Costo: $	Impacto: ALTO	Complejidad: BAJA

2.I: ¿Proporciona/realiza el WWS capacitaciones anuales de concientización sobre ciberseguridad para todo el personal del WWS que cubran conceptos básicos de ciberseguridad?

Recomendación: Realice una capacitación de concientización sobre ciberseguridad, como mínimo anualmente, para ayudar a que todos los empleados comprendan la importancia de la ciberseguridad y cómo evitar los ataques informáticos y responder a ellos.

¿Por qué es importante este control?

To help create and maintain a culture of cybersecurity, your WWS should provide regular, basic cybersecurity training to all personnel. While cybersecurity covers many areas, there are certain basic security concepts that should be frequently emphasized to promote better cyber practices. Regularly trained personnel are more likely to identify and respond quickly to a potential cyber incident or prevent one from occurring altogether. Regular training is also critical as cybersecurity threats constantly evolve.

Consejos de implementación

Establezca un cronograma para realizar capacitaciones periódicas para todo el personal del WWS que cubran los conceptos básicos de ciberseguridad. La capacitación debe realizarse anualmente, como mínimo.

Establezca una política que requiera que los empleados nuevos reciban una capacitación inicial sobre ciberseguridad dentro de los 10 días posteriores a su incorporación. La capacitación debe considerar la función del empleado nuevo y cubrir temas básicos de seguridad.

ORIENTACIÓN ADICIONAL

- Desarrolle una agenda para la capacitación que cubra conceptos básicos de ciberseguridad, como el robo de identidad, la vulneración del correo electrónico comercial, la seguridad de las contraseñas, las últimas tendencias y amenazas en ingeniería social y las buenas prácticas de higiene informática. La ingeniería social es una forma común de estafar a las personas a través de las redes sociales (p. ej., Facebook) y la interacción humana (p. ej., correo electrónico) para obtener información sensible y acceso. Utilice conceptos de capacitación que sean familiares para el personal de WWS, incluyendo ejemplos reales basados en el equipo y los sistemas utilizados por el WWS. Por ejemplo, si el WWS les entrega teléfonos inteligentes a los empleados, incluya capacitación específica relacionada con la seguridad de los teléfonos inteligentes. Dado que es probable que todo el personal reciba correo electrónico, la capacitación siempre debe incluir las buenas prácticas de ciberseguridad para revisar y abrir correos electrónicos.
- Desarrolle los materiales de capacitación de manera que sean fáciles de seguir y que el personal pueda consultarlos más adelante. Actualice las presentaciones de PowerPoint, los módulos de aprendizaje en línea y los folletos para cada capacitación. Proporcione enlaces a recursos adicionales donde el personal del WWS pueda aprender más sobre temas de ciberseguridad. Para mantener la ciberseguridad relevante y actualizada, considere agregar un segmento breve sobre ciberseguridad en las reuniones y sesiones informativas del personal del WWS para compartir un consejo rápido o información relacionada con la ciberseguridad.

ORIENTACIÓN ADICIONAL

- El personal al que los atacantes suelen dirigirse, como ejecutivos, asistentes ejecutivos, ingenieros, personal de SCADA, personal de TI, operadores y personal de recursos humanos y finanzas, debe recibir una capacitación más especializada. Hay muchas oportunidades de capacitación gratuitas disponibles en línea y de manera presencial, incluyendo las de la CISA y la NICCS (consulte los recursos a continuación).

Recursos

Capacitación sobre ciberseguridad para sistemas de agua de la EPA: *https://www.epa.gov/waterresilience/cybersecurity-exercises-and-technical-assistance-courses*

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 3 (Crear una cultura de ciberseguridad y proteger contra los riesgos internos) proporcionan información sobre cómo crear una cultura de ciberseguridad en una empresa de servicios de agua potable y aguas residuales, lo que incluye ofrecer formación en materia de ciberseguridad al personal de estas empresas. *https://www.waterisac.org/fundamentals*

Estándar 800-50 (revisión 1) del NIST Creación de un Programa de aprendizaje sobre ciberseguridad y privacidad: Proporciona orientación a las agencias y organizaciones federales para desarrollar y gestionar un enfoque de ciclo de vida para crear un Programa de aprendizaje sobre ciberseguridad y privacidad (CPLP). *https://csrc.nist.gov/pubs/sp/800/50/r1/final*

Estándar 800-82 (revisión 3) del NIST, Guía para la seguridad de la tecnología operacional (TO): La sección 6.2.2 en la página 108 proporciona orientación para capacitación sobre TO. *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

Guía de plantillas de políticas del NIST: Consulte la Política de capacitación y concientización sobre seguridad. Contiene cronogramas de capacitación, registros, presentaciones, etc. que demuestran que esta capacitación se lleva a cabo como mínimo anualmente. *https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Awareness-and-Training-Policy.docx*

Capacitación de la CISA del DHS: Proporciona capacitación en línea sin costo sobre una variedad de temas de ciberseguridad. *https://www.cisa.gov/cybersecurity-training-exercises*

Portal de aprendizaje virtual de la CISA del DHS: Proporciona capacitación en línea sin costo sobre una variedad de temas de ciberseguridad. *https://www.cisa.gov/resources-tools/training/ics-virtual-learning-portal*

NICCS Aprendizaje CISA: Proporciona capacitación gratuita en línea sobre ciberseguridad para empleados de gobiernos estatales, locales, tribales y territoriales. *https://niccs.cisa.gov/education-training/cisa-learning*

StopRansomware.gov: Esta es la ubicación única oficial del gobierno de EE. UU. donde encontrará recursos para abordar el *ransomware* de manera más efectiva.
https://www.cisa.gov/stopransomware

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 8 de la página 3 de este recurso para obtener información adicional.
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems