Costo: $	Impacto: ALTO	Complejidad: BAJA

4.A: ¿Tiene el WWS un procedimiento escrito para informar incidentes de ciberseguridad, incluyendo cómo hacerlo (p. ej., llamada telefónica, envío por Internet) y a quién (p. ej., FBI u otra fuerza de aplicación de la ley como la CISA, reguladores estatales, WaterISAC, proveedor de seguro informático)?

Recomendación: Documente el procedimiento para informar incidentes de ciberseguridad con prontitud para prestar mejor ayuda a las fuerzas de aplicación de la ley, recibir asistencia con la respuesta y recuperación y promover la concientización en el sector del agua sobre las amenazas de ciberseguridad.

¿Por qué es importante este control?

Informar incidentes a agencias externas puede ayudar a los WWS a responder mejor y recuperarse de un incidente de ciberseguridad. La información transmitida también puede ayudar a evitar que se produzcan delitos informáticos en otros WWS y organizaciones, así como proporcionar información sobre tendencias y concientización en el sector del agua.

Consejos de implementación

Desarrolle un procedimiento y una plantilla de informe para informar incidentes de ciberseguridad con prontitud.

Identifique al personal del WWS responsable de informar a organizaciones externas.

Especifique los procedimientos de escalamiento (p. ej., a quién notificar) para informar a las organizaciones externas identificadas y los plazos para transmitir la información. Los diagramas de flujo u otros elementos visuales pueden ayudar al personal del WWS a comprender en qué orden deben notificar a otros y qué información deben transmitir.

Distribuya el procedimiento y la plantilla de informe al personal del WWS. Incluya esta información en otros documentos de respuesta a emergencias, como su plan de respuesta a emergencias o plan de respuesta a incidentes de ciberseguridad.

En virtud de la Ley de Informes de Incidentes Informáticos para Infraestructura Crítica (CIRCIA) de 2022, la CISA del DHS debe emitir regulaciones, que deben pasar por un proceso de notificación y comentarios, que exijan que las entidades cubiertas informen los incidentes informáticos cubiertos y los pagos de rescate hechos como consecuencia de un ataque de *ransomware* a la CISA. La Notificación de Propuesta de Reglamentación de la CISA propone aplicar estos requisitos a al menos algunas entidades en los WWS. La EPA revisará esta guía según sea necesario cuando la CISA emita la Norma Final de la CIRCIA. Si el WWS está suscrito a un seguro informático o tiene un proveedor de servicios de respuesta a incidentes informáticos, incluya a estos proveedores como contactos dentro del procedimiento escrito. A menudo, existen plazos de presentación de informes obligatorios asociados con la presentación de reclamos contra el seguro informático o los proveedores de servicios de respuesta a incidentes.

ORIENTACIÓN ADICIONAL

El procedimiento escrito debe incluir información de contacto para informar a:

- La agencia local de aplicación de la ley del WWS.
- CISA del DHS: las organizaciones deben enviar un informe de incidentes de la CISA en línea, enviar un correo electrónico a report@cisa.gov o llamar al 888-282-0870.
- Oficina Federal de Investigación (FBI): las organizaciones deben comunicarse con la oficina local del FBI más cercana o presentar un informe a través del Centro de Quejas de Delitos en Internet (IC3) del FBI.
- WaterISAC y los centros de fusión locales/estatales: para informar a WaterISAC, el WWS puede presentar un informe WaterISAC en línea, enviar un correo electrónico a analyst@waterisac.org o llamar al 866-426-4722.
- El proveedor del seguro informático del WWS o el titular de un contrato de respuesta a incidentes informáticos (si corresponde).

La plantilla de informe debe incluir lo siguiente:

- Fecha y hora en que el WWS detectó el incidente.
- Fecha y hora en que ocurrió el incidente.
- Breve descripción del incidente, incluyendo la identificación del método del potencial ataque.
- Lista de activos afectados.
- Identificación de cualquier información de identificación personal (PII) que el incidente pueda haber comprometido.
- Fecha, hora y descripción de las medidas correctivas/de respuesta que el WWS llevó a cabo.
- Personal del WWS/distribuidor(es) involucrado en la detección y respuesta al incidente.

La información que el WWS comparte con el DHS, el FBI o cualquier otra agencia del gobierno federal, puede ser elegible para recibir protección en virtud del Programa de Información de Infraestructura Crítica Protegida (PCII). Para obtener más información sobre qué puede calificar para la protección del PCII y los procedimientos a seguir para solicitar protección del PCII, consulte la hoja informativa sobre el PCII de la CISA.

Recursos

Informar a la CISA del DHS: Proporciona información sobre cómo informar incidentes y actividades sospechosas. *https://www.cisa.gov/report*

Informar al FBI: Proporciona información sobre cómo denunciar delitos informáticos. *https://www.fbi.gov/investigate/cyber*

Informar a WaterISAC: Proporciona información sobre cómo denunciar incidentes y actividades sospechosas. *https://www.waterisac.org/report-incident*

Guía de plantillas de gestión de políticas del NIST: Consulte el SOP y la plantilla de informe para informar sobre incidentes de ciberseguridad que se distribuye a todo el personal de la empresa de servicios públicos. *https://www.cisecurity.org/wp-content/uploads/2020/06/Computer-Security-Threat-Response-Policy.docx*

Hoja informativa sobre el PCII de la CISA del DHS: Explica las protecciones que ofrece el programa PCII. *https://www.cisa.gov/publication/pcii-fact-sheet*; *https://www.cisa.gov/resources-tools/programs/Protegered-critical-infrastructure-information-pcii-program/submit-critical-infrastructure-information*

Hojas informativas de respuesta a incidentes informáticos de la CISA del DHS: Esta guía se puede utilizar para ayudar a mejorar la planificación de respuesta a incidentes y colaborar con socios federales. *https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf*