Guía de respuesta a incidentes

Sector de agua y aguas residuales

Publicación: enero de 2024

Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency)
Oficina Federal de Investigaciones (Federal Bureau of Investigation)
Agencia de Protección Ambiental (Environmental Protection Agency)

Resumen ejecutivo

Los agentes de amenazas cibernéticas son conscientes de los puntos únicos de falla y los atacan de forma deliberada. Un riesgo o una falla de una organización del sector de agua y aguas residuales (WWS, por sus siglas en inglés) podría causar impactos en cascada en todo el sector, así como en otros sectores de infraestructura fundamental.

Hay muchos aspectos del amplio y complejo sector WWS que plantean desafíos para aumentar la resiliencia cibernética en todo el sector:

- La gobernanza y la regulación involucran una combinación de autoridades federales y estatales, locales, tribales y territoriales.
- Los niveles de madurez de ciberseguridad en todo el sector son dispares.
- A menudo, las empresas de servicios públicos del sector WWS deben priorizar los recursos limitados para la funcionalidad de sus sistemas de agua sobre la ciberseguridad.
- Las soluciones universales a los desafíos cibernéticos en un entorno diverso, rico en objetivos y pobre en recursos son inviables.

A fin de brindar un apoyo significativo en materia de ciberseguridad al sector WWS que pueda ayudar con estos desafíos, la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés), en conjunto con la Agencia de Protección Ambiental (EPA, por sus siglas en inglés) y la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), así como los socios del Gobierno federal y del sector WWS que se indican en la sección de agradecimientos de esta guía, ha creado esta Guía de respuesta a incidentes (IRG, por sus siglas en inglés) conjunta para el sector WWS.

El valor único[1] de esta IRG conjunta es que brinda a los propietarios y los operadores del sector WWS información sobre las funciones, los recursos y las responsabilidades federales para cada etapa del ciclo de vida de respuesta a incidentes (IR, por sus siglas en inglés) cibernéticos. Los propietarios y los operadores del sector pueden utilizar esta información para aumentar sus respectivos planes y procedimientos de IR. Capacitando a las empresas de servicios públicos individuales del sector WWS, los autores de esta guía (la CISA, la FBI, la EPA y los socios del Gobierno federal y del sector WWS que recibieron un agradecimiento) tienen como objetivo impulsar mejoras en la resiliencia cibernética y en la respuesta a incidentes en todo el sector WWS.

[1] Existen múltiples recursos para orientar la planificación de respuesta a incidentes (IR), p. ej., la Publicación especial (SP, por sus siglas en inglés) 800-61, revisión 2, del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) (NIST SP 800-61).

Agradecimientos

Además de quienes colocaron su sello en conjunto, la Agencia de Protección Ambiental y la Oficina Federal de Investigaciones, la Oficina de Inteligencia y Análisis del Departamento de Seguridad Nacional (DHS I&A, por sus siglas en inglés) contribuyó a esta IRG.

Las siguientes personas y organizaciones también contribuyeron a esta IRG: AlexRenew, American Water, Asociación de Administradores de Agua Potable del Estado (ASDWA, por sus siglas en inglés), Centro de Innovación Cibernética y Tecnológica (CCTI, por sus siglas en inglés), ciudad de Dover, Instituto de Preparación Cibernética (CRI, por sus siglas en inglés), DC Water, Dragos, Distrito Municipal de Servicios Públicos del Este de la Bahía (East Bay Municipal Utility District), EMA Inc., Google/Mandiant, Sociedad Internacional de Automatización (ISA, por sus siglas en inglés), Programa de Agua Potable (Drinking Water Program) en Maine de los Centros para el Control y la Prevención de Enfermedades (CDC, por sus siglas en inglés) y el Departamento de Salud y Servicios Humanos (DHHS, por sus siglas en inglés), Microsoft, Célula de Integración de Ciberseguridad y Comunicaciones de Nueva Jersey (NJCCIC, por sus siglas en inglés), Distrito de Agua y Saneamiento de Platte Canyon (Platte Canyon Water & Sanitation District), Comisión de Servicios Públicos de San Francisco (SFPUC, por sus siglas en inglés), Schneider Electric, Tenable, Tetra Tech, Trinity River Authority of Texas, Water Environment Federation, WaterISAC, West Yost Inc., Xylem y personas de la Asociación Americana de Obras Hidráulicas (AWWA, por sus siglas en inglés).

Descargo de responsabilidad

Índice

Propósito

Como coordinadora nacional para la seguridad y resiliencia de la infraestructura fundamental, la CISA creó esta guía de respuesta a incidentes (IRG), junto con la Oficina Federal de Investigaciones (FBI), la Agencia de Protección Ambiental (EPA) y los socios del sector federal, privado y sin fines de lucro a los que se agradeció más arriba, para proporcionar información sobre cómo las empresas de servicios públicos del sector de sistemas de agua y aguas residuales (en lo sucesivo, simplificado como "WWS") pueden trabajar con socios federales durante cada etapa del ciclo de vida del incidente cibernético.[2] Esta IRG asesora a las empresas de servicios públicos del WWS tanto sobre la idoneidad como sobre los medios de colaboración con entidades federales específicas para cada etapa del ciclo de vida. Las empresas de servicios públicos pueden utilizar esta IRG para aumentar su planificación de IR y colaborar con los socios federales y el WWS antes, en el transcurso y después de un incidente cibernético. **Nota:** Las empresas de suministro de agua con los medios y la capacidad para participar en un proceso colectivo más amplio de IR durante un incidente cibernético deben consultar el Anexo I: Una respuesta colectiva más avanzada.

