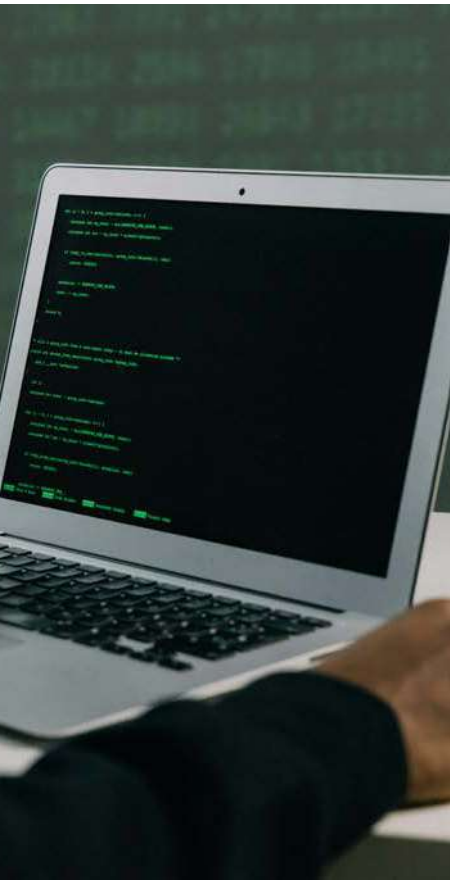
www.mexis.net

NO HAY CAPACIDAD DE RESPUESTA

A INCIDENTES DE CIBERSEGURIDAD EN EL GOBIERNO: ATDT

mexis aggity



La ATDT anunció una política general y la creación de un Centro de Operaciones de Ciberseguridad (CSOC) para fomentar el reporte, la colaboración y las prácticas básicas de higiene digital en coordinación con industria, academia y dependencias.

La cabeza de la nueva Dirección de Ciberseguridad de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) admitió que el gobierno federal no tiene capacidad de respuesta a incidentes de ciberseguridad dentro de las instituciones de la Administración Pública Federal.

Durante el **2do Foro Nacional de Ciberseguridad**, organizado por la **Alianza México** Ciberseguro (AMCS) en la Universidad Panamericana, **Heidy Karla Rocha Ruiz**, directora de Ciberseguridad, aseguró que esta incapacidad hace vulnerables a las instituciones de gobierno.

De acuerdo con la funcionaria, el uso de tecnologías del sector privado es lo que permite a las instituciones del gobierno federal hacer frente a las **amenazas de ciberseguridad** que estás enfrentan.

“Desde la **Agencia de Transformación Digital y Telecomunicaciones (ATDT)**, los retos que vemos son que principalmente no se es capaz de tener una respuesta ante incidentes, es decir, pasa un incidente de ciberseguridad y no se tiene la capacidad de respuesta, desde identificarlo, que viene trabajándose meses atrás, en alguna dependencia, por parte de un grupo atacante y ya cuando es visible ante la dependencia, en la Unidad de Tecnologías de la Información de la dependencia, es porque ya tenían tiempo atrás. Esto pues nos hace muy muy vulnerables”, dijo Rocha Ruiz, durante su participación en el panel Actualidad y futuro en la ciberseguridad. ¿Hacia dónde vamos” del **2do Foro Nacional de Ciberseguridad.**

El panel fue moderado por Ernesto Ibarra, coordinador de la Alianza México Ciberseguro (AMCS), y también participaron Patricia Chávez Obregón, en representación del secretario de Seguridad y Protección Ciudadana, Omar García Harfuch, y Miguel Ángel Cañada, del Instituto Nacional de Ciberseguridad de España (Incibe).

