iván Rodríguez

política
@eleconomista.mx

eleconomista.mx

COEDITOR GRÁFICO:
David Mercado

DETIENEN A DIPUTADA DE MORENA CON ARSENAL

La Fiscalía General de Justicia del Estado de Puebla confirmó la detención de la diputada local suplente de Morena, Sandra Nelly Cadena Santos, en posesión de armas de fuego largas y cortas, así como granadas de uso exclusivo del Ejército.

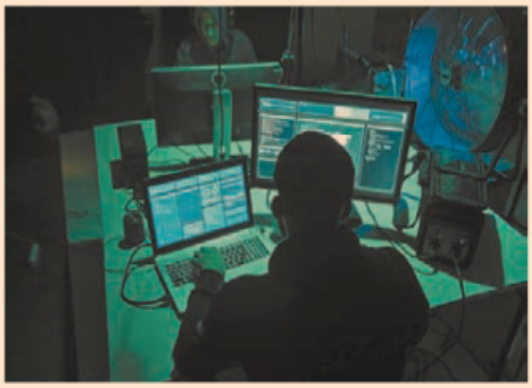
"La Fiscalía de Puebla cumplió orden de cateo en un inmueble de Tecamachalco y aseguró a Jesús N. y Sandra Nelly N. en posesión de armas de fuego largas y cortas, además de granadas de uso exclusivo del ejército. El inmueble también está asegurado, la investigación continúa", mencionó la Fiscalía al confirmar que la mujer fue detenida junto con su esposo, Jesús Portilla García. *(Jorge Monroy)*

Encabezan Pemex, Presidencia y SEP intentos de hackeo en 2021

En aumento, ciberataques a instituciones públicas

- Falta unificar criterios en el gobierno federal para combatir problema: expertos

Héctor Molina e Iván Rodríguez
política@eleconomista.mx



Los delincuentes buscan capturar los sistemas de instituciones públicas para robar información sensible. FOTO: ESPECIAL

Las instituciones a nivel federal registran millones de ciberataques anualmente cuyo objetivo es secuestrar los sistemas y robar información; una situación que se ha incrementado en los últimos años, según muestran estadísticas de las mismas instituciones.

En informes divulgados a través de la plataforma de transparencia, la Presidencia de la República; las secretarías de Educación Pública, Defensa Nacional, Marina, de Salud y de Economía, así como la Suprema Corte de Justicia de la Nación (SCJN), el Instituto Nacional Electoral (INE), la Fiscalía General de la República (FGR) y Petróleos Mexicanos (Pemex), han reportado el número de ciberataques que han registrado sus sistemas.

Entre estas instituciones destaca el caso de Pemex ya que tan sólo entre enero y junio pasado la petrolera ha registrado 128 millones 809,396 ciberataques cuyo objetivo ha sido robar información de sus sistemas.

Este registro es el más alto al menos desde el 2015, año en el que se contabilizaron un total de 47 millones 714,307; en el 2016 fueron 4 millones 467,446; un año después el número se disparó a 44 millones 810,658.

Para el 2018, Pemex registró 76 millones 357,979 ciberataques; en el 2019 la cifra bajó a 7 millones 85,934 y para el 2020 se contabilizaron 861,670 eventos, de acuerdo al informe emitido por la empresa estatal a través de la solicitud con folio: 1857200220321.

En segundo lugar en número de ciberataques, para este 2021, está la Presidencia de la República ya que en el primer semestre contabilizó un total de 78 millones 676,967 ciberataques.

Así como Pemex, este año ha marcado un máximo en el número de ataques para la Presidencia desde el 2015, según informó la instancia en la solicitud con folio 0210000102921 realizada por un peticionario.

Mientras que en tercer lugar entre las instituciones referidas se ubicó Educación Pública con un total de 3 millones 614,697 eventos de ciberataques a sus sistemas.

Instituciones como el INE (dos millones 968,244 ciberataques); la SCJN (312,716); Banxico (17,669); la Secretaría de Salud (14,742); Marina (4,608); el Ejército (1,107) y Economía (15) han registrado también miles de ataques a sus sistemas en la primera mitad del año.

Otras instituciones como el SAT, la Secretaría de Energía, del Trabajo, Gobernación, Seguridad y Relaciones Exteriores han indicado que, o no tienen registros sobre el tema, o no han presentado ciberataques a sus sistemas entre el 2015 y hasta el primer semestre del 2021.

Pemex ha registrado, entre enero y junio pasado, 128 millones 809,396 eventos de ciberataque cuyo objetivo ha sido robar información de sus sistemas.

Posibles motivos

Julio Olivares, director de Innovación y Diseño de Soluciones en Innovación de Ácumen Telecomunicaciones, explicó que algunos de los ciberataques enfocados en organismos públicos pueden tener como único propósito desprestigiar a dichos organismos o afectar su credibilidad, con el consecuente impacto negativo en su interacción con los ciudadanos.

Mientras que el objetivo de otros, opinó Carlos Tlahuel Pérez, coordinador de Seguridad de la Información en la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, es obtener dinero por medio del secuestro de información y extorsión.

El experto de la UNAM detalló que en cada dependencia debe existir un departamento de gestión de seguridad de la información, el cual tiene como labor generar un análisis de riesgos, es decir, ver qué tan protegida o desprotegida está la organización.

En cuanto a cómo califica el nivel de protección de las instituciones frente a estos ataques, Tlahuel Pérez explicó "se ve el resultado cuando se atacan o resisten ataques, por ejemplo, si alguna institución nunca ha reportado problemas o no tiene activos llamativos para la delincuencia lo está haciendo muy bien", abundó.

Luis Fridman, CEO de Avantika, empresa que brinda servicios de TI y ciberseguridad detalló que a pesar de que el gobierno ha tomado acciones para prevenir los ciberataques y combatir el ciberdelito, todavía existen áreas de oportunidad para estar a la altura de esta problemática.

"Las instituciones públicas, por más que sus líderes en ciberseguridad y sus planes se hayan profesionalizado en los últimos años, carecen de un elemento fundamental: el liderazgo que unifique y dicte criterios en el tema, que se asegure de su cumplimiento y efectividad y que integre las mejores prácticas de jugadores en el extranjero a nuestra realidad tecnológica nacional", indicó.

Pendiente en caso Ayotzinapa, indagar decisiones del gobierno de EPN: ONG

Redacción
política@eleconomista.mx

El CentroPro de Derechos Humanos que ha acompañado a los padres de los 43 normalistas de Ayotzinapa indicó que a siete años de la desaparición de los normalistas y a tres años de la actual administración del presidente Andrés Manuel López Obrador aún hay pendientes importantes en el caso como investigar las decisiones de altas autoridades del gobierno anterior.

En un análisis presentado por la organización civil sobre el caso, precisó que entre los pendientes está el "consolidar nuevas acusaciones contra perpetradores de la desaparición forzada identificados con prueba lícita y contra actores privados que recobraron su libertad debido a las irregularidades de la investigación anterior".

La ONG también precisó como pendientes "investigar con decisión a las altas autoridades del anterior gobierno que tomaron la decisión política de cerrar el caso con la verdad histórica, sin que hubiese evidencia científica para ello", además de "resolver los graves retrasos en la asistencia victimal y las cargas desproporcionadas de requisitos impuestos a las víctimas, debidos a los cambios en la CEAV (Comisión Ejecutiva de Atención a Víctimas) y al desmantelamiento de sus mecanismos presupuestales. Máxime considerando que dos padres han muerto durante la pandemia".

En este análisis, la organización refirió como "rezagos estructurales" el que si bien el caso de la desaparición de los normalistas muestra que las fuerzas castrenses han sido opacas en entregar información en el caso, aún siguen administrando información y se encuentran "más empoderadas que nunca".

Además de que si bien en el asunto de los normalistas ha existido colaboración de las víctimas, dicha situación no se ha replicado en otros casos.

Avances parciales

En contraparte, el CentroPro calificó como avances parciales el que se hayan realizado nuevas identificaciones genéticas de normalistas.

Otro avance, indicó la ONG, es "el inicio de procesos penales por delincuencia organizada en contra de elementos de seguridad federales", entre ellos un capitán del Ejército y el que se investigue actos de tortura cometidos durante la indagatoria anterior.

s1875_u4549