Alcance

Esta guía proporciona información sobre posibles funciones, recursos y responsabilidades de IR de entidades gubernamentales federales específicas para apoyar a las entidades del WWS durante cada etapa del ciclo de vida del incidente cibernético. También sirve para contextualizar la importancia y el impacto potencial de un incidente cibernético del WWS para la seguridad nacional.

Esta guía no pretende lo siguiente:

- Exigir medidas.
- Proporcionar exhaustivas prácticas recomendadas cibernéticas.
- Establecer requisitos.
- Recomendar configuraciones técnicas.
- Compartir información sobre amenazas cibernéticas.
- Promocionar a proveedores o productos y servicios de proveedores.
- Entrar en conflicto con los requisitos reglamentarios establecidos u otros requisitos legales, ni reemplazarlos o sustituirlos.

Público

La CISA, la EPA, la FBI y los socios han adaptado esta guía para propietarios y operadores de empresas de servicios públicos del WWS de EE. UU., específicamente, para el personal de empresas de servicios públicos del WWS dedicado a la planificación y respuesta para incidentes cibernéticos. El personal debe consultar esta guía para obtener información sobre las funciones, las responsabilidades y los recursos federales relacionados con la respuesta a incidentes cibernéticos. La familiaridad con esta información preparará mejor a las empresas de servicios públicos del WWS para responder a un incidente cibernético y recuperarse de este. **Nota:** No se requiere experiencia técnica para utilizar esta guía de manera efectiva.

---

[2] Según lo definido en NIST SP 800-61: SP 800-61, revisión 2, Guía para el manejo de incidentes de seguridad informática.

Contexto de las amenazas

Los agentes cibernéticos maliciosos tienen diferentes objetivos y capacidades, lo que puede dar lugar a una amplia variedad de actividad de amenazas. La dependencia que muchos sectores de infraestructura fundamental de EE. UU. (incluidos los de energía, atención médica y salud pública) tienen del WWS hace que el sector sea un objetivo para los agentes de amenazas cibernéticas. Al atacar la infraestructura fundamental del WWS de EE. UU., los agentes cibernéticos maliciosos llevan a cabo actividades alineadas con sus objetivos generales, que pueden tener motivaciones financieras o políticas. En los últimos años, varios incidentes cibernéticos maliciosos han afectado al WWS, entre los que se incluyen el acceso no autorizado y el ransomware.[3]

Los agentes de amenazas cibernéticas suelen usar ransomware contra las empresas de servicios públicos del WWS. En las redes de tecnología operativa (OT, por sus siglas en inglés) conectadas a Internet, el ransomware puede propagarse rápidamente para afectar las operaciones. Por ejemplo, en julio de 2021, delincuentes cibernéticos utilizaron el ransomware ZuCaNo, mediante acceso remoto, para poner en riesgo una computadora de adquisición de datos y control de supervisión (SCADA, por sus siglas en inglés) en la red de OT de una empresa de servicios públicos del WWS con sede en Maine. Este incidente provocó que la empresa de servicios públicos volviera al control manual de procesos fundamentales. Además, en agosto de 2021, agentes cibernéticos maliciosos utilizaron la variante de ransomware Ghost contra una empresa de servicios públicos del WWS con sede en California. La variante de ransomware residió en el sistema durante aproximadamente un mes antes de su descubrimiento cuando tres servidores de SCADA mostraron un mensaje de ransomware.[4]

Los agentes cibernéticos de Estados nación también han demostrado un intento de atacar a las empresas de servicios públicos del WWS de EE. UU.
De acuerdo con el aviso conjunto sobre ciberseguridad "Agentes cibernéticos afiliados a los Cuerpos de la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés) explotan los controladores lógicos programables (PLC, por sus siglas en inglés) en múltiples sectores, incluidas las instalaciones de sistemas de agua y aguas residuales de EE. UU.",[5] en noviembre de 2023, el grupo de agentes cibernéticos "CyberAv3ngers", que está afiliado a los Cuerpos de la Guardia Revolucionaria Islámica (IRGC) del Gobierno iraní, atacó y puso en riesgo los controladores lógicos programables (PLC) de la serie Unitronics Vision elaborados por Israel que se utilizan en las empresas de servicios públicos del WWS de EE. UU. Los agentes cibernéticos probablemente accedieron al dispositivo afectado explotando las debilidades de ciberseguridad, incluida la seguridad deficiente de las contraseñas y la exposición a Internet.

---

[3] FBI, CISA, EPA, NSA. "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." Joint Cybersecurity Advisory. Oct. 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

[4] En el mismo lugar.

[5] FBI, CISA, NSA, EPA, INCD. "Cybersecurity Advisory IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities." Joint Cybersecurity Advisory. Dec. 1, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

Respuesta colectiva

1. Socios federales clave

Montones de entidades federales trabajan para asegurar el ciberespacio. Sin embargo, para los fines de esta guía, las empresas de servicios públicos del WWS pueden limitar su enfoque a los socios federales con equidad de ciberseguridad directa en el WWS: la CISA, la EPA, la FBI, la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) y la Oficina de Inteligencia y Análisis (I&A, por sus siglas en inglés) del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés).

La CISA es líder operativa de la ciberseguridad federal, coordinadora nacional para la seguridad y resiliencia de la infraestructura fundamental, y actúa como la agencia federal principal para la respuesta de activos. La CISA trabaja en estrecha colaboración con las siguientes entidades:

- La EPA, que es la agencia de administración de riesgos del sector del WWS.
- La FBI, que es líder federal para la respuesta a amenazas, el antiterrorismo y la contrainteligencia, así como un organismo de seguridad federal.
- La ODNI, que es líder de inteligencia para el análisis y el conocimiento de amenazas.
- La DHS I&A, que es líder de la prestación de inteligencia a socios estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés), y del sector privado.

