**Guía de la EPA Para Mejorar la Ciberseguridad en Sistemas de Agua Potable y Aguas Residuales**

**Descargo de responsabilidad**

La División de Infraestructura Hídrica y Resiliencia Informática de la Oficina de Aguas Subterráneas y Agua Potable revisó y aprobó este documento para su publicación. Este documento no impone requisitos legales sobre ninguna de las partes. Ni el Gobierno de Estados Unidos ni sus empleados, contratistas, o los empleados de estos, dan garantías, expresas o implícitas, ni asumen ninguna responsabilidad legal por el uso por parte de terceros de la información, los productos o los procesos que se analizan en este documento, ni suponen que su uso por parte de terceros infringiría derechos de propiedad privada. La mención de nombres o productos comerciales no constituye un aval ni una recomendación de uso. Además, la orientación que proporciona este documento sirve como una guía voluntaria para ayudar a las entidades de agua y aguas residuales con el fin de evaluar, comprender y combatir los riesgos informáticos para sus operaciones, [activos](#Glossary) organizacionales y personas.

**Índice**

[1.0 Antecedentes 1](#_Toc183698421)

[1.1. ¿Cuál es el propósito de esta publicación? 1](#_Toc183698422)

[1.2. Usos opcionales de la orientación que proporciona esta publicación 1](#_Toc183698423)

[2.0 Asistencia técnica para mejorar la ciberseguridad
en sistemas de agua y aguas residuales 2](#_Toc183698424)

[2.1. Asistencia técnica sobre ciberseguridad 3](#_Toc183698425)

[2.2. Herramientas y orientación sobre ciberseguridad 3](#_Toc183698426)

[2.3. Capacitación sobre ciberseguridad 5](#_Toc183698427)

[2.4. Recursos financieros para ciberseguridad 5](#_Toc183698428)

[3.0 Lista de verificación de ciberseguridad de la EPA para sistemas de agua potable y aguas residuales 6](#_Toc183698429)

[3.1. ¿Qué es la Lista de verificación de ciberseguridad de la EPA? 6](#_Toc183698430)

[3.2. ¿Cómo deben utilizar los WWS la Lista de verificación
de ciberseguridad de la EPA? 6](#_Toc183698431)

[3.3. ¿Cuáles son las alternativas a la Lista de verificación
de ciberseguridad de la EPA? 6](#_Toc183698432)

[4.0 Prácticas prioritarias de ciberseguridad para sistemas de agua y aguas residuales 7](#_Toc183698433)

[5.0 Riesgos de la inteligencia artificial para los sistemas de agua y aguas residuales 13](#_Toc183698434)

[APÉNDICE A: Lista de Verificación de Ciberseguridad de la EPA para Sistemas de Agua Potable y Aguas Residuales A-1](#_Toc193960095)

[APÉNDICE B: Hojas Informativas de la Lista de Verificación de la EPA B-1](#_Toc193960096)

[APÉNDICE C: Glosario de Términos C-1](#_Toc193960097)

# Antecedentes

## ¿Cuál es el propósito de esta publicación?

La Agencia de Protección Ambiental de Estados Unidos (EPA) elaboró esta publicación para ayudar a los propietarios y operadores de sistemas de agua potable y aguas residuales (WWS) con el fin de evaluar las deficiencias en sus prácticas y [controles](#Glossary) de ciberseguridad actuales, e identificar medidas que pueden reducir el riesgo de sufrir ataques informáticos. Además, como se describe en la sección 1.2, los propietarios y operadores de sistemas de agua comunitaria (CWS) sujetos a los requisitos de la sección 1433 de la Ley de Agua Potable Segura (SDWA) (según las enmiendas de la [*Ley de Infraestructura Hídrica de Estados Unidos*](https://www.epa.gov/ground-water-and-drinking-water/americas-water-infrastructure-act-2018-awia)) pueden usar esta guía como opción para abordar la ciberseguridad en [evaluaciones de riesgos y resiliencia](#Glossary) y en [planes de respuesta a emergencias](#Glossary).

Los WWS son a menudo objeto de actividad informática maliciosa que posee el potencial para interferir en las operaciones y puede dar lugar a elevados costos de respuesta y recuperación. Un ataque informático sobre un WWS vulnerable puede ser especialmente preocupante, ya que podría permitir a un rival manipular [tecnología operacional (TO)](#Glossary) y esto podría alterar la producción de agua limpia y segura. Por consiguiente, los propietarios y operadores de los WWS deben evaluar sus prácticas y controles de ciberseguridad de manera periódica y tener en cuenta las medidas que pueden reducir sus riesgos. Esto ayudará a evitar que los WWS sufran un ataque informático y asistirá en la respuesta en caso de que ocurra uno.

Específicamente, los propietarios y operadores de los WWS deben evaluar cómo el uso de la [tecnología de la información (TI)](#Glossary) y la TO en sus operaciones, equipos y redes, junto con la evolución de los estándares y las recomendaciones de ciberseguridad, la nueva información disponible sobre amenazas informáticas y otras consideraciones, pueden justificar una reevaluación de sus prácticas y controles de ciberseguridad. Esta guía y los recursos técnicos adicionales que figuran en la sección 2 pueden ayudar a los propietarios y operadores de los WWS con esta evaluación.

## Usos opcionales de la orientación que proporciona esta publicación

La EPA recomienda que todos los propietarios y operadores de los WWS, sin importar el tipo de sistema y la población a la que prestan servicios, evalúen los riesgos y la resiliencia de sus sistemas de TI y TO ante amenazas informáticas y desarrollen planes de mitigación de riesgos para abordar las vulnerabilidades informáticas en operaciones críticas. La orientación de esta publicación es un método para ayudar a los propietarios y operadores de los WWS con estas medidas esenciales:

* Evaluar las prácticas y los controles actuales de ciberseguridad de los WWS para identificar posibles vulnerabilidades a las amenazas informáticas.
* Desarrollar un plan con medidas específicas, recursos, cronogramas y responsabilidades para reducir el riesgo y mejorar la resiliencia a los ataques informáticos.
* Identificar recursos adicionales para ayudar a mejorar la ciberseguridad.

Además, los propietarios y operadores de los CWS que prestan servicio a más de 3 300 personas tienen la obligación, en virtud de la sección 1433 de la SDWA, de considerar la ciberseguridad cuando desarrollan o actualizan [evaluaciones de riesgos y resiliencia y planes de respuesta a emergencias](https://www.epa.gov/waterresilience/awia-section-2013). El cumplimiento de la sección 1433 de la SDWA exige lo siguiente:

* Evaluar los riesgos y la resiliencia de las tuberías y las transmisiones construidas, las barreras físicas, las fuentes de agua, la recolección y admisión de agua, las instalaciones de tratamiento previo, tratamiento, almacenamiento y distribución, los sistemas electrónicos, informáticos u otros sistemas automatizados (incluyendo la seguridad de estos sistemas) que utiliza el sistema; las prácticas de monitoreo del sistema; la infraestructura financiera del sistema; el uso, el almacenamiento o la manipulación de distintos productos químicos por parte del sistema; y la gestión y el mantenimiento del sistema; y puede incluir una evaluación de las necesidades de capital y operacionales para la gestión de riesgos y resiliencia del sistema.
* Preparar o revisar, cuando sea necesario, un plan de respuesta a emergencias que incorpore los resultados de la evaluación, que deberá incluir estrategias y recursos para mejorar la resiliencia del sistema, incluyendo la seguridad física e informática del sistema.

La orientación en esta publicación proporciona un enfoque que los propietarios y operadores de los CWS sujetos a la sección 1433 de la SDWA pueden seguir para cumplir estos requisitos. Como opción, varias de las herramientas y los recursos de otras organizaciones gubernamentales y del sector privado que se incluyen en la sección 2 de esta publicación también son métodos efectivos para abordar la ciberseguridad en virtud de la sección 1433 de la SDWA.

# Asistencia técnica para mejorar la ciberseguridad en sistemas de agua y aguas residuales

Existe asistencia técnica, orientación, herramientas, capacitación y financiación que pueden ayudar a los propietarios y operadores de los WWS a mejorar la ciberseguridad disponible a través de la EPA y otras organizaciones gubernamentales y del sector privado. En esta sección, se resumen programas y recursos clave. Existe información adicional disponible de asistencia sobre ciberseguridad para los WWS en el sitio web de [*Ciberseguridad para el sector del agua de la EPA*](https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector).

Este apoyo de la EPA y otras organizaciones gubernamentales y del sector privado puede ayudar a los propietarios y operadores de los WWS a identificar deficiencias en sus prácticas de ciberseguridad actuales y a adoptar nuevas medidas para reducir el riesgo y crear resiliencia. Además, puede facilitar abordar la ciberseguridad en las evaluaciones de riesgos y resiliencia y en los planes de respuesta a emergencias de los CWS que deben cumplir con la sección 1433 de la SDWA.