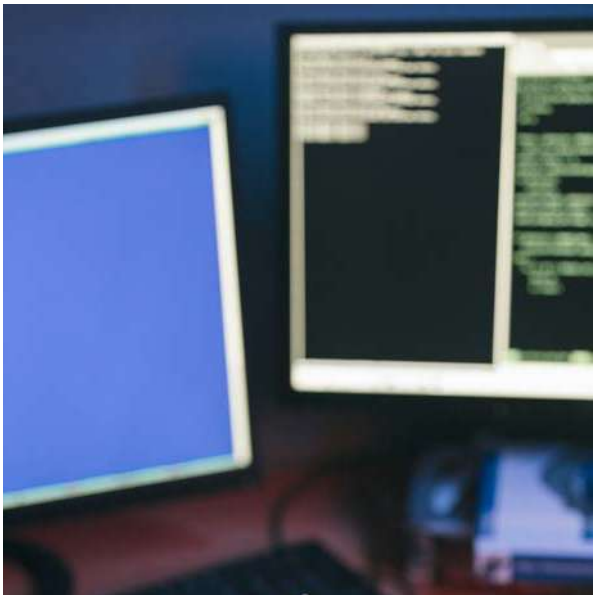
Diagnóstico

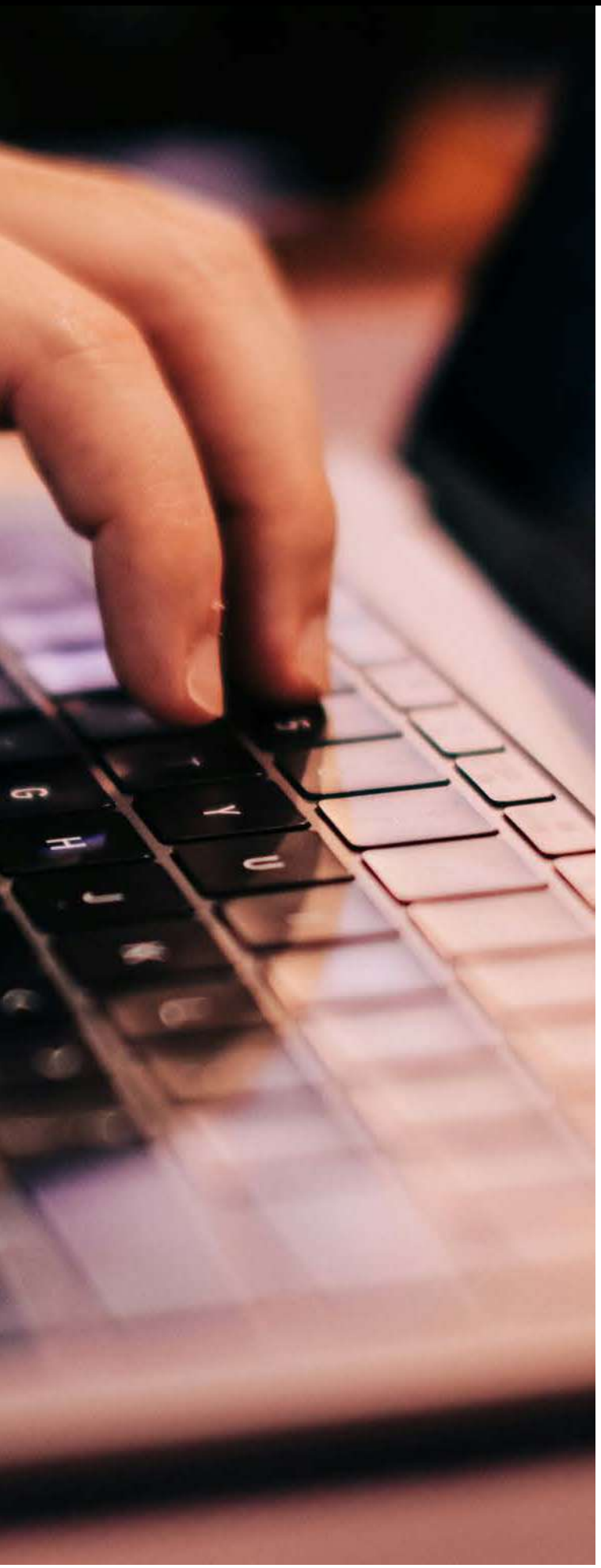
La declaración de Rocha funciona como diagnóstico. La ATDT reconoce que las instituciones públicas no cuentan con una capacidad operativa de detección y respuesta que permita contener a tiempo un ataque sofisticado.

Esa carencia, explicó la funcionaria, se traduce en que los incidentes pueden pasar meses sin ser detectados por la propia dependencia afectada, hasta que "ya es visible" y entonces la unidad de TI se enfrenta a un problema ya consolidado.

“El retraso en la identificación es parte del problema: en ocasiones se trabaja meses sin saberlo”, dijo Miguel Ángel Cañada durante el foro, al poner en perspectiva internacional el fenómeno y señalar que en ataques complejos la detección puede demorarse “o aproximadamente un ciberataque, entre los ocho o nueve meses hasta que es detectado por el que lo sufre”.

Para Rocha, la realidad operativa del gobierno federal está, por ahora, atada a proveedores y soluciones privadas. “Afortunadamente tenemos la parte de la industria de la que somos clientes nosotros en la Administración Pública Federal y esto nos sitúa en un nivel, digamos, pues no tan tan bajo a nivel nacional”, dijo la directora, señalando que el acceso a tecnología comercial reduce, pero no elimina, la brecha de protección.





Política de ciberseguridad

La ATDT propone un enfoque doble: elevar la madurez técnica de las dependencias y construir una **cultura de reporte y colaboración.** Rocha anunció la próxima publicación de una política general de ciberseguridad, acompañada de lineamientos y guías de implementación que, según la funcionaria, no pretenden ser “una normativa simplemente para que se cumpla en papel”, sino instrumentos de apoyo para la contención y remediación conjunta entre agencia y dependencias.