Cada una de estas entidades federales desempeña funciones distintas y fundamentales para asegurar el WWS, y aprovechar sus respectivas autoridades y políticas ejecutivas.

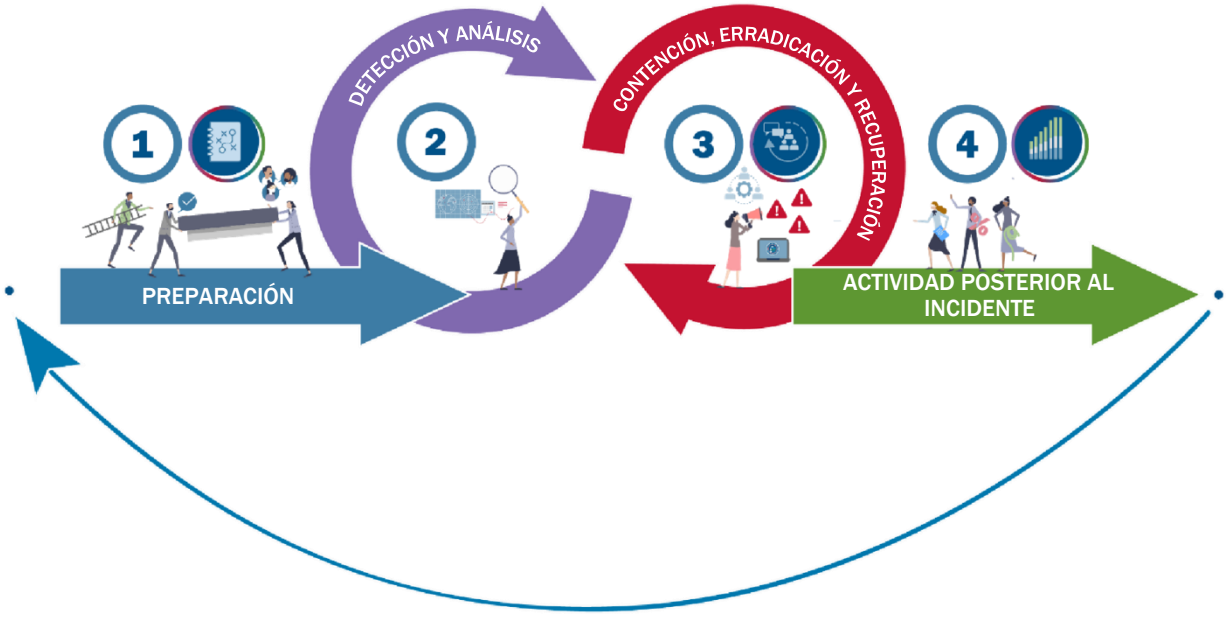
A medida que las empresas de servicios públicos del WWS analizan esta guía, deben considerar las funciones que estos socios federales pueden tener en los planes individuales de IR, así como los recursos, las herramientas y los servicios disponibles de estos socios.

1.1. Intercambio de información

Las empresas de servicios públicos deben tener en cuenta que la información específica que pueden proporcionar a los socios federales sobre un incidente cibernético podría ser invaluable. El intercambio bidireccional de información impulsa la respuesta federal colectiva y respalda la prestación de apoyo fundamental a las entidades afectadas. En incidentes que involucran a más de una entidad, el intercambio bidireccional de información puede permitir al Gobierno federal generar y compartir una imagen completa.

2. Proceso de respuesta a incidentes

Esta sección guía a las empresas de servicios públicos por el ciclo de vida de IR, identifica formas de interactuar con la respuesta a nivel federal y destaca medidas clave a fin de posicionarse y prepararse mejor para colaborar con socios federales. Las cuatro fases del ciclo de vida de IR, tal como se ilustran en la figura 1 y se definen en NIST SP 800-61, son la preparación; la detección y el análisis; la contención, la erradicación y la recuperación; y las actividades posteriores al incidente.



El ciclo de vida de IR proporciona a las organizaciones un marco paso a paso para identificar un incidente cibernético y responder a este. Esta IRG aprovecha el marco del ciclo de vida de IR, lo que permite a las empresas de servicios públicos del WWS aumentar sus propios planes de IR con información sobre las funciones, las responsabilidades y los recursos federales.

Figura 1: Ciclo de vida de respuesta a incidentes y vulnerabilidades

2.1. Preparación

La preparación, ilustrada en la figura 2, es la primera de cuatro etapas en el ciclo de vida de IR. La preparación para la respuesta a incidentes puede parecer contradictoria. Sin embargo, la preparación garantiza que una organización esté mejor posicionada para prevenir incidentes cibernéticos y reduce tanto el impacto como el tiempo necesario para volver a las operaciones normales. Si bien no hay dos empresas de servicios públicos que tengan las mismas consideraciones de planificación, unos pasos simples y priorizados pueden hacer que la preparación sea controlable.

Recursos del plan de IR

NIST SP 800-61: Guía para el manejo de incidentes de seguridad informática

Manuales de respuesta a vulnerabilidades e incidentes de ciberseguridad del Gobierno federal de la CISA.