## Asistencia técnica sobre ciberseguridad

* El [*Programa de asistencia técnica sobre ciberseguridad para el sector del agua*](https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector)de la EPA responde preguntas o solicitudes enviadas para consultar con un experto en temas de ciberseguridad de los WWS. El tiempo de respuesta planificado es dos días hábiles por correo electrónico o teléfono. Toda la asistencia es remota.
	+ Nota: Este programa no se dedica a temas de respuesta o recuperación de incidentes informáticos. Los informes de incidentes informáticos se redireccionarán a la Oficina Federal de Investigación (FBI) o a la [Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) del Departamento de Seguridad Nacional (DHS)](#Glossary). Otras preguntas fuera del alcance de este programa se redireccionarán a recursos alternativos.
* El [*Programa de evaluación de ciberseguridad para el sector del agua*](https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program)de la EPA lleva a cabo evaluaciones de ciberseguridad de los WWS. Las evaluaciones se realizan con la Lista de verificación de ciberseguridad de la EPA que se incluye en la sección 3. Los resultados de las evaluaciones se usan para desarrollar un plan de mitigación de riesgos de ciberseguridad con medidas prioritarias.
* Los [*Asesores de ciberseguridad (CSA) de la CISA*](https://www.cisa.gov/about/regions)ofrecen asistencia sobre ciberseguridad a propietarios y operadores de infraestructura crítica y a gobiernos estatales, locales, tribales y territoriales. Los CSA pueden proporcionar información sobre los productos y servicios de ciberseguridad de la CISA y actuar como enlace a los programas de informática de la CISA. Los CSA también se dedican a temas de respuesta a incidentes informáticos.
* El programa [*Análisis gratuito de vulnerabilidades informáticas para empresas de servicios públicos de agua*](https://www.cisa.gov/sites/default/files/2023-09/23-05187d%20-%20Water%20Vulnerability%20Scanning%20Fact%20SheetV2_508c.pdf) de la CISA utiliza herramientas automatizadas para hacer un análisis de [vulnerabilidades](#Glossary) en redes externas. Estas herramientas buscan vulnerabilidades y [configuraciones](#Glossary) débiles que los rivales puedan aprovechar para cometer un ataque informático. La EPA recomienda que los WWS se inscriban en este programa.
* El [*Programa Circuit Rider*](https://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program-technical-assistance-rural-water-systems) del área de Desarrollo Rural del Departamento de Agricultura de Estados Unidos proporciona asistencia técnica a sistemas de agua rurales que experimentan problemas operacionales, financieros y gerenciales diarios. Este servicio está disponible en cada estado y territorio.

## Herramientas y orientación sobre ciberseguridad

* La [*Herramienta de evaluación de ciberseguridad para sistemas de agua*](https://www.epa.gov/system/files/documents/2024-08/epa-water-cybersecurity-assessment-tool-3.1_links.xlsx) de la EPA consiste en una autoevaluación de un WWS para identificar deficiencias de ciberseguridad y desarrollar un plan de mitigación de riesgos de ciberseguridad. Este programa se basa en la Lista de verificación de ciberseguridad de la EPA (consulte la sección 3). El [*Programa de asistencia técnica sobre ciberseguridad para el sector del agua*](https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector) de la EPA asiste a un WWS mediante una evaluación de ciberseguridad y un desarrollo de planes de mitigación de riesgos de un tercero.
* La CISA ofrece varios productos y herramientas que sirven de orientación para fortalecer la seguridad y resiliencia de instalaciones de infraestructura crítica, incluyendo los WWS, contra ataques informáticos.
* El [*Kit de herramientas de ciberseguridad para sistemas de agua y aguas residuales*](https://www.cisa.gov/water) de la CISA destaca los recursos de la CISA que ofrecen protección contra los ataques informáticos y reducen sus impactos.
* El sitio web [*Buenas prácticas de ciberseguridad*](https://www.cisa.gov/topics/cybersecurity-best-practices)de la CISA incluye información sobre varias áreas de actividad y programas sobre ciberseguridad para organizaciones y personas.
* El sitio web de [*Amenazas y avisos informáticos*](https://www.cisa.gov/topics/cyber-threats-and-advisories) de la CISA ofrece información actualizada sobre amenazas informáticas, agentes de amenazas, detección de incidentes y respuesta e incluye el acceso a [*Alertas y avisos de ciberseguridad*](https://www.cisa.gov/news-events/cybersecurity-advisories), que se actualizan con frecuencia a medida que se dispone de información nueva sobre amenazas y vulnerabilidades informáticas.
* La [*Herramienta de evaluación de ciberseguridad (CSET)*](https://www.cisa.gov/downloading-and-installing-cset) es una herramienta de [*software*](#Glossary) de escritorio que sirve de guía a los propietarios y operadores de activos en un proceso paso a paso que les permite evaluar las prácticas de seguridad del [sistema de control industrial (ICS)](#Glossary) y de la red de TI.
* De igual forma, la [*Revisión de resiliencia informática*](https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr)es una evaluación basada en entrevistas de la capacidad de una organización de gestionar el riesgo informático durante las operaciones habituales y en momentos de crisis.
* El [*Instituto Nacional de Estándares y Tecnología*](https://www.nist.gov/cybersecurity) (NIST) del Departamento de Comercio de Estados Unidos desarrolla estándares y pautas de ciberseguridad para infraestructura crítica, agencias federales y el público. El [*Marco de ciberseguridad*](https://www.nist.gov/cyberframework) del NIST es una lista voluntaria y estructurada de resultados de ciberseguridad que las organizaciones en diversos sectores de infraestructura crítica pueden usar para evaluar, priorizar y comunicar sus iniciativas en materia de ciberseguridad.
* El Centro de Intercambio y Análisis de Información sobre Agua ([*WaterISAC*](https://www.waterisac.org/)) es un servicio por suscripción que ofrece datos, casos prácticos y análisis relacionados con amenazas de seguridad a sistemas de agua, incluyendo delitos informáticos, y proporciona recursos para respaldar la respuesta, la mitigación y las iniciativas de resiliencia.
* La Asociación Americana de Obras Hídricas ([*AWWA*](https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance)) proporciona numerosos recursos para evaluar la exposición a riesgos informáticos, establecer prioridades y ejecutar una estrategia de ciberseguridad proactiva en los WWS.
	+ La [*Guía de gestión de riesgos de ciberseguridad para el sector del agua*](https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960) aborda la protección de los ICS en los WWS contra los ataques informáticos.
	+ La [*Herramienta de gestión de riesgos de ciberseguridad para el sector del agua*](https://cybersecurity.awwa.org/?_gl=1*1qxeadh*_ga*MzA1NDk2NDg3LjE3MTUwMDA1MzI.*_ga_V6LK6LPN9V*MTcxNjA3MDE3My4yLjEuMTcxNjA3MDc4OC42MC4wLjA.)usa respuestas a preguntas sobre aplicaciones de tecnología en un WWS para generar una lista prioritaria de controles que pueden ayudar a identificar y mitigar vulnerabilidades de ciberseguridad.
	+ La [*Guía de gestión de riesgos de ciberseguridad para sistemas pequeños del sector del agua*](https://www.awwa.org/wp-content/uploads/WaterSectorCybersecurityRiskMgmt.pdf)está diseñada para ayudar a los WWS que prestan servicio a menos de 10 000 personas y, especialmente, a aquellos que prestan servicio a menos de 3 300 personas, a mejorar sus prácticas de ciberseguridad.

## Capacitación sobre ciberseguridad

* La [*Capacitación sobre ciberseguridad*](https://www.epa.gov/waterresilience/cybersecurity-training) de la EPA ofrece capacitación presencial y virtual sobre buenas prácticas de ciberseguridad, evaluaciones de vulnerabilidades y desarrollo de planes de mitigación de riesgos para los WWS.
* La Asociación Nacional de Aguas Rurales (NRWA) ofrece capacitación sobre ciberseguridad y apoyo para ayudar a los WWS pequeños y rurales que prestan servicio a menos de 10 000 personas.
* El [*programa de educación informática*](https://nrwa.org/issues/cybersecurity/) de la NRWA ayudará a los WWS pequeños a gestionar sus riesgos de ciberseguridad mediante: (1) la creación de un programa de capacitación orientado a sistemas pequeños, (2) la capacitación de Circuit Riders para ayudar a que los sistemas pequeños gestionen los riesgos de ciberseguridad, y (3) la integración con otras iniciativas de ciberseguridad para WWS.
* La NRWA ha establecido una [*asociación con WaterISAC*](https://content.nrwa.org/home/news/15663771/national-rural-water-association-nrwa-national-rural-water-association-and-waterisac-collaborate-to-benefit-small-water-utilities-nationwide) para los miembros de la NRWA que prestan servicio a poblaciones de 3 300 personas o menos. Los miembros elegibles recibirán una actualización sobre resiliencia de seguridad de WaterISAC y tendrán acceso a seminarios web mensuales de informes sobre amenazas de ISAC, así como a su centro de recursos.

## Recursos financieros para ciberseguridad

* La página web [*Financiación para ciberseguridad*](https://www.epa.gov/waterresilience/cybersecurity-funding)de la EPA proporciona información sobre programas federales que proporcionan financiación para respaldar la resiliencia informática en los WWS. Los programas actuales incluyen el [*Fondo rotatorio de agua potable*](https://www.epa.gov/sites/default/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf), el [*Fondo rotatorio estatal de agua limpia*](https://www.epa.gov/sites/default/files/2021-05/documents/cwsrf_cybersecurity_fs_final_0.pdf) y [el *Programa de subvención estatal y local para ciberseguridad de la CISA*](https://www.cisa.gov/cybergrants/slcgp).

