PERIÓDICO	PÁGINA	FECHA	SECCIÓN
REFORMA	2	27/02/2023	LEGISLATIVO

Carece de inventario de información sensible.- ASF

Tiene CNBV protección débil en ciberseguridad

Cumple 25% de áreas con menos de lo que se requiere y en 40% debe fortalecerse

CHARLENE DOMÍNGUEZ

La Comisión Nacional Bancaria y de Valores (CNBV), responsable de regular, supervisar y sancionar entidades del sistema financiero, muestra debilidad en controles de ciberseguridad críticos.

Hay cinco rubros de ciberseguridad (25 por ciento) en semáforo rojo, que carecen de control al tener un nivel de cumplimiento menor a 30 por ciento de lo requerido, identificó la Auditoría Superior de la Federación (ASF).

Estos controles son protección de datos, activos de hardware, pruebas de penetración, programa de concientización de seguridad y acceso basado en necesidad de saber.

En protección de datos, la CNBV no tiene inventariada información sensible almacenada, procesada o transmitida por sus sistemas ni los que tiene con proveedores de servicio.

Además, carece de una metodología para clasificar datos y activos críticos, detalló la ASF.

"No se cuenta con una herramienta automatizada en el perímetro de la red para monitorear la transferencia no autorizada de información sensible.

"A pesar de que se monitorea la red, no se cuenta con mecanismos para detectar el uso no autorizado del cifrado de datos", sostuvo.

De igual manera, otros ocho controles (40 por ciento) de ciberseguridad de la la CNBV están en amarillo, pues requieren fortalecerse.

Estos controles son activos de software, seguridad perimetral, respuesta y gestión de incidentes, monitoreo y control de cuentas, así como control de acceso inalámbrico.

De igual manea, uso controlado de privilegios administrativos, mantenimiento, supervisión y análisis de registros de auditoría y la restricción y control de puertos, protocolos y servicios.

Sobre el monitoreo y control de cuentas, la Auditoría señaló que la CNBV no cuenta con un punto de autenticación centralizado para los sistemas de red, de seguridad y de la nube.

"Las cuentas de administración con privilegios elevados no utilizan autenticación de factores múltiples. Se carece de un proceso automatizado para la revocación de acceso a los sistemas, inmediatamente después de la terminación o cambio de responsabilidades.

"No se generan alertas por la desviación del comportamiento normal de inicio de sesión", expuso.

Solo en siete controles (35 por ciento), la CNBV alcanzó un nivel aceptable de cumplimiento.

Para evaluar la ciberseguridad de la CNBV, la Auditoría utilizó el marco CIS, que se refiere a los Controles Críticos de Seguridad del Centro de Seguridad de Internet para la infraestructura crítica de las TIC, es decir, el Centro de Datos, Telecomunicaciones, Seguridad Perimetral, Ambientes de Desarrollo y Controles de Acceso.

Puntos críticos

De 20 controles de ciberseguridad críticos, la CNBV presenta carencias en cinco de ellos.

Semáforo de madurez de los controles de ciberseguridad

● CARENCIA DE CONTROL ○ REQUIERE FORTALECER

- ● Protección de datos
- ● Control de acceso basado en necesidad de saber
- ● Inventario y control de activos de hardware
- ● Pruebas de penetración y ejercicios de equipo
- ● Programa de capacitación y concientización de seguridad
- ○ Respuesta y gestión incidentes
- ○ Control de acceso inalámbrico
- ○ Monitoreo y control de cuentas
- ○ Seguridad perimetral
- ○ Inventario y control de activos de software
- ○ Uso controlado de privilegios administrativos

Fuente: ASF