Lista de cotejo de acciones en caso de incidentes de ciberseguridad de la Agencia de Protección Ambiental (EPA)

Orientación de administración de riesgos de ciberseguridad del sector de agua de la Asociación Americana de Obras Hidráulicas (AWWA)

Consideraciones de planificación de la Agencia Federal para el Manejo de Emergencias (FEMA, por sus siglas en inglés) para incidentes cibernéticos: orientación para administradores de emergencias

Recursos de referencia cibernética

Objetivos de Desempeño de Ciberseguridad (CPG, por sus siglas en inglés) Intersectoriales de la CISA

Evaluaciones de riesgos de ciberseguridad de la CISA

Evaluaciones de revisión validada del diseño de la arquitectura (VADR, por sus siglas en inglés) de la CISA

Análisis de vulnerabilidades de la CISA: vulnerability@cisa.dhs.gov

Herramientas y servicios gratuitos de ciberseguridad

Recursos comunitarios del WWS

Oficinas regionales de la CISA

Centro de Análisis e Intercambio de Información (ISAC, por sus siglas en inglés) de Agua

Asociación Americana de Obras Hidráulicas (AWWA)

Red de Respuesta de la Agencia de Agua y Aguas Residuales (WARN, por sus siglas en inglés)

Instituto de Preparación Cibernética

Sistema de Mando de Incidentes para los Sistemas de Control Industrial (ICS4ICS, por sus siglas en inglés)

Water Environment Federation

Figura 2: Fase de preparación

2.1.1. Creación de un plan de respuesta a incidentes a nivel organizacional

Crear un plan de IR a nivel organizacional es fundamental para prepararse para un incidente cibernético y establecer una postura para interactuar con las entidades federales. No existen dos planes de IR iguales, ya que dependen de las características individuales de la empresa de servicios públicos y de los requisitos únicos que esta tiene para presentar informes a las autoridades estatales, locales, territoriales o tribales (SLTT); y a los proveedores de seguros cibernéticos, así como de otras posibles obligaciones de presentación de informes.[6] Sin embargo, independientemente de los recursos, el tamaño, la ubicación, las obligaciones de presentación de informes o la estructura de propiedad, el hecho de tener un plan de IR individual es fundamental para interactuar con las agencias federales durante una crisis.[7]

2.1.2. Elevación de la referencia cibernética

Establecer una referencia sólida de ciberseguridad que incluya los controles y las protecciones fundamentales que se encuentran en los Objetivos de Desempeño de Ciberseguridad (CPG) de la CISA puede ayudar a una organización a desarrollar una arquitectura de red más defendible y reducir la posibilidad de convertirse en un objetivo fácil de oportunidades para un adversario. Mejorar la postura cibernética de una organización requiere comprender su referencia de ciberseguridad actual. Como la CISA entiende que estas mejoras requieren tiempo y recursos, les recomienda a las empresas de servicios públicos del WWS consultar los CPG para comenzar el proceso de fortalecimiento de su referencia de ciberseguridad. Una referencia sólida también es un elemento fundamental para que las organizaciones puedan detectar incidentes, responder a estos y recuperarse de ellos de forma efectiva. Por ejemplo, garantizar la segmentación de los sistemas informáticos y de OT, contar con copias de seguridad del sistema y mantener prácticas de registro suficientes son medidas recomendadas para minimizar los impactos de los incidentes cibernéticos y maximizar la capacidad de una organización para recuperarse rápidamente de estos incidentes.

2.1.3. Creación de la comunidad cibernética del sector de agua y aguas residuales

Las comunidades cibernéticas impulsan una respuesta colectiva. Las empresas de servicios públicos de cualquier nivel de madurez cibernética pueden interactuar con grupos, flujos de información y oficinas locales existentes que mejoren y eleven la postura de ciberseguridad del sector. Aunque esta interacción puede costar tiempo y recursos a las empresas de servicios públicos individuales, en definitiva, crea mejores condiciones para una respuesta colectiva a un incidente cibernético. Por lo tanto, esta guía recomienda encarecidamente que las empresas de servicios públicos de todos los tamaños investiguen sus comunidades cibernéticas locales y se integren en estas.[8]

2.2. Detección y análisis

La fase de detección y análisis, ilustrada en la figura 3, es el siguiente paso en el ciclo de vida de IR. Una respuesta sólida en esta etapa requiere dos componentes fundamentales: (1) informes precisos y oportunos, y (2) análisis colectivos rápidos para comprender el alcance total y el impacto de un incidente cibernético. Primero, para determinar si se debe informar un incidente, la empresa

---

[6] Para obtener más información sobre los seguros cibernéticos, consulte el sitio Seguro cibernético | Comisión Federal de Comercio (Federal Trade Commission).

[7] Para obtener más recursos sobre cómo crear un plan de IR a nivel organizacional, consulte el Anexo II.

[8] Para obtener sugerencias sobre cómo interactuar con su comunidad cibernética local, consulte el Anexo II.

de servicios públicos debe hacer todo lo posible para validar y confirmar que está experimentando un incidente cibernético malicioso. Segundo, caso por caso, la empresa de servicios públicos, a nivel organizacional, debe seguir los requisitos de presentación de informes obligatorios y considerar las opciones de presentación de informes opcionales para todos los incidentes confirmados.
Tercero, después de confirmar e informar el incidente a nivel organizacional, la empresa de servicios públicos debe determinar si puede participar en acciones de análisis colectivo a nivel estatal/federal para la actividad de amenazas. **Nota:** Para comprender cómo funciona el análisis colectivo a nivel federal, consulte el Anexo I de esta guía.

Objetivos de Desempeño de Ciberseguridad de la CISA

Lista de cotejo de acciones en caso de incidentes de ciberseguridad de la EPA

Nivel organizacional: proveedores de productos y servicios, proveedores de seguros y otros terceros.