# Lista de verificación de ciberseguridad de la EPA para sistemas de agua potable y aguas residuales

## ¿Qué es la Lista de verificación de ciberseguridad de la EPA?

La Lista de verificación de ciberseguridad de la EPA (Apéndice A) es una serie de preguntas diseñadas para evaluar las prácticas y los controles de ciberseguridad en un WWS. Las preguntas están acompañadas de medidas recomendadas que permiten implementar la práctica o el control en su totalidad. Ciertas prácticas y controles están designados como de alta prioridad, tal como se analiza en la sección 4 a continuación.

La Lista de verificación de ciberseguridad de la EPA se originó en las [*Metas de desempeño de ciberseguridad multisectorial*](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals) (CPG) de la CISA, que son prácticas básicas de ciberseguridad en sectores de infraestructura crítica y con un valor reconocido para la reducción de riesgos. La CISA desarrolló las CPG en colaboración con cada uno de los 16 sectores de infraestructura crítica, y están alineadas con el [*Marco de ciberseguridad*](https://www.nist.gov/cyberframework) del NIST. La EPA adaptó las CPG a un formato de preguntas simplificadas para utilizar durante una evaluación de ciberseguridad de un WWS.

## ¿Cómo deben utilizar los WWS la Lista de verificación de ciberseguridad de la EPA?

Las preguntas de la Lista de verificación de ciberseguridad de la EPA están diseñadas para identificar deficiencias en la ciberseguridad básica en un WWS, que podrían aumentar la vulnerabilidad del WWS a un ataque. Se recomienda que, después de completar la Lista de verificación de ciberseguridad de la EPA, los propietarios y operadores de los WWS desarrollen un plan de mitigación de riesgos para abordar las deficiencias en las prácticas y los controles de ciberseguridad.

Las [*Hojas informativas*](https://www.epa.gov/waterresilience/wcat-fact-sheets)en el Apéndice B tienen información sobre la implementación de la práctica o el control que figura en cada pregunta de la Lista de verificación de ciberseguridad de la EPA. Se puede encontrar asistencia técnica adicional sobre la adopción de las prácticas y los controles en la Lista de verificación de ciberseguridad de la EPA en el [*Programa de asistencia técnica sobre ciberseguridad para el sector del agua*](https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector) de la EPA (descrito en la sección 2).

## ¿Cuáles son las alternativas a la Lista de verificación de ciberseguridad de la EPA?

El uso de la Lista de verificación de ciberseguridad de la EPA es voluntario. Como se analizó en la sección 2, muchas otras organizaciones gubernamentales y del sector privado ofrecen métodos y orientación valiosos para evaluar la ciberseguridad en un WWS y adoptar prácticas y controles de ciberseguridad con el fin de reducir los riesgos y mejorar la resiliencia. Para los WWS, la EPA recomienda utilizar los métodos de evaluación de ciberseguridad de la [*CISA*](https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr), el [*NIST*](https://www.nist.gov/cyberframework) y la [*AWWA*](https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance) (consulte la sección 2 para ver las descripciones) o adoptar los estándares de la [*Organización Internacional de Normalización*](https://www.iso.org/standard/27001) y la [*Sociedad Internacional de Automatización/Comisión Electrotécnica Internacional*](https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards).

# Prácticas prioritarias de ciberseguridad para sistemas de agua y aguas residuales

Los WWS tienen recursos limitados para la ciberseguridad y posiblemente necesiten priorizar la adopción de medidas de mitigación de riesgos después de una evaluación de las deficiencias de ciberseguridad. La EPA, la CISA y el FBI han publicado las [*Principales medidas informáticas para proteger los sistemas de agua*](https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf) (principales medidas informáticas). Esta hoja informativa enumera las medidas prioritarias que los propietarios y operadores de los WWS deben tomar para reducir los riesgos informáticos y mejorar la resiliencia a los ataques informáticos.

Para favorecer la adopción de estas principales medidas informáticas, la EPA identificó las prácticas y los controles de ciberseguridad de la Lista de verificación de ciberseguridad de la EPA en el Apéndice A que están alineados con cada medida. La tabla 1 muestra estas prácticas y controles y las recomendaciones asociadas de la Lista de verificación de ciberseguridad de la EPA, agrupados por la principal medida informática correspondiente.

Se recomienda a los WWS a adoptar las prácticas y los controles de ciberseguridad mencionados en la tabla 1. Cuando un WWS no puede adoptar una práctica o un control de ciberseguridad en particular a causa de restricciones logísticas, de infraestructura o de otro tipo, debe buscar medidas alternativas o compensatorias para mitigar la vulnerabilidad.

Tanto en la Lista de verificación de ciberseguridad de la EPA que se incluye en el Apéndice A como en la [*Herramienta de evaluación de ciberseguridad para sistemas de agua*](https://www.epa.gov/system/files/documents/2024-08/epa-water-cybersecurity-assessment-tool-3.1_links.xlsx), las preguntas y recomendaciones de la tabla 1 están designadas como prácticas de ciberseguridad prioritarias. Esta designación también se aplica en la plantilla del plan de mitigación de riesgos, y los propietarios y operadores de los WWS la deben tener en cuenta para la implementación de los planes de mitigación de riesgos.

**Tabla 1:** *Prácticas prioritarias de ciberseguridad para sistemas de agua y aguas residuales*

| **Pregunta** | **Recomendación** |
| --- | --- |
| **1. Reduzca la exposición al Internet público** |
| ¿El WWS se asegura de que los activos conectados al Internet público no exponen de manera innecesaria servicios que se pueden aprovechar (p. ej., [protocolo de escritorio remoto](#Glossary)) y elimina las conexiones entre los activos de TO e Internet? **(2.W, 2.X)****Enlace a la hoja informativa 2.W:** <https://www.epa.gov/system/files/documents/2024-07/ensure-that-assets.pdf> **Enlace a la hoja informativa 2.X:**<https://www.epa.gov/system/files/documents/2024-07/eliminate-connections-between.pdf>  | *Recomendación: Elimine los puertos y servicios expuestos de manera innecesaria en activos públicos mediante una revisión periódica y elimine las conexiones de los activos de TO al Internet público, a menos que sea explícitamente necesario para las operaciones.*  |
| **2. Realice evaluaciones de ciberseguridad periódicas** |
| ¿El WWS realiza evaluaciones de ciberseguridad periódicas? | *Recomendación: Realice una evaluación de ciberseguridad de manera periódica para comprender las vulnerabilidades actuales en los sistemas de TO y TI. Las evaluaciones le permiten identificar, evaluar y priorizar la mitigación de vulnerabilidades en redes de TO y TI.* |
| ¿El WWS tiene una función/puesto/cargo designado responsable de planificar, obtener recursos y ejecutar actividades de ciberseguridad en el WWS? **(1.B)****Enlace a la hoja informativa 1.B:**<https://www.epa.gov/system/files/documents/2024-07/have-a-named-role.pdf>  | *Recomendación: Identifique una función/puesto/cargo responsable de la ciberseguridad en el WWS. La persona que ocupe esta función/puesto/cargo es responsable de todas las actividades de ciberseguridad del WWS.* |
| **3. Cambie de inmediato las contraseñas predeterminadas** |
| ¿El WWS cambia las contraseñas predeterminadas y requiere una longitud mínima para las contraseñas? **(2.A, 2.B)****Enlace a la hoja informativa 2.A:**<https://www.epa.gov/system/files/documents/2024-07/change-default-passwords.pdf>**Enlace a la hoja informativa 2.B:**<https://www.epa.gov/system/files/documents/2024-07/require-a-minimum.pdf>  | *Recomendación: Cambie todas las contraseñas predeterminadas del fabricante o distribuidor antes de que el equipo o el software se ponga en marcha, e implemente un requisito de longitud mínima para las contraseñas a través de una política o controles administrativos establecidos en el sistema.* |
| ¿El WWS requiere el uso de la [autenticación multifactor (MFA)](#Glossary) siempre que sea posible, pero, como mínimo, para el acceso remoto a las redes de TO y TI del WWS? **(2.H)****Enlace a la hoja informativa 2.H:**<https://www.epa.gov/system/files/documents/2024-07/require-multi-factor.pdf>  | *Recomendación: Implemente la MFA de la manera más generalizada posible para las redes de TO y TI. Como mínimo, se debe usar la MFA para el acceso remoto a la red de TO.* |
| **4. Realice el inventario de activos de TO y TI** |
| ¿El WWS mantiene un [inventario](#Glossary) actualizado de todos los activos de la red de TO y TI? **(1.A)****Enlace a la hoja informativa 1.A:**<https://www.epa.gov/system/files/documents/2024-07/maintain-an-updated-inventory.pdf>  | *Recomendación: Revise periódicamente (como mínimo, trimestralmente) y mantenga una lista de todos los activos de TO y TI con una* [dirección IP](#Glossary)*. Esto incluye equipos de terceros y heredados (es decir, antiguos).*  |
| ¿El WWS mantiene documentación actualizada que explica la preparación y los ajustes (es decir, la configuración) de los activos críticos de TO y TI? **(2.O)****Enlace a la hoja informativa 2.O:**<https://www.epa.gov/system/files/documents/2024-07/maintain-current-documentation.pdf>  | *Recomendación: Mantenga documentación precisa sobre la configuración original y actual de los activos de TO y TI, incluyendo la versión de* software *y* [firmware](#Glossary)*.* |
| **5. Desarrolle e implemente planes de respuesta y recuperación de incidentes de ciberseguridad** |
| ¿El WWS tiene un plan de respuesta a incidentes (IR) de ciberseguridad escrito para situaciones de amenazas críticas (p. ej., deshabilitación o manipulación de [sistemas de control](#Glossary) de procesos, pérdida o robo de datos operacionales o financieros, exposición de información sensible) que se implementa y actualiza de manera periódica? **(2.S)****Enlace a la hoja informativa 2.S:**<https://www.epa.gov/system/files/documents/2024-07/have-a-written.pdf>  | *Recomendación: Desarrolle, implemente y actualice un plan de IR para incidentes de ciberseguridad que puedan afectar las operaciones del WWS. Participe en ejercicios basados en el debate (p. ej.,* [TTX](#Glossary)*) y basados en operaciones (p. ej.,* [simulacros](#Glossary)*) para mejorar la respuesta a posibles incidentes informáticos.* |
| ¿El WWS tiene 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 CISA, reguladores estatales, WaterISAC, ¿proveedor de seguro informático)? **(4.A)****Enlace a la hoja informativa 4.A:**<https://www.epa.gov/system/files/documents/2024-07/have-a-written-procedure.pdf>  | *Recomendación: Documente el procedimiento para informar incidentes de ciberseguridad 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.* |
| **6. Realice copias de seguridad de los sistemas de TO/TI** |
| ¿El WWS realiza [copias de seguridad](#Glossary) de los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica de [PLC](#Glossary), diagramas de ingeniería, registros de personal) según un cronograma periódico, almacena las copias de seguridad separadas de los sistemas de origen y prueba las copias de seguridad de manera periódica? **(2.R)****Enlace a la hoja informativa 2.R:**<https://www.epa.gov/system/files/documents/2024-07/backup-systems-necessary_0.pdf>  | *Recomendación: Realice copias de seguridad periódicas de los sistemas de TO/TI para que pueda recuperarlos a un estado conocido y seguro en el caso de que se vean comprometidos. Pruebe los procedimientos de copia de seguridad y aísle las copias de seguridad de las conexiones de red. Implemente la regla 3-2-1 del NIST:* *3) Conserve tres copias: una primaria y dos de seguridad.* *2) Conserve las copias de seguridad en dos tipos de medios diferentes.* *1) Almacene una copia fuera del sitio.* |
| **7. Reduzca la exposición a vulnerabilidades** |
| ¿El WWS aplica parches o mitiga de algún modo las vulnerabilidades conocidas en el plazo recomendado? **(1.E)****Enlace a la hoja informativa 1.E:**<https://www.epa.gov/system/files/documents/2024-07/patch-or-otherwise.pdf>  | *Recomendación: Identifique y aplique parches a las vulnerabilidades en función de los riesgos (p. ej., primero los activos críticos) lo más rápido posible.* |
| ¿El WWS requiere credenciales únicas y diferentes para que los usuarios accedan a las redes de TO y TI y cuentas diferentes de usuario y con privilegios (p. ej., [administrador del sistema](#Glossary))? **(2.C, 2.E)****Enlace a la hoja informativa 2.C:**<https://www.epa.gov/system/files/documents/2024-07/require-unique.pdf> **Enlace a la hoja informativa 2.E:**<https://www.epa.gov/system/files/documents/2024-07/separate-user.pdf>  | *Recomendación: Requiera que cada usuario individual tenga dos nombres de usuario y contraseñas diferentes; una cuenta para acceder a la red de TI y la otra cuenta para acceder a la red de TO, para reducir el riesgo de que un atacante pueda desplazarse entre ambas redes mediante un mismo inicio de sesión. Restrinja los privilegios del administrador del sistema a cuentas de usuario diferentes para acciones administrativas solamente y evalúe los privilegios administrativos de manera periódica para garantizar que las personas que tienen estos privilegios tengan la información precisa.*  |
| ¿El WWS prohíbe la conexión de *hardware* no autorizado (p. ej., [dispositivos](#Glossary) USB, medios extraíbles, computadoras portátiles ingresadas al sitio por otras personas) a los activos de TO y TI? **(2.V)****Enlace a la hoja informativa 2.V:**<https://www.epa.gov/system/files/documents/2024-07/prohibit-the-connection_0.pdf>  | *Recomendación: Cuando sea factible, quite, deshabilite o proteja de algún modo los puertos físicos (p. ej., puertos USB en una computadora portátil) para evitar la conexión a activos no autorizados.* |
| ¿El WWS deshabilita de inmediato el acceso a una cuenta o red cuando el acceso ya no es necesario por motivos de jubilación, cambio de función, desvinculación u otros factores? **(2.D)****Enlace a la hoja informativa 2.D:**<https://www.epa.gov/system/files/documents/2024-07/immediately-disable-access.pdf>  | *Recomendación: Deshabilite de inmediato el acceso a cuentas o redes después de un cambio en la situación de una persona que hace que el acceso no sea necesario (p. ej., jubilación, cambio de puesto).* |
| **8. Realice capacitaciones de concientización sobre ciberseguridad** |
| ¿El WWS proporciona/realiza capacitaciones anuales de concientización sobre ciberseguridad para todo el personal del WWS que cubran conceptos básicos de ciberseguridad? **(2.I)****Enlace a la hoja informativa 2.I:**<https://www.epa.gov/system/files/documents/2024-07/provide-at-least.pdf>  | *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.* |

# Riesgos de la inteligencia artificial para los sistemas de agua y aguas residuales

El uso actual de la [inteligencia artificial](#Glossary) (IA) por parte de los WWS es limitado, pero las posibles ventajas de la IA para las operaciones y gestión del WWS pueden impulsar una amplia adopción en el futuro. En consecuencia, los propietarios y operadores de los WWS deben ser conscientes de las posibles ventajas y riesgos, y la gestión de riesgos de los sistemas de IA.

Los sistemas de IA analizan grandes volúmenes de datos históricos y en tiempo real para tomar decisiones y hacer predicciones. Un sistema de IA con la configuración correcta podría respaldar, automatizar u optimizar posiblemente muchos procesos comerciales y operacionales en los WWS. Los ejemplos incluyen la optimización de los controles de bombas, la planificación de ampliaciones del sistema, la respuesta rápida a situaciones de emergencia, la comunicación con los clientes y el monitoreo de la calidad del agua. Se prevé que las futuras investigaciones e implementaciones de sistemas de IA en los WWS demuestren otras áreas que se beneficiarían con el uso de la IA.

No obstante, la implementación de sistemas de IA en los WWS también conlleva el riesgo del mal funcionamiento de la IA, ya sea por una causa accidental o un acto intencional. Sin importar la causa, si un sistema de IA funciona mal en un WWS, podría hacer predicciones incorrectas y tomar decisiones que podrían interrumpir los servicios de agua y aguas residuales, y posiblemente dañar la infraestructura.

Las causas accidentales de mal funcionamiento de la IA podrían incluir la instalación o capacitación incorrecta de la IA, entradas imprevistas de datos en la IA o capacitación insuficiente para empleados o distribuidores que integran, monitorean o se conectan con la IA. Un rival podría provocar el mal funcionamiento o la falla de la IA tomando el control de la IA o ingresando datos corruptos en la IA. El acceso a la IA por parte de rivales podría ocurrir a través de vectores usados en ataques informáticos convencionales (p. ej., contraseñas débiles, ingeniería social).

En consideración de las promesas y los riesgos de la IA, el presidente emitió la [*Orden Ejecutiva 14110, “Desarrollo y uso seguros, protegidos y confiables de la inteligencia artificial (IA)”*](https://www.congress.gov/crs-product/R47843) el 23 de octubre de 2023. Esta Orden Ejecutiva aborda la gestión y protección de la IA en la infraestructura crítica, junto con otras preocupaciones, como la protección de la privacidad y las libertades civiles, además de la promoción de la innovación. En cumplimiento de esta orden, las agencias federales están emitiendo guías sobre cómo abordar y gestionar los riesgos de la IA para infraestructura crítica, incluyendo los WWS.

El [*Centro de Recursos de Inteligencia Artificial Confiable y Responsable*](https://airc.nist.gov/home) del NIST es un repositorio en línea de guías y capacitación que respalda el desarrollo y la implementación de tecnologías de IA. Incluye el [*Marco para la gestión de riesgos de la IA*](https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF) del NIST, que está diseñado para aumentar la confiabilidad de los sistemas de IA y fomentar el desarrollo, la implementación y el uso responsables de los sistemas de IA.

Este marco está dividido en dos partes. La parte 1 analiza los riesgos de la IA y las características de los sistemas confiables, que se definen como válidos y confiables, seguros, protegidos y resilientes, responsables y transparentes, explicables e interpretables, con privacidad mejorada e imparciales, con manejo de sesgos perjudiciales. La parte 2 comprende el “núcleo” del marco. Describe cuatro funciones específicas para ayudar a las organizaciones a abordar los riesgos de los sistemas de IA.

1. Gobernar: establecer una cultura organizacional de la gestión de riesgos de la IA.
2. Mapear: comprender su contexto de uso y perfil de riesgo particulares con relación a la IA.
3. Medir: desarrollar sistemas para evaluar, analizar y gestionar los riesgos de la IA.
4. Gestionar: priorizar y actuar en función de los riesgos de la IA para la seguridad.