“Consideramos mejor hacer este reporte hacia la agencia y entrar a colaborar con las dependencias en la parte de la contención y la remediación”, dijo.

El componente humano aparece como otro eslabón débil. Desde la Secretaría de Seguridad y Protección Ciudadana, Patricia Chávez subrayó la necesidad de profesionalizar la investigación y la prevención.

La coordinación con 46 unidades de policía cibernética y la atención a fraudes que se generan por fallas básicas (contraseñas comprometidas, ingeniería social) son muestras de que la capacidad operativa debe ampliarse en todos los niveles (federal, estatal y municipal).
“La mayoría de los trámites son a nivel estatal y municipal”, dijo Chávez.

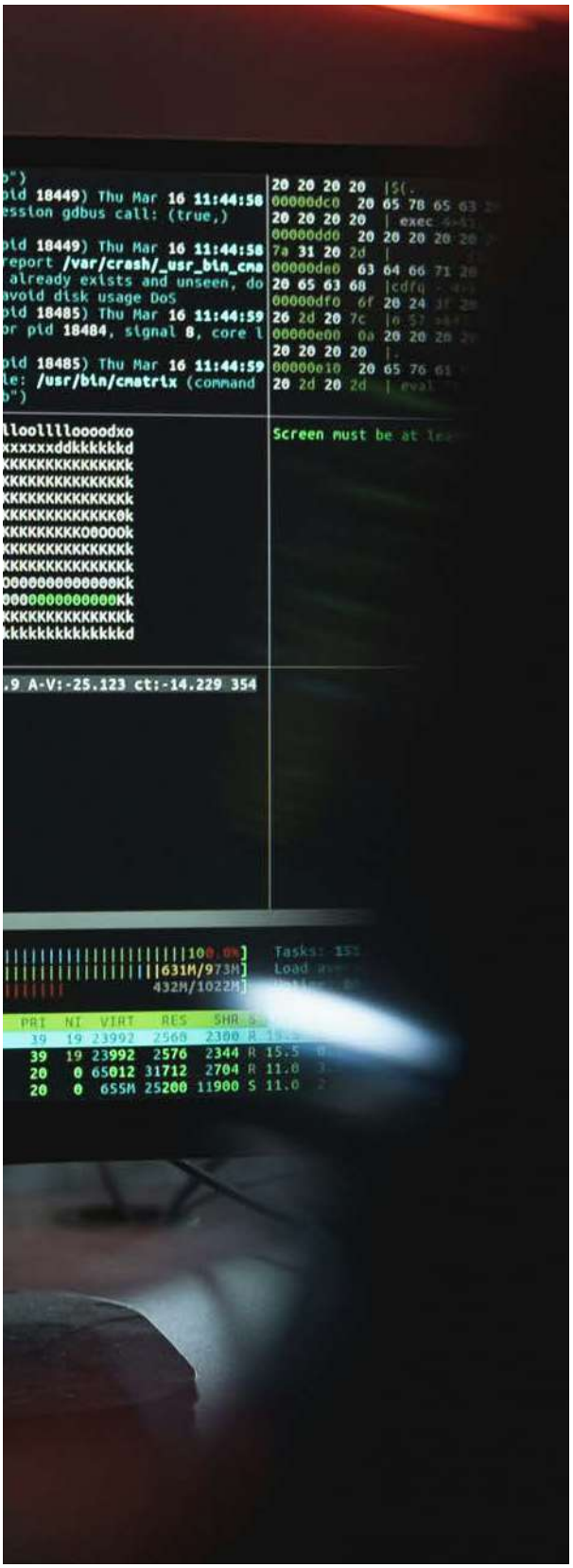
Creación de un CSOC

La directora de Ciberseguridad de la ATDT también advirtió problemas de gobernanza y trazabilidad. Sin métricas claras de madurez y sin mecanismos federados de intercambio de información, el diagnóstico y la priorización de inversiones serán fragmentarios.

La **ATDT** plantea, en el mediano plazo, construir un **Centro de Operaciones de Ciberseguridad (CSOC)**, es decir, un sistema de intercambio y monitoreo federado en materia de ciberseguridad, el cual permita compartir telemetría y coordinar respuestas a nivel internacional cuando la naturaleza de los ataques así lo requiera.

Los panelistas insistieron además en que no todo es tecnología puntera. "Estamos descuidando cosas muy básicas como diseño seguro, como administración de servidores", advirtió Rocha, quien urgió a reforzar prácticas elementales de higiene digital mientras se avanza hacia soluciones de frontera.

Mejorar la detección y respuesta, formar talento en masa y construir mecanismos federados de colaboración pública-privada. La intención no es lanzar una normativa para que se cumpla en papel, dijo Rocha, sino colaborar estrechamente con industria, academia y dependencias para elevar la madurez del Estado en ciberseguridad.



Fuente de información:
eleconomista.com.mx