Nivel SLTT: centros de fusión estatales, oficinas de administración de emergencias.

Nivel federal:

EPA: División de Infraestructura de Agua y Resiliencia Cibernética (Water Infrastructure and Cyber Resilience Division) por correo electrónico a watercyberta@epa.gov para proporcionar información de la situación de forma voluntaria.

CISA: por correo electrónico a report@cisa.gov, por teléfono al **(888) 282-0870** o comunicándose con una oficina regional local de la CISA.

FBI: comunicándose con la oficina central a través de www.ic3.gov o contactando a una oficina local de la FBI.

Análisis y asistencia técnicos de la CISA:

- **Análisis forense de hosts**
- **Análisis forense de redes**
- **Análisis forense de nubes**
- **Análisis forense de sistemas físicos y cibernéticos (CPFS, por sus siglas en inglés)**
- **Análisis de malware automatizado**
- **Análisis de códigos y medios**

Figura 3: Fase de detección y análisis

2.2.1. Validar

Como parte de la IR, las empresas de servicios públicos deben evaluar las redes y los sistemas afectados para detectar comportamientos del adversario.[9] Antes de informar un incidente, es importante **validar** que la actividad inusual no sea el resultado de actividades comunes relacionadas con errores del usuario, como configuraciones incorrectas del cortafuegos, problemas de control de acceso, etc. A continuación, se muestran algunas señales de que una organización puede estar experimentando un incidente cibernético malicioso:

- **Comportamiento inusual del sistema:** Si un sistema funciona más lento de lo habitual, falla con frecuencia o muestra demasiadas ventanas emergentes.
- **Actividad de red desconocida:** La actividad o el tráfico de la red muestra transferencias de datos inusuales o inesperadas, conexiones a direcciones de protocolos de Internet (IP, por sus siglas en inglés) desconocidas o intentos de acceso no autorizado.
- **Pérdida o modificación de datos sin explicación:** Los archivos desaparecen o se dañan repentinamente, o su contenido se modifica sin autorización.
- **Alertas del software de seguridad:** El software antimalware o cortafuegos de la empresa de servicios públicos envía advertencias.
- **Intentos de suplantación de identidad:** La empresa de servicios públicos recibe correos electrónicos, mensajes o llamadas telefónicas sospechosos que solicitan información personal o credenciales de inicio de sesión.
- **Redes o sistemas inusuales:** Dispositivos desconocidos o puntos de acceso no autorizados comienzan a aparecer en las redes del sistema.

La Lista de cotejo de acciones en caso de incidentes de ciberseguridad de la EPA y los Objetivos de Desempeño de Ciberseguridad de la CISA pueden brindar más orientación para ayudar a las empresas de servicios públicos a validar si están experimentando un incidente cibernético.

[9] Según los Manuales de respuesta a vulnerabilidades e incidentes de ciberseguridad del Gobierno federal de la CISA.

2.2.2. Informar

Nota: El panorama de informes de incidentes cibernéticos está en constante evolución.[10] Esta guía no pretende proporcionar una descripción completa de todos los canales de presentación de informes posibles. En cambio, pretende complementar los recursos existentes de respuesta a incidentes cibernéticos de una organización con posibles ejemplos ilustrativos de vías clave de presentación de informes para tener en cuenta. Las organizaciones deben consultar a su asesor legal para identificar los requisitos de presentación de informes legales, contractuales, reglamentarios y de otro tipo relevantes que puedan aplicarse en el momento del incidente cibernético.

Como siguiente fase del ciclo de vida de IR, la empresa de servicios públicos debe revisar sus obligaciones de presentación de informes y considerar participar en actividades adicionales y voluntarias de presentación de informes o intercambio de información.

Primero, el hecho de informar el incidente a nivel organizacional puede brindar acceso a la asistencia de un proveedor, un proveedor de servicios administrados (MSP, por sus siglas en inglés) o un proveedor de servicios de seguridad administrados (MSSP, por sus siglas en inglés), o una compañía de seguros. Segundo, el hecho de informar un incidente a nivel estatal y federal puede aumentar la comprensión del alcance total y el impacto del incidente cibernético, especialmente si este no es un caso aislado.

Si un adversario ataca a múltiples entidades de infraestructura fundamental, es posible que los Gobiernos federales y estatales no se den cuenta del alcance total de un incidente hasta que este haya progresado al punto de interrumpir los servicios. Los Gobiernos federales y estatales trabajan en conjunto con ciertas organizaciones, como WaterISAC, la Asociación Americana de Obras Hidráulicas y Water Environment Federation (WEF), para desarrollar una imagen más clara del panorama de amenazas del sector. La presentación de informes a cualquier nivel facilita la respuesta colectiva.

Informar sobre un incidente cibernético potencial o en curso podría impulsar numerosas medidas de respuesta federales. La CISA puede determinar que el dispositivo vulnerable que los agentes de amenazas están explotando en el sistema de OT de una empresa de servicios públicos del WWS se usa comúnmente en todo el sector. Luego, la CISA podría coordinarse con el proveedor del dispositivo afectado para que este pueda desarrollar estrategias de mitigación o corrección y notificar a otros clientes. Además, la información de amenazas cibernéticas (CTI, por sus siglas en inglés) que una empresa de servicios públicos del WWS comunique puede ayudar a la FBI a atribuir la actividad cibernética maliciosa a un Estado nación específico o a una amenaza persistente avanzada (APT, por sus siglas en inglés) delictiva. Una vez identificada, la FBI podría realizar actividades policiales para impedir más ataques de esa APT.