Cada una de estas funciones está desglosada en categorías y subcategorías con medidas y resultados específicos.

La CISA ha publicado el documento [*Mitigar el riesgo de la inteligencia artificial: pautas de seguridad para propietarios y operadores de infraestructura crítica*](https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf). Las pautas enumeran diez categorías de uso de la IA en la infraestructura crítica, como la automatización de las operaciones, la optimización del desempeño, la detección de eventos y el pronóstico. Además, se definen tres categorías de riesgos relacionados con la IA a nivel del sistema: ataques que usan la IA, ataques dirigidos a los sistemas de IA y fallas en el diseño y la implementación de la IA. Para cada categoría de riesgo se proporcionan subcategorías de riesgos y estrategias de mitigación asociadas. Además, estas pautas están alineadas con el Marco para la gestión de riesgos de la IA del NIST e incluyen medidas recomendadas que las instalaciones de infraestructura crítica deben tomar en cada una de las cuatro funciones básicas del marco del NIST (indicadas anteriormente).

La hoja informativa [*Implementar sistemas de IA de manera segura*](https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF) fue publicada de manera conjunta por la Agencia de Seguridad Nacional de EE. UU., la CISA, el FBI, el Australian Signals Directorate, el Canadian Centre for Cyber Security, el National Cyber Security Centre de Nueva Zelanda, y el National Cyber Security Centre del Reino Unido. Se desarrolló para cumplir tres metas: (1) mejorar la confidencialidad, integridad y disponibilidad de los sistemas de IA; (2) garantizar que las vulnerabilidades conocidas de ciberseguridad en los sistemas de IA se mitiguen de manera adecuada, y (3) proporcionar metodologías y controles para proteger, detectar y responder a actividad maliciosa contra sistemas de IA y datos y servicios relacionados.

Además de estos materiales de orientación del gobierno federal disponibles en este momento, muchas organizaciones del sector privado ofrecen información sobre la implementación segura y eficaz de sistemas de IA en infraestructura crítica. Los propietarios y operadores de los WWS deben ser conscientes de esta tecnología de rápida evolución y considerar si la implementación de sistemas de IA en sus instalaciones podría ser beneficiosa. Además, deben mantenerse actualizados sobre las amenazas actuales que usan la IA para facilitar los ataques informáticos en instalaciones de infraestructura crítica e incorporar estrategias de mitigación recomendadas en sus programas de ciberseguridad.

APÉNDICE A: Lista de Verificación de Ciberseguridad de la EPA para Sistemas de Agua Potable y Aguas Residuales

Las prácticas prioritarias de ciberseguridad para los WWS se indican con un \* después de la pregunta.

1. **IDENTIFICAR.**
	1. ¿Mantiene el WWS un inventario actualizado de todos los activos de la red de tecnología operacional (TO) y tecnología de la información (TI)? \*

*Recomendación: Revise periódicamente (como mínimo, trimestralmente) y mantenga una lista de todos los activos de TO y TI con una dirección IP. Esto incluye equipos de terceros y heredados (es decir, antiguos).*

* 1. ¿Tiene el WWS una función/puesto/cargo designado responsable de planificar, obtener recursos y ejecutar actividades de ciberseguridad en el WWS? \*

Recomendación: Identifique una función/puesto/cargo responsable de la ciberseguridad en el WWS. La persona que ocupe esta función/puesto/cargo es responsable de todas las actividades de ciberseguridad del WWS.

* 1. ¿Tiene el WWS una función/puesto/cargo designado responsable de planificar, obtener recursos y ejecutar actividades de ciberseguridad específicas de TO?

Recomendación: Identifique una función/puesto/cargo responsable de garantizar la planificación, obtención de recursos y ejecución de actividades de ciberseguridad específicas de TO.

* 1. ¿Proporciona el WWS oportunidades periódicas para fortalecer la comunicación y coordinación entre el personal de TO y TI, incluyendo a los distribuidores?

Recomendación: Facilite reuniones entre el personal de TO y TI con el fin de proporcionar oportunidades para que todas las partes comprendan mejor las necesidades de seguridad organizacional y fortalecer las relaciones laborales.

* 1. ¿Aplica el WWS parches o mitiga de algún modo las vulnerabilidades conocidas en el plazo recomendado? \*

*Recomendación: Identifique y aplique parches a las vulnerabilidades en función de los riesgos (p. ej., primero los activos críticos) lo más rápido posible.*

* 1. Este número de control se incluye aquí en coherencia con las Metas de desempeño de ciberseguridad multisectorial (CPG) de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA), pero no se aplica a la mayoría de los WWS.

1.G/H. ¿Requiere el WWS que todos los distribuidores y proveedores de servicios de TO notifiquen al WWS sobre incidentes o vulnerabilidades de seguridad en un plazo en función de los riesgos?

*Recomendación: Requiera que los distribuidores y proveedores de servicios notifiquen al WWS sobre posibles incidentes y vulnerabilidades de seguridad dentro de un plazo estipulado que se describa en los documentos y contratos de adquisición.*

* 1. ¿Incluye el WWS la ciberseguridad como criterio de evaluación para la adquisición de activos y servicios de TO y TI?

*Recomendación: Incluya la ciberseguridad como criterio de evaluación cuando adquiera activos y servicios. Cuando sea factible, busque sistemas que sean seguros por diseño y de forma predeterminada.*

1. **PROTEGER.**
	1. ¿Cambia el WWS las contraseñas predeterminadas? \*

*Recomendación: Cambie todas las contraseñas predeterminadas del fabricante o distribuidor antes de que el equipo o el software se ponga en marcha.*

* 1. ¿Requiere el WWS una longitud mínima para las contraseñas? \*

*Recomendación: Implemente un requisito de longitud mínima para las contraseñas a través de una política o controles administrativos establecidos en el sistema.*

* 1. ¿Requiere el WWS credenciales únicas y diferentes para que los usuarios accedan a las redes de TO y TI? \*

*Recomendación: Requiera que cada usuario individual tenga dos nombres de usuario y contraseñas diferentes; una cuenta para acceder a la red de TI y la otra cuenta para acceder a la red de TO, para reducir el riesgo de que un atacante pueda desplazarse entre ambas redes mediante un mismo inicio de sesión.*

* 1. ¿Deshabilita el WWS de inmediato el acceso a una cuenta o red cuando el acceso ya no es necesario por motivos de jubilación, cambio de función, desvinculación u otros factores? \*

*Recomendación: Deshabilite de inmediato el acceso a cuentas o redes después de un cambio en la situación de una persona que hace que el acceso no sea necesario (p. ej., jubilación, cambio de puesto).*

* 1. ¿Diferencia el WWS las cuentas de usuario y con privilegios (p. ej., administrador del sistema)? \*

*Recomendación:* *Restrinja los privilegios del administrador del sistema a cuentas de usuario diferentes para acciones administrativas solamente y evalúe los privilegios administrativos de manera periódica para garantizar que las personas que tienen estos privilegios tengan la información precisa.*

* 1. ¿Segmenta el WWS las redes de TO y TI y deniega las conexiones a la red de TO de forma predeterminada, a menos que se permita explícitamente (p. ej., por dirección IP y puerto)?

*Recomendación: Requiera que las conexiones entre las redes de TO y TI se realicen a través de un intermediario,* como un cortafuegos, un servidor bastión, un servidor de accesos directos o una zona desmilitarizada, que se monitorea y registra.

* 1. ¿Detecta y bloquea el WWS intentos fallidos recurrentes de inicio de sesión?

*Recomendación: Habilite que se notifique al administrador del sistema después de una cantidad específica de intentos fallidos recurrentes de inicio de sesión en un breve período. En este punto, los futuros intentos de inicio de sesión de la cuenta sospechosa deben bloquearse durante un tiempo específico o hasta que un administrador los vuelva a habilitar.*

* 1. ¿Requiere el WWS el uso de la autenticación multifactor (MFA) siempre que sea posible, pero, como mínimo, para el acceso remoto a las redes de TO y TI del WWS? \*

*Recomendación: Implemente la MFA de la manera más generalizada posible para las redes de TO y TI. Como mínimo, se debe usar la MFA para el acceso remoto a la red de TO.*

* 1. ¿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.

* 1. ¿Ofrece el WWS capacitación sobre ciberseguridad específica de TO al menos anualmente al personal que usa TO como parte de sus tareas habituales?

Recomendación: Proporcione capacitación especializada sobre ciberseguridad enfocada en TO a todo el personal que utilice activos de TO.

* 1. ¿Usa el WWS cifrado eficaz para mantener la confidencialidad de los datos en tránsito?

Recomendación: Cuando envíe información y datos, use los estándares de cifrado de seguridad de la capa de transporte (TLS) o capa de puertos seguros (SSL).

* 1. ¿Usa el WWS cifrado para mantener la confidencialidad de los datos sensibles almacenados?

Recomendación: No almacene datos sensibles, incluso credenciales (es decir, nombres de usuario y contraseñas) en archivos de texto sin formato.

* 1. ¿Usa el WWS controles de seguridad de correo electrónico para reducir las amenazas de correo electrónico habituales, como la suplantación de identidad, el robo de identidad y la intercepción?

Recomendación: Asegúrese de que los controles de seguridad de correo electrónico estén habilitados en toda la infraestructura de correo electrónico corporativo.

* 1. ¿Deshabilita el WWS las macros de Microsoft Office o código integrado similar de forma predeterminada en todos los activos?

