PERIÓDICO | PÁGINA | FECHA | SECCIÓN
La Jornada | 4 | 24/10/2025 | LEGISLATIVO

Incumplieron firmas que contrató la GN

ENRIQUE MÉNDEZ Y ARTURO SÁNCHEZ

Las empresas contratadas por la Guardia Nacional para la seguridad de sus sistemas de correo electrónico y de protección de datos no cumplieron los mecanismos para el resguardo de información y sistemas, concluyó la Auditoría Superior de la Federación (ASF).

En el análisis de la cuenta pública 2024 revisó distintos contratos para comunicación satelital semifija y vehicular, y transmisiones por radio, así como protección de correo electrónico y de los dispositivos ante amenazas cibernéticas.

Los auditores analizaron dos convenios con la firma NetControll Group por 11 millones 806 mil pesos y 43 millones 183 mil 200, respectivamente.

El primero se refiere al servicio de cifrado de correo electrónico de la Guardia Nacional, que incluía una solución avanzada para resguardo de punto a punto del contenido enviado, con la finalidad de brindar y mantener la comunicación segura dentro y fuera de la red institucional, y que contenía soporte técnico.

No obstante, la ASF corroboró que "la solución no contó con la capacidad de detección de ataques personalizados dirigidos ni se habilitó el cifrado mediante certificados; tampoco se acreditó un diseño de alta disponibilidad para el servicio que fuera compatible con el esquema de *email* de la corporación".

También faltó que implementara la integración mediante interfaz de programación de aplicaciones con los sistemas, y no se justificó la falta de esta medida de seguridad, indicó la Auditoría. Además, careció de procesos de notificación a usuarios respecto a la detección de amenazas y no se previeron umbrales para el análisis de patrones de comportamiento de riesgo.

El segundo contrato se refiere al servicio de protección de los dispositivos finales de la Guardia Nacional, como equipos de cómputo y servidores ante amenazas de software malicioso, suplantación de identidad, ingeniería social, ataques de fuerza bruta, denegación de servicios y secuestro de datos, también acompañadas de soporte técnico.

Empero, la ASF confirmó: "no se acreditó que la plataforma incluyera capacidades de análisis de vulnerabilidades ni prevención contra código que explota una vulnerabilidad e identificación de ataques posexplotación".