La presentación de informes puede ser un proceso confuso. Por lo general, hay tres niveles de consideración para la presentación de informes: organizacional, SLTT y federal. La Tabla 1 indica los pasos para la presentación de informes a nivel organizacional y SLTT, y la Tabla 2 proporciona los pasos para la presentación de informes a nivel federal.

---

[10] Se incluye más información sobre los requisitos federales de presentación de informes de incidentes cibernéticos en EE. UU., ya sea vigentes o propuestos en el Gobierno federal de EE. UU. a partir de septiembre de 2023, en el Apéndice B del informe del DHS: *Armonización de la presentación de informes de incidentes cibernéticos al Gobierno federal*, disponible en https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.

Tabla 1: Actividades y niveles de presentación de informes a nivel organizacional y SLTT

Nivel de presentación de informes	Actividad
Presentación de informes a nivel organizacional: Existen dos actividades de presentación de informes a nivel organizacional que se deben considerar.	Primero, si el incidente involucra una solución o un producto específicos, la empresa de servicios públicos debe considerar informárselo de inmediato al equipo de asistencia o al **equipo de respuesta a incidentes de seguridad de productos (PSIR, por sus siglas en inglés)** del proveedor si está disponible. Muchos proveedores tienen equipos de PSIR que mantienen portales de presentación de informes con direcciones de correo electrónico y portales web para recibir información sobre vulnerabilidades o incidentes del producto.[11]
	Segundo, la empresa de servicios públicos debería considerar informar el incidente a su **proveedor de seguros cibernéticos** designado para activar los servicios y las protecciones que correspondan.
Presentación de informes a nivel SLTT: Las entidades SLTT cuentan con orientación o mandatos únicos para informar incidentes cibernéticos, y las empresas de servicios públicos deben comprender claramente los requisitos específicos de su estado.	Por ejemplo, el estado de la empresa de servicios públicos puede requerir que los incidentes que afecten o puedan afectar el suministro de agua potable segura se informen a la Agencia de Primacía Estatal (State Primacy Agency).
	Además, cada estado cuenta con **oficinas de servicios de administración de emergencias** que tienen una función durante la respuesta a incidentes cibernéticos, especialmente si existen posibles consecuencias físicas derivadas del incidente cibernético.
	Por último, todos los estados tienen **centros de fusión** que monitorean los incidentes cibernéticos, y cada estado puede disponer de recursos adicionales de IR para empresas de servicios públicos que no pueden obtener asistencia externa.

[11] Según la norma 29147 de la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y los proveedores del marco de PSIR de FIRST.org.

Tabla 2: Actividades y niveles de presentación de informes a nivel federal

Nivel de presentación de informes	Actividad
Presentación de informes a nivel federal:[12] Como se indicó anteriormente, los socios federales con equidad de ciberseguridad directa en el sector de sistemas de agua y aguas residuales son la CISA, la EPA, la FBI y la ODNI. Estos son los agentes federales clave para que las empresas de servicios públicos consideren participar, especialmente, para permitir la IR colectiva. Esta guía describe *a quién* presentar informes, *por qué* es importante y *cómo* hacerlo. Las secciones a la derecha describen las posibles líneas de esfuerzo en términos de respuesta federal si un incidente alcanza el umbral colectivo. La CISA recomienda encarecidamente informar los incidentes cibernéticos a estas entidades federales.	**La CISA** cuenta con dos métodos principales de presentación de informes: de forma directa a una región o al centro operativo de la CISA, disponible las 24 horas, los 7 días de la semana. **Regiones de la CISA:** Una empresa de servicios públicos puede presentar un informe a la oficina regional de la CISA de su localidad. Una oficina regional de la CISA tiene varias funciones que puede realizar una vez que confirma un incidente. Por ejemplo, la oficina regional puede hacer lo siguiente: • Comunicarse con otros socios federales en nombre de la víctima. • Ir físicamente a la empresa de servicios públicos para brindar orientación o coordinación. • Plantear las necesidades de la víctima a la oficina central de la CISA. • Coordinarse con los centros de fusión estatales y federales pertinentes. • Ayudar a una víctima a abordar la respuesta federal. Además, las oficinas regionales de la CISA establecen relaciones personalizadas con la FBI y otras entidades federales en la medida de lo posible. Consulte cisa.gov/regions para obtener información de contacto para cada región. **Central de la CISA:** Una empresa de servicios públicos puede informar un incidente a la CISA enviando un correo electrónico a report@cisa.gov o llamando al (888) 282-0870. Para la presentación de informes, se requiere información del punto de contacto (POC, por sus siglas en inglés) de la empresa de servicios públicos, un número para devolver la llamada y una descripción del incidente. La ventaja de presentar el informe de esta manera es que el centro funciona las 24 horas del día, los 7 días de la semana, y garantiza que la CISA en general esté al tanto de la actividad.
	FBI: Una empresa de servicios públicos puede informar un incidente a la **oficina central de la FBI** ingresando a www.ic3.gov o comunicándose con una oficina local de la FBI. La FBI recomienda a las organizaciones presentar un informe, especialmente si el incidente tiene las siguientes características: • Involucra una pérdida significativa de datos, disponibilidad del sistema o control de los sistemas. • Afecta a un gran número de víctimas. • Indica el acceso no autorizado a sistemas informáticos críticos o que estos presentan un software malicioso. • Afecta la infraestructura fundamental o las funciones gubernamentales centrales. • Afecta la seguridad nacional, la seguridad económica o la salud y la seguridad pública.
	EPA: La EPA es la agencia de administración de riesgos del sector del WWS. Comuníquese con la **División de Infraestructura de Agua y Resiliencia Cibernética de la EPA** enviando un correo electrónico a watercyberta@epa.gov para proporcionar información de la situación de forma voluntaria.

