PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EL FINANCIERO	8	22/02/2023	LEGISLATIVO

CUENTA PÚBLICA 2021

Advierte la ASF riesgo de *hackeo* en la CNBV

CRISTIAN TÉLLEZ
ctellez@elfinanciero.com.mx

La Auditoría Superior de la Federación (ASF) detectó en la Comisión Nacional Bancaria y de Valores (CNBV) una falta de planeación e implementación de la infraestructura de equipo de cómputo, con lo que puede correr el riesgo de sufrir un *hackeo*.

Como parte del tercer informe de revisión de la Cuenta Pública 2021, la ASF consideró que la CNBV presenta carencias en los controles de seguridad cibernética y se necesita fortalecerlos.

El órgano alertó que la CNBV debe reforzar el monitoreo y control de cuentas, las respuestas y gestión de incidentes, al igual que las restricciones en puertos y protocolos de seguridad.

La ASF en su auditoría consideró que "no se utiliza una herramienta de descubrimiento activo para identificar equipos conectados a la red; no se actualiza el inventario de activos de hardware dinámicamente".

El informe agrega que el organismo tampoco cuenta con un inventario actualizado, principalmente de aquellos equipos capaces de almacenar o procesar información, al igual que no cuenta con certificados de autenticidad para que la gente de confianza pueda usar la red interna.

Entre las recomendaciones que destacaron fue que "la CNBV elabore un proyecto normativo para que la Dirección General de Informática cuente con un manual específico que describa la estructura organizacional, objetivos y funciones de la totalidad de los roles que desempeñan actividades de tecnologías de información y comunicaciones".

Asimismo, señaló que la comisión carece de un plan de pruebas de respaldos a fin de verificar su integridad y garantizar que las copias de los respaldos funcionen correctamente y no cuenta un punto de autenticación centralizado para los sistemas de red, de seguridad y de la nube.

Añadieron que es con "el fin de tener trazabilidad en las actividades operativas y administrativas plasmadas y que éstas sean acordes con los perfiles de puesto del personal de esa dirección a fin de asegurar el uso eficiente y seguro de los recursos informáticos y de telecomunicaciones de la comisión"

Además, matizó que no se capacitó al personal en materia de seguridad de la información, ciberseguridad y los principales tipos de ciberataques y no se contó con un programa de concientización de *hackeo* formalizado.

En este aspecto, el reporte detalló que el personal de desarrollo de software tampoco recibió capacitación relacionada con la escritura de código seguro.

FOCOS

Presenta debilidad. Según el informe de la Auditoría, no se capacitó al personal de la CNBV en materia de seguridad de la información, ciberseguridad, así como sobre los principales tipos de ciberataques.

Está aislada. De acuerdo con el informe de la cuenta pública 2021 de la ASF, la CNBV no demostró tener comunicación con otras instancias de gobierno o centros de intercambio de información de incidentes.