Costo: $	Impacto: MEDIO	Complejidad: BAJA

5.A: ¿Tiene el WWS la capacidad de recuperarse de manera segura y efectiva de un incidente de ciberseguridad?

Recomendación: Desarrolle, mantenga y ejecute planes para recuperar y restaurar activos o sistemas críticos para la misión o la actividad comercial que podrían verse afectados por un incidente de ciberseguridad.

¿Por qué es importante este control?

La planificación de contingencias para los sistemas de TO y TI del WWS es parte de un programa general para lograr la continuidad de las operaciones para las funciones de la misión y comerciales de la empresa de servicios públicos. La planificación de contingencias aborda la restauración del sistema y la implementación de procesos comerciales o de misión alternativos cuando los sistemas de TO y TI se ven comprometidos o sufren filtraciones.

Consejos de implementación

Coordine y pruebe el desarrollo de un plan de contingencia con los departamentos de servicios públicos responsables de los planes relacionados (p. ej., ERP del WWS).

Asegúrese de que exista la capacidad necesaria para el procesamiento de la información, las telecomunicaciones y el soporte de operaciones durante las interrupciones de TO y TI.

Planifique la reanudación de las funciones esenciales de la misión y comerciales dentro de un tiempo definido a partir de la activación del plan de contingencia y pruebe este tiempo de respuesta.

ORIENTACIÓN ADICIONAL

- Desarrolle un plan de contingencia que:
  - Identifique las funciones de la misión y comerciales esenciales del WWS y los requisitos de contingencia asociados.
  - Proporcione objetivos de recuperación, prioridades de restauración y métricas.
  - Aborde las funciones, las responsabilidades y las personas asignadas para las contingencias con información de contacto.
  - Aborde el mantenimiento de las funciones de la misión y comerciales esenciales a pesar de una interrupción, compromiso o falla del sistema de TO o TI.
  - Aborde la eventual restauración total del sistema.
  - Aborde el intercambio de información de contingencia.
  - Sea revisado y aprobado por el líder de ciberseguridad del WWS.
- Distribuya copias del plan de contingencia según sea necesario.
- Coordine las actividades de planificación de contingencias con las actividades de manejo de incidentes.
- Revise el plan de contingencia del WWS con una frecuencia determinada.
- Incorpore en el plan las lecciones aprendidas a partir de las pruebas, la capacitación o la implementación del plan de contingencia.
- Proteja el plan de contingencia de la divulgación y modificación no autorizadas.

Planifique la continuación de las funciones esenciales de la misión y comerciales con una pérdida mínima o nula de la continuidad operacional y mantener esa continuidad hasta que todos los sistemas de TO y TI se restauren por completo.

Coordine y pruebe su plan de contingencia con los planes de contingencia de los proveedores de servicios externos (p. ej., el distribuidor de SCADA) según corresponda para garantizar que se puedan satisfacer los requisitos de contingencia.

Identifique los activos críticos de TO y TI del WWS que respaldan las funciones esenciales de la misión y comerciales (consulte la hoja informativa 1.A).

Recursos

Lista de verificación de medidas a incidentes de ciberseguridad de la EPA: Esta lista de verificación describe las medidas que las empresas de servicios públicos de agua potable y aguas residuales pueden tomar para prepararse, responder y recuperarse ante incidentes informáticos.
https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf

Plantilla de respuesta a incidentes informáticos de la EPA: Esta plantilla personalizable se puede utilizar como punto de partida para crear el plan de respuesta a incidentes de ciberseguridad de su empresa de servicios públicos, diseñado para ayudar a su empresa de servicios públicos a responder a un incidente informático.
https://www.epa.gov/waterresilience/cybersecurity-planning

Publicación especial 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Esta publicación proporciona un catálogo de controles de seguridad y privacidad para sistemas de información y organizaciones para proteger las operaciones y los activos de la organización, a las personas y a otras organizaciones de un conjunto diverso de amenazas y riesgos, incluyendo ataques hostiles, errores humanos, desastres naturales, fallas estructurales, entidades de inteligencia extranjeras y riesgos de privacidad. Consulte la sección 3.6, “Contingency Planning” (Planificación de contingencias) y la tabla C-6, “Contingency Planning Family” (Familia de planificación de contingencias).
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Capacitación sobre respuesta a incidentes: La CISA ofrece cursos gratuitos de capacitación sobre respuesta a incidentes (IR) para empleados gubernamentales y contratistas de los gobiernos federal, estatales, locales, tribales y territoriales, socios educativos y de infraestructura crítica y el público en general.
https://www.cisa.gov/incident-response-training

Guía 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

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 1 (Planificar para incidentes, emergencias y desastres) proporciona información sobre la planificación de respuesta.
https://www.waterisac.org/fundamentals