[12] La información de contacto federal en este documento está actualizada al 17 de enero de 2024.

2.2.3. Análisis y asistencia técnicos de la CISA

La CISA y sus socios federales están listos para ayudar a las organizaciones a prepararse para los incidentes cibernéticos, responder a estos y mitigar su impacto. Caso por caso, las agencias federales podrían proporcionar herramientas y servicios sin costo a las empresas de servicios públicos afectadas. La CISA puede proporcionar análisis y asistencia técnicos de forma virtual o en el sitio a una organización luego de recibir un informe. Esta asistencia puede incluir lo siguiente:

- Orientación personalizada. La CISA puede proporcionar orientación estratégica y táctica a las organizaciones de infraestructura fundamental que se vieron afectadas por incidentes de ciberseguridad mediante experiencia técnica, inteligencia sobre amenazas, medidas de mitigación tácticas y las prácticas recomendadas de la industria. La CISA adapta esta orientación a la organización afectada.
- Asistencia técnica. Cuando la CISA brinda orientación y asistencia técnica de forma remota o en el sitio, la víctima recibirá recomendaciones accesibles y personalizadas en relación con los resultados del análisis del comportamiento del agente de amenazas y los artefactos relacionados:
    - Análisis forense de hosts. La CISA examina una amplia gama de sistemas host y proporciona un análisis detallado de puntos de conexión y artefactos forenses (tanto individuales como a escala) para detectar anomalías o la presencia del adversario. La CISA trabaja con las entidades afectadas para implementar tecnologías que faciliten los servicios de participación y realicen análisis de frecuencia, de registros y otros análisis forenses.
    - Análisis forense de redes. La CISA lleva a cabo actividades de detección de intrusiones a nivel de red para apoyar directamente las actividades de búsqueda e IR. La CISA trabaja con las entidades afectadas para instalar soluciones de supervisión de red a fin de ayudar en las actividades de participación, desarrollar firmas basadas en el tráfico de la red para identificar la actividad del adversario y examinar el tráfico de la red a escala.
    - Análisis forense de nubes. La CISA proporciona experiencia en la arquitectura de seguridad, el panorama tecnológico y el nexo de respuesta a incidentes para tecnologías basadas en la nube. La CISA brinda orientación sobre la utilización efectiva de las tecnologías de la nube, lo que facilita la capacidad de la empresa de servicios públicos para implementar rápidamente capacidades de respuesta a incidentes.
    - Análisis forense de sistemas físicos y cibernéticos (CPFS). La CISA brinda análisis forense y búsqueda de amenazas de entornos que incluyen sistemas de control industrial (ICS, por sus siglas en inglés) o SCADA mediante analistas de ICS especialmente capacitados y experimentados. Estos analistas utilizan planes de búsqueda adaptados a entornos y circunstancias específicos. El CPFS incluye el análisis del tráfico de la red, el análisis de hosts y las comunicaciones por radio con protocolos en serie e interrogación a nivel de dispositivos del campo de ICS. Los analistas de CPFS mantienen competencia en las estructuras y metodologías generales que se encuentran en los 16 sectores de infraestructura fundamental a fin de estar preparados para brindar asistencia experta a las entidades de ICS afectadas.

- **Análisis de malware automatizado**. La CISA genera un informe automatizado para quienes envían informes, y este brinda indicadores de riesgo (IOC, por sus siglas en inglés), la asignación de MITRE ATT&CK® e información sobre la mitigación.
- **Análisis de códigos y medios**. La CISA proporciona un análisis en profundidad de ingeniería inversa de muestras de malware. La CISA proporciona sus conclusiones mediante informes detallados de análisis de malware, que explican cómo operó el malware enviado cuando se ejecutó y detallan los indicadores asociados.

2.2.4. Análisis y asistencia técnicos de la FBI

La FBI cuenta con escuadrones cibernéticos especialmente capacitados en cada una de sus 56 oficinas locales. Estos trabajan en colaboración con los socios de los grupos de trabajo interinstitucionales de todo el Gobierno para brindar análisis y asistencia técnicos. Al igual que la CISA, la FBI implementa recursos caso por caso, según los mecanismos de informes y priorización.

- En la FBI, el personal de respuesta a un incidente cibernético son los agentes especiales cibernéticos de la oficina local. Antes de un incidente, la oficina local prioriza la interacción con empresas, negocios y propietarios y operadores de infraestructura fundamental para desarrollar relaciones y conocimientos relacionados con cada entidad.
- Cuando se produce un incidente, la oficina local administra la respuesta y el despliegue de agentes especiales y personal técnico al sitio, una posible investigación y, si corresponde, la implementación de capacidades técnicas avanzadas adicionales, como el Equipo de Acción Cibernética (CAT, por sus siglas en inglés). **Nota:** Cuando ocurre un incidente, la empresa de suministro de agua debe proporcionar lo siguiente a la FBI: (1) la facultad de firma de consentimientos para realizar actividades de investigación y (2) la disposición de las redes informáticas y de OT. Comúnmente, la FBI, a discreción del equipo del caso, proporcionará a la entidad la información encontrada como parte de las actividades de investigación. Esta información puede detallar los resultados de actividad maliciosa o la falta de esta.
- El CAT de respuesta rápida se compone de agentes especiales y científicos informáticos que se especializan en la respuesta a incidentes cibernéticos. El CAT brinda apoyo en la investigación y respuestas a preguntas fundamentales que pueden hacer avanzar un caso rápidamente. Con capacitación avanzada en intrusiones informáticas, investigaciones forenses y análisis de malware, el CAT puede desplegarse en todo el país en cuestión de horas para responder a incidentes importantes. Tras la activación de un equipo del caso, el CAT estará en el sitio dentro de las 24 horas cuando se trate de ubicaciones en los Estados Unidos continentales (CONUS, por sus siglas en inglés) y dentro de las 48 horas cuando se trate de ubicaciones fuera de los Estados Unidos continentales (OCONUS, por sus siglas en inglés). Consulte https://www.fbi.gov/news/stories/the-cyber-action-team.