*Recomendación: Deshabilite las macros integradas y el código ejecutable similar de forma predeterminada en todos los activos.*

* 1. ¿Mantiene el WWS documentación actualizada que explica la preparación y los ajustes (es decir, la configuración) de los activos críticos de TO y TI? \*

*Recomendación: Mantenga documentación precisa sobre la configuración original y actual de los activos de TO y TI, incluyendo la versión de software y firmware.*

* 1. ¿Mantiene el WWS documentación actualizada que describe la topología de la red (es decir, las conexiones entre todos los componentes de red) en las redes de TO y TI del WWS?

*Recomendación: Mantenga documentación completa y precisa sobre todas las topologías de red de TO y TI del WWS para facilitar la respuesta y recuperación de incidentes.*

* 1. ¿Requiere el WWS la aprobación antes de instalar o implementar nuevo *software*?

*Recomendación: Solo permita que los administradores instalen software nuevo en un activo del WWS.*

* 1. ¿Realiza el WWS copias de seguridad de los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica de PLC, diagramas de ingeniería, registros de personal) según un cronograma periódico, almacena las copias de seguridad separadas de los sistemas de origen y prueba las copias de seguridad de manera periódica? \*

*Recomendación: Realice copias de seguridad periódicas de los sistemas de TO/TI para que pueda recuperarlos a un estado conocido y seguro en el caso de que se vean comprometidos. Pruebe los procedimientos de copia de seguridad y aísle las copias de seguridad de las conexiones de red. Implemente la regla 3-2-1 del NIST:*

*3) Conserve tres copias: una primaria y dos de seguridad.*

*2) Conserve las copias de seguridad en dos tipos de medios diferentes.*

*1) Almacene una copia fuera del sitio.*

* 1. ¿Tiene el WWS un plan de respuesta a incidentes (IR) de ciberseguridad escrito para situaciones de amenazas críticas (p. ej., deshabilitación o manipulación de sistemas de control de procesos, pérdida o robo de datos operacionales o financieros, exposición de información sensible) que se implementa y actualiza de manera periódica? \*

*Recomendación: Desarrolle, implemente y actualice un plan de IR para incidentes de ciberseguridad que puedan afectar las operaciones del WWS. Participe en ejercicios basados en el debate (p. ej., TTX) y basados en operaciones (p. ej., simulacros) para mejorar la respuesta a posibles incidentes informáticos.*

* 1. ¿Recopila el WWS registros de seguridad (p. ej., acceso al sistema y las redes, detección de programas maliciosos) para usar en la detección e investigación de incidentes?

*Recomendación: Recopile y almacene registros o datos de tráfico de red para ayudar a detectar ataques informáticos e investigar actividad sospechosa.*

* 1. ¿Protege el WWS los registros de seguridad del acceso no autorizado y la alteración?

*Recomendación: Almacene los registros de seguridad en un sistema central o base de datos al que solo puedan acceder usuarios autorizados y autenticados.*

* 1. ¿Prohíbe el WWS la conexión de *hardware* no autorizado (p. ej., dispositivos USB, medios extraíbles, computadoras portátiles ingresadas al sitio por otras personas) a los activos de TO y TI? \*

*Recomendación: Cuando sea factible, quite, deshabilite o proteja de algún modo los puertos físicos (p. ej., puertos USB en una computadora portátil) para evitar la conexión a activos no autorizados.*

* 1. ¿Se asegura el WWS de que los activos conectados al Internet público no exponen de manera innecesaria servicios que se pueden aprovechar (p. ej., protocolo de escritorio remoto)? \*

*Recomendación: Elimine los puertos y servicios expuestos de manera innecesaria en activos públicos y realice revisiones periódicas.*

* 1. ¿Elimina el WWS las conexiones entre los activos de TO e Internet? \*

*Recomendación:* *Elimine las conexiones de los activos de TO al Internet público, a menos que sea explícitamente necesario para las operaciones.*

1. **DETECTAR.**
	1. ¿Mantiene el WWS una lista de las amenazas y tácticas, técnicas y procedimientos (TTP) de rivales para realizar ataques informáticos relevantes para el WWS?

Recomendación: Reciba alertas de la CISA, priorice la lista de vulnerabilidades conocidas aprovechadas (KEV) y mantenga documentación sobre los TTP relevantes para el WWS.

1. **RESPONDER.**
	1. ¿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)?[[1]](#footnote-2) \*

*Recomendación: Documente el procedimiento para informar incidentes de ciberseguridad 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.*

* 1. Este número de control se incluye aquí en coherencia con las CPG de la CISA, pero no se aplica a la mayoría de los WWS.
	2. Este número de control se incluye aquí en coherencia con las CPG de la CISA, pero no se aplica a la mayoría de los WWS.

1. **RECUPERAR.**

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.*

APÉNDICE B: Hojas Informativas de la Lista de Verificación de la EPA

Se pueden encontrar las hojas informativas de la Lista de verificación de la EPA en el sitio web [*Hojas informativas*](https://www.epa.gov/waterresilience/wcat-fact-sheets) de la EPA.

APÉNDICE C: Glosario de Términos

| **Término** | **Definición** |
| --- | --- |
| Activo | Una instalación, un dispositivo, información o proceso informático que tiene valor. |
| Acuerdo de nivel de servicio (SLA) | Un compromiso entre un proveedor de servicios (p. ej., distribuidor) y un cliente (p. ej., un WWS). Los aspectos de la calidad y disponibilidad del servicio, además de las responsabilidades individuales de las partes, se acuerdan de manera anticipada.  |
| Administrador del sistema | Persona responsable de gestionar, actualizar y manejar los sistemas informáticos. Esta persona puede ser un empleado del WWS o un distribuidor.  |
| Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA)  | La CISA lidera la iniciativa nacional por comprender, gestionar y reducir el riesgo para la infraestructura informática y física del país. La CISA desarrolla y publica una variedad de información, recursos, herramientas y capacitación para el sector de agua y otros sectores de infraestructura crítica.  |
| Arquitectura de referencia empresarial de Purdue (PERA) o modelo de Purdue | Un modelo de seis capas para la segmentación de redes de ICS que define los componentes del sistema que se encuentran en cada una de las capas y los controles de límite de red para proteger cada capa y, en última instancia, la red del ICS. |
| Asesores de ciberseguridad (CSA) de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) | Profesionales que proporcionan asistencia de ciberseguridad a propietarios de infraestructura crítica, incluyendo los WWS, como preparación informática, evaluaciones y recursos de protección, además de coordinación y apoyo para incidentes. |
| Ataque a la cadena de suministro | Un tipo de ataque informático dirigido a un distribuidor externo de confianza que ofrece servicios o *software* vital para la cadena de suministro. Los ataques a la cadena de suministro son difíciles de detectar, dado que dependen de *software* en el que se confía y pueden distribuirse de manera generalizada (p. ej., ataque SolarWinds). |
| Autenticación de mensajes basada en dominios, informes y conformidad (DMARC) | Un protocolo que usa registros del marco de políticas del remitente (SPF) o de DKIM para autenticar correos electrónicos. Permite rechazar correos electrónicos fraudulentos.  |
| Autenticación multifactor (MFA) | Una función que requiere más de un factor de autenticación distinto, como un código enviado por mensaje de texto a un teléfono celular, para activar o iniciar sesión en una cuenta. |
| Base de datos nacional de vulnerabilidades (NVD) | La NVD se estableció para proporcionar un repositorio de datos del Gobierno de EE. UU. sobre las vulnerabilidades y ajustes de configuración de *software*.  |
| Bloqueo automático de cuenta o umbral de bloqueo de cuenta | Política que determina la cantidad de veces que una persona puede intentar iniciar sesión con credenciales incorrectas antes de que el sistema la bloquee. |
| Capa de puertos seguros (SSL) | Un protocolo que usa un WWS para proteger información privada durante la transmisión a través de Internet. |
| Catálogo de vulnerabilidades conocidas aprovechadas (KEV)  | Una lista de vulnerabilidades que la CISA ha identificado que están siendo aprovechadas o que agentes de amenazas han usado para perpetrar ataques. |
| Centro de Quejas de Delitos en Internet del FBI (IC3) | Una división de la Oficina Federal de Investigación (FBI) centrado en presunta actividad delictiva facilitada por Internet. |
| Centros de Intercambio y Análisis de Información (ISAC) | Una organización que recopila, analiza y distribuye información práctica sobre amenazas a sus miembros y les proporciona herramientas para mitigar los riesgos y mejorar la resiliencia. Por ejemplo, WaterISAC proporciona estos servicios a los WWS. |
| Cifrado | Cualquier procedimiento que un WWS usa para convertir texto o datos sin formato en texto o datos codificados o “cifrados” para evitar que una persona diferente del destinatario previsto decodifique y lea el texto o los datos. |
| Cifrado de datos transparente (TDE) | El TDE permite al usuario cifrar datos sensibles almacenados en bases de datos a nivel de archivo. Protege los datos inactivos, no los datos en tránsito. |
| Cifrar | Proceso mediante el que un WWS convierte texto o datos sin formato en texto o datos codificados o “cifrados”. |
| Código integrado | Código generado por un sitio web de terceros, como YouTube o X (antes conocido como Twitter), que un usuario puede copiar y pegar en su propia página web. Este código integrado mostrará luego los mismos medios, aplicación o *feed* en la página web del usuario que en el sitio web original. |
| Comisión Electrotécnica Internacional (IEC) | Una organización global sin fines de lucro con membresía que reúne a 173 países y coordina el trabajo de 20 000 expertos de todo el mundo. Facilita el acceso a la electricidad y verifica la seguridad, el desempeño y la interoperabilidad de dispositivos y sistemas eléctricos y electrónicos, incluyendo dispositivos de consumidores, como teléfonos móviles y refrigeradores, equipos de oficina y médicos, TI, generación de electricidad y más. |
| Configuración | La configuración de un sistema o componente de TO o TI, incluyendo las condiciones, los parámetros y las especificaciones. |
| Conmutador de red | Un dispositivo que conecta usuarios, aplicaciones y equipos dentro de una red para que puedan comunicarse entre sí y compartir recursos. |
| Control | Una práctica o medida que un WWS usa para prevenir, detectar y mitigar amenazas y ataques informáticos. Las prácticas abarcan desde controles físicos, como quitar puertos USB en computadoras portátiles, a controles técnicos, como usar cortafuegos y autenticación multifactor. |
| Control de supervisión y adquisición de datos (SCADA) | Un tipo de sistema de control industrial. Es un conjunto de componentes de *software* y *hardware* que permite a los usuarios controlar, monitorear y automatizar procesos. Los sistemas SCADA ayudan a recopilar y analizar datos en tiempo real.  |
| Controlador lógico programable (PLC) | Una computadora industrial pequeña diseñada originalmente para llevar a cabo las funciones lógicas ejecutadas por equipos eléctricos (p. ej., relés, conmutadores y temporizadores/contadores mecánicos). Los PLC han evolucionado en controladores con la capacidad de controlar procesos complejos, y los WWS a menudo los usan en sistemas SCADA. |
| Controles compensatorios | Controles de seguridad y privacidad que un WWS implementa en lugar de los controles básicos. Los controles compensatorios proporcionan protección equivalente o similar para un sistema de TO y TI. |
| Copia de seguridad | El proceso de crear una copia de datos críticos del WWS que pueden usarse para la recuperación en caso de que se pierdan o corrompan los datos originales. |
| Correo identificado por claves de dominio (DKIM) | Método de autenticación de correo electrónico para verificar la autenticidad de los correos electrónicos. |
| Cortafuegos | Un dispositivo que restringe la comunicación de datos entre dos redes conectadas. Un cortafuegos puede ser una aplicación instalada en una computadora de uso general o un dispositivo independiente que permite o rechaza el flujo de información entre las redes. Habitualmente, un WWS usa cortafuegos para definir límites de zonas, como entre los sistemas de TO y TI en un WWS. |
| Credenciales | Información única de un usuario específico que se requiere para iniciar sesión en un sistema o programa. Por ejemplo, un nombre de usuario y contraseña. |
| Cuenta con privilegios | Una cuenta de usuario que tiene más privilegios que los usuarios comunes. Por ejemplo, las cuentas con privilegios podrían instalar o eliminar *software*, actualizar el sistema operativo o modificar los ajustes del sistema o de las aplicaciones. Estas cuentas también podrían tener acceso a archivos a los que los usuarios estándar no pueden acceder. En un WWS, un administrador del sistema probablemente tendría una cuenta con privilegios. |
| Dirección de control de acceso a medios (MAC) | Un identificador único asignado a un controlador de interfaz de red (NIC) para usar como dirección de red. Habitualmente, los fabricantes de dispositivos asignan las direcciones MAC, de modo que los dispositivos ya vienen con esta dirección asignada, a diferencia de las direcciones IP. También se conoce como dirección de *hardware* o dirección física. |
| Dirección de protocolo de Internet (IP) | Una dirección numérica que identifica un dispositivo en Internet o una red local.  |
| Dispositivos | Artículos de *hardware* informático, que incluye computadoras de escritorio, computadoras portátiles, servidores y tabletas. |
| Ejecutable | Un fragmento de un código informático o programación que puede realizar tareas establecidas de acuerdo con sus instrucciones codificadas. Los archivos ejecutables son usados por un programa o rutina informático. |
| Ejercicio práctico (TTX) | Un ejercicio basado en el debate en el que el personal con funciones y responsabilidades en un plan de IR en particular se reúne en un salón o en grupos pequeños para validar el contenido del plan, debatiendo sobre las funciones de cada uno durante una emergencia informática y sus respuestas a un incidente informático en particular. Un facilitador inicia el debate presentando una situación y hace preguntas en función de la situación. |
| Enrutador | Un dispositivo que se comunica entre Internet y los dispositivos en un WWS que se conectan a Internet. |
| Evaluación de riesgos y resiliencia (RRA) | Una evaluación de los riesgos para el WWS, incluyendo actos malintencionados y peligros naturales, y de la resiliencia a estos riesgos.  |
| Fast Identity Online (FIDO)/protocolo de cliente a autenticador (CTAP) | Desarrollados por FIDO Alliance, el protocolo CTAP permite la comunicación sin el uso de contraseñas entre un autenticador externo (p. ej., teléfonos móviles, dispositivos conectados) y otro cliente (p. ej., navegador) o plataforma (p. ej., sistema operativo, como Microsoft Windows). |
| *Firmware* | Programa de *software* o instrucciones programadas en la memoria flash de solo lectura (ROM) de un dispositivo de *hardware*. Permite que el dispositivo se comunique con otro *hardware* informático. |
| Gestión de información y eventos de seguridad (SIEM)  | Una herramienta que recopila datos de registros de eventos de una amplia gama de fuentes (p. ej., dispositivos, *software*), identifica actividad diferente de la “normal” con análisis en tiempo real y toma las medidas correspondientes. Ayuda a las organizaciones a detectar, analizar y responder a amenazas de seguridad antes de que interrumpan las operaciones.  |
| Información de identificación personal (PII) | Información que permite inferir de manera directa o indirecta la identidad de una persona. |
| Instituto Nacional de Estándares y Tecnología (NIST) | Una organización que desarrolla estándares, pautas, buenas prácticas y otros recursos sobre ciberseguridad para satisfacer las necesidades de la industria, las agencias federales y el público general de EE. UU. |
| Inteligencia artificial  | La capacidad de un dispositivo de llevar a cabo funciones que están normalmente asociadas con la inteligencia humana, como razonar, aprender y mejorar. |
| Intercepción | La intercepción permite a los atacantes acceder a datos, aplicaciones o sistemas, y permite principalmente ataques contra la confidencialidad. Esto podría consistir en ver o copiar archivos de manera no autorizada, escuchar conversaciones telefónicas o leer el correo electrónico de otra persona. Estos ataques pueden llevarse a cabo contra datos inactivos (p. ej., almacenados en un servidor) o en movimiento (p. ej., un correo electrónico en tránsito del remitente al destinatario). |
| Interfaz humano-máquina (HMI) | Interfaz o panel de usuario que conecta un usuario con una máquina, sistema o dispositivo. El término “HMI” se usa habitualmente en el contexto de un proceso industrial, como en la interacción con un sistema SCADA. Por ejemplo, un operador del WWS podría usar una HMI para verificar si una bomba determinada está funcionando. |
| Intranet | Una red de comunicaciones local que a menudo se usa para mejorar la comunicación, la colaboración y la participación en una organización. Comúnmente excluye a cualquier persona externa a la organización. |
| Inventario | Lista o registro formal de los bienes de la organización en un WWS.  |
| Listas de control de acceso | Listas que identifican personas que pueden acceder a un sistema de tecnología operacional (TO) o tecnología de la información (TI). |
| Macro | Una acción configurada que permite a los usuarios automatizar tareas y agregar funcionalidad en archivos (p. ej., un botón de comando y una macro asociada en un formulario). La macro contiene los comandos que el botón realizará cada vez que un usuario hace clic sobre él. |
| Marco de ciberseguridad (CSF) del NIST | Orientación voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones, como los WWS, gestionen mejor y reduzcan los riesgos de ciberseguridad. Además de ayudar a las organizaciones a gestionar y reducir los riesgos, el NIST diseñó el CSF para fomentar las comunicaciones sobre gestión de riesgos de ciberseguridad entre las partes interesadas internas y externas de las organizaciones. |
| Marco de políticas del remitente (SPF) | Un método de autenticación de correo electrónico que ayuda a proteger el correo electrónico saliente y que no se marque como correo basura por las organizaciones que lo reciben.  |
| Marco para la gestión de riesgos de la inteligencia artificial (AI RMF) | Un marco desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) que está diseñado para ayudar a los desarrolladores, usuarios y evaluadores de sistemas de IA a gestionar mejor los riesgos de la IA que puedan afectar a las personas, las organizaciones, la sociedad o el medioambiente. |
| MITRE ATT&CK | Una pauta para clasificar y describir ataques e intrusiones informáticos. |
| Objeto de directiva de grupo (GPO) | Permite que un administrador del sistema determine cómo interactuarán los usuarios y computadores. Las directivas de grupo son principalmente herramientas de seguridad, y un WWS puede usarlas para aplicar ajustes de seguridad a usuarios y computadoras, como requerir una longitud mínima de contraseña. |
| Parches | Actualizaciones de *software* y sistemas operativos que abordan vulnerabilidades de seguridad en un programa o producto. Los distribuidores de *software* pueden elegir emitir actualizaciones para corregir errores de desempeño y proporcionar funciones de seguridad mejoradas. |
| Plan de respuesta a emergencias (ERP) | Un plan que describe estrategias, recursos, otros planes y procedimientos que los WWS pueden usar para prepararse y responder a un incidente natural o causado por el hombre que pone en riesgo la vida, la propiedad o el medioambiente. |
| Plan de respuesta a incidentes (IR) | Una serie de procedimientos predeterminados y documentados para detectar y responder a un incidente informático. Algunos WWS pueden incluir su plan de IR de ciberseguridad como parte del plan de respuesta a emergencias del WWS.  |
| Prevención de pérdida de datos (DLP) | La práctica de detectar y prevenir filtraciones de datos, extracciones (robo o eliminación o movimientos no autorizados de datos desde un dispositivo) o destrucción indeseada de datos sensibles. Las organizaciones usan la DLP para proteger y asegurar sus datos y para cumplir con las regulaciones. |
| Programa Circuit Rider del área de Desarrollo Rural (RD) del Departamento de Agricultura de Estados Unidos (USDA) | Los Circuit Riders proporcionan asistencia técnica a sistemas de agua rurales sobre temas operacionales, financieros o gerenciales. |
| Programa de Información de Infraestructura Crítica Protegida (PCII) | El Programa de PCII protege información que habitualmente no es de dominio público y está relacionada con la seguridad de infraestructura crítica o sistemas protegidos, incluyendo documentos, registros u otra información de leyes federales, estatales y locales sobre divulgación. Esto permite a socios como los WWS compartir de manera segura su información de infraestructura crítica con la CISA sin temor a que sea divulgada. |
| Protocolo de escritorio remoto (RDP) | Un protocolo de comunicaciones de red desarrollado por Microsoft. Permite que los administradores del sistema diagnostiquen de manera remota problemas que tengan los usuarios individuales y da a los usuarios acceso remoto a sus computadoras de escritorio de trabajo físicas. Los técnicos de soporte a menudo usan el RDP para diagnosticar y reparar el sistema de un usuario de manera remota. |
| Punto de acceso inalámbrico | Un dispositivo que crea una red de área local (WLAN), a menudo en una oficina o edificio de gran tamaño. Un punto de acceso que se conecta a un enrutador, conmutador o concentrador cableado y proyecta una señal wifi en un área designada. |
| Red privada virtual (VPN) | Un servicio que extiende una red privada a una red pública (p. ej., Internet) y proporciona un canal seguro y cifrado entre el dispositivo del usuario y la red privada. Una VPN permite a los usuarios trabajar de manera remota.  |
| Registro | Un registro de los eventos que suceden dentro de los sistemas y las redes de TO y TI de un WWS. |
| Robo de identidad (*phishing*) | Correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos que engañan a las personas para descargar programas maliciosos, compartir información sensible (p. ej., números de Seguro Social y tarjetas de crédito, números de cuentas bancarias, credenciales de inicio de sesión) o para llevar a cabo otras acciones que los expongan o expongan su WWS a delitos informáticos. |
| Segmentación de la red | Dividir una red en múltiples segmentos o “subredes”, cada una actuando como su propia red pequeña. Esta función permite controlar el flujo de información entre subredes. Los WWS pueden usar la segmentación para mejorar el monitoreo, impulsar el desempeño, localizar los problemas técnicos y mejorar la ciberseguridad. |
| Seguridad de la capa de transporte (TLS) | Un protocolo de autenticación y cifrado ampliamente implementado en navegadores y servidores web. El tráfico del protocolo de transferencia de hipertexto (HTTP) (un método estándar para la comunicación entre clientes y servidores web) transmitido mediante TLS se conoce como protocolo seguro de transferencia de hipertexto (HTTPS).  |
| Seguridad de la capa de transporte de inicio (STARTTLS) | Un protocolo usado para garantizar que el correo electrónico se transporte de manera segura de un servidor a otro.  |
| Servicios activos | Programas que se ejecutan en segundo plano. |
| Servidor | Un programa o dispositivo informático que proporciona un servicio (como intercambio de datos o recursos) a otro programa informático y su usuario, también conocido como cliente. |
| Servidor bastión | Una computadora de propósito especial en una red de TO o TI que un sistema de agua potable y aguas residuales (WWS) diseña y configura específicamente para resistir ataques informáticos. |
| Servidor de accesos directos | Un dispositivo reforzado y monitoreado que abarca dos zonas de seguridad de la red disímiles y proporciona un medio controlado de acceso entre ellas. Fundamentalmente, funciona como un puente cerrado entre las zonas. |
| Sistema de agua comunitaria (CWS) | Un sistema de agua pública que suministra agua a la misma población durante todo el año.  |
| Sistema de control | Un sistema que ayuda a implementar un procedimiento o proceso (p. ej., tratamiento de agua). Algunos sistemas de control son el control de supervisión y adquisición de datos (SCADA), el sistema de control distribuido (DCS), los controladores lógicos programables (PLC) y otros tipos de sistemas de control industrial. |
| Sistema de control industrial (ICS) | Un sistema que se utiliza para controlar procesos industriales, como el tratamiento y la distribución de agua. Los ICS incluyen sistemas SCADA (a menudo usados en los WWS para controlar activos geográficamente dispersos), DCS y sistemas de control más pequeños que usan PLC para controlar procesos localizados.  |
| Sistema de detección de intrusiones/Sistema de protección contra intrusiones (IDS/IPS) | Ambos sistemas están dentro de una red para alertar cuando se detecta una intrusión no deseada. Un IDS está diseñado para proporcionar solo una alerta sobre un posible incidente. Un IPS, por el contrario, actúa bloqueando el intento de intrusión o corrigiendo de algún modo el ataque. |
| Sistema de información | Conjunto interconectado de recursos de información bajo el mismo control de gestión directa que comparten una funcionalidad común. Un sistema normalmente incluye *hardware*, *software*, información, datos, aplicaciones, comunicaciones y personas.  |
| Sistema operativo (OS) | *Software* que actúa como interfaz entre el *hardware* informático y el usuario. Las aplicaciones (p. ej., Microsoft Office) requieren un entorno en el que funcionar y realizar tareas. El OS ayuda a los usuarios a interactuar con las aplicaciones y otro *hardware* y programas. El OS también realiza tareas como archivar, almacenar en la memoria y gestionar procesos.  |
| Sociedad Internacional de Automatización (ISA) | Una asociación profesional sin fines de lucro fundada en 1945 para crear un mundo mejor a través de la automatización. La ISA desarrolla estándares globales ampliamente utilizados, otorga certificaciones a profesionales, proporciona educación y capacitación, publica libros y artículos técnicos, organiza conferencias y exhibiciones y ofrece programas de trabajo en redes y de desarrollo profesional a sus miembros y clientes. |
| Sociedad Internacional de Automatización/Comisión Electrotécnica Internacional (ISA/IEC) 62443 | La serie de estándares ISA/IEC 62443, desarrollada por el comité ISA99 y adoptada por la IEC, proporciona un marco flexible para abordar y mitigar las vulnerabilidades de seguridad actuales y futuras en los sistemas de control y automatización industriales (IACS). |
| *Software* | Un conjunto de datos, programas e instrucciones que se utiliza para manejar computadoras y ejecutar tareas específicas, que comprende desde sistemas operativos hasta distintas aplicaciones, esenciales para llevar a cabo una amplia variedad de funciones digitales. |
| Suplantación de identidad (*spoofing*) | Un tipo de estafa en la que un atacante oculta una dirección de correo electrónico, un nombre de visualización, un número de teléfono, un mensaje de texto o una URL de sitio web para convencer a un objetivo de que está interactuando con una fuente conocida y confiable. |
| Tácticas, técnicas y procedimientos (TTP) | Este es el término usado por profesionales de ciberseguridad para describir los comportamientos, los procesos, las acciones y las estrategias usadas por un atacante para cometer ataques informáticos. |
| Tecnología de la información (TI) | Una serie de recursos que una organización usa para recopilar, procesar, mantener, utilizar, intercambiar, distribuir o eliminar información. |
| Tecnología operacional (TO) | Los componentes de *hardware*, *software* y *firmware* de un sistema que un WWS usa para detectar o generar cambios en procesos físicos a través del control y monitoreo directos de dispositivos físicos. Para muchos WWS, esto consiste en un sistema SCADA. |
| Tráfico de red | La cantidad de datos que se desplaza entre una red durante un tiempo determinado. |
| Vulnerabilidad | Una falla o debilidad en una parte del *software* o *firmware* que un atacante puede usar para modificar el código de la aplicación, dañar un activo, obtener acceso a una red o ejecutar otra actividad maliciosa.  |
| Zona desmilitarizada (DMZ) | Una red perimetral que sirve como valla y rige el intercambio de información entre redes informáticas internas y externas. Regula la manera en que la información fluye desde una red interna hacia una red externa, y qué usuarios de la red externa pueden acceder a la red interna. A menudo se usa entre las redes de TO y TI de un WWS.  |

1. En virtud de la Ley de Informes de Incidentes Informáticos para Infraestructura Crítica (CIRCIA) de 2022, la CISA 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 el sector del agua y aguas residuales. Esta recomendación se revisará según sea necesario cuando se emita la Norma Definitiva de la CIRCIA. [↑](#footnote-ref-2)