2.3. Contención, erradicación y recuperación

La contención, erradicación y recuperación es el siguiente paso en el ciclo de vida de IR. A nivel organizacional, las empresas de servicios públicos del WWS continuarán siguiendo sus planes de IR establecidos durante todo el proceso de respuesta. Mientras tanto, a nivel colectivo, los socios se centrarán en garantizar una respuesta coordinada durante toda la fase de contención, erradicación y recuperación. Según la gravedad del incidente, el enfoque de los socios puede centrarse adicionalmente en coordinar el análisis y la asistencia técnicos para las entidades afectadas.

El intercambio continuo de información entre las partes interesadas afectadas ayuda a impulsar medidas de respuesta y mitigación.

La CISA trabaja en estrecha colaboración con socios interinstitucionales y del sector privado para compartir conocimientos relacionados con incidentes cibernéticos. La CISA publica orientación de mitigación y avisos sobre ciberseguridad en su página web.

La EPA publica alertas específicas sobre el agua en su página web, en la que las empresas de servicios públicos del WWS también pueden suscribirse para recibir información de la División de Infraestructura de Agua y Resiliencia Cibernética (WICRD, por sus siglas en inglés).

La CISA puede proporcionar información a las empresas de servicios públicos del WWS afectadas para ayudarlas a contener y erradicar a los agentes de amenazas no autorizados dentro de sus activos.

La asistencia para la corrección y mitigación puede incluir la mitigación de vulnerabilidades del software y el asesoramiento sobre respuestas y desalojos.

Figura 4: Fase de contención, erradicación y recuperación

2.3.1. Mensajería coordinada e intercambio de información

Aunque cada incidente o amenaza cibernéticos es particular y requiere una respuesta colectiva personalizada, los propietarios y operadores de empresas de servicios públicos del WWS deben centrarse en las siguientes actividades potenciales que, probablemente, formen parte de la mayoría de las respuestas:

- **Orientación de mitigación**: En el caso de un incidente cibernético, la CISA y otros socios desarrollarán, coordinarán y distribuirán alertas y orientación de mitigación relevantes durante la respuesta. Estas comunicaciones pueden incluir lo siguiente:
    - **Avisos sobre ciberseguridad:** La CISA y los socios interinstitucionales relevantes, p. ej., la FBI, desarrollan, sellan en conjunto y publican estos avisos, que contienen información técnica relevante y actualizada en relación con el incidente cibernético actual, incluidas las medidas de mitigación. La CISA los publica en su página web.
    - **Alertas personalizadas de ciberseguridad:** La EPA publica alertas específicas sobre el agua en su página web, que también brinda un formulario de inscripción para suscribirse a información general que la División de Infraestructura de Agua y Resiliencia Cibernética (WICRD) puede enviar.
- **Intercambio de información:** Durante la respuesta colectiva, los socios compartirán continuamente información relevante para apoyar los esfuerzos de respuesta y defensa. La información típica que se comparte con la CISA, o que la agencia comparte, durante los esfuerzos de respuesta incluye tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) relevantes del adversario, indicadores de riesgo (IOC) pertinentes y otros datos técnicos relevantes que las empresas de servicios públicos o sus proveedores de servicios externos pueden utilizar en su respuesta a nivel organizacional. Es probable que esta información se comparta a través de los canales de comunicación establecidos en las fases preparatorias de la respuesta colectiva. La CISA y sus socios suelen utilizar esta información con el propósito de determinar la necesidad y el contenido de los avisos sobre ciberseguridad.[13]

2.3.2. Asistencia para la corrección y mitigación

Según el tipo de incidente, la CISA puede proporcionar información vital a los propietarios y operadores de empresas de servicios públicos del WWS sobre las medidas defensivas que deben tomar para contener y erradicar a los agentes de amenazas no autorizados en sus activos.

- **Mitigación de vulnerabilidades del software.** La CISA y otros socios pueden desarrollar y proporcionar medidas de mitigación contra las vulnerabilidades del software antes y después de la explotación.
- **Desalojo del adversario y respuesta contra este.** Después de la explotación y la infiltración, la CISA y otros socios pueden brindar asesoramiento sobre una medida efectiva para contrarrestar el movimiento de los adversarios dentro de las redes y los activos de las empresas de servicios públicos del WWS. La CISA y otros socios también pueden brindar

[13] Para obtener más información sobre el intercambio de información con el Gobierno federal durante un incidente, consulte el Anexo I.

orientación sobre cómo quitar los métodos de persistencia del adversario y desalojar el control de este dentro de las redes y los activos de las empresas de servicios públicos del WWS.

2.4. Actividad posterior al incidente

La actividad posterior al incidente es el último paso en el ciclo de vida de IR. Al concluir cualquier incidente cibernético, es importante que todos los socios relevantes lleven a cabo un análisis retrospectivo del incidente y de cómo lo manejaron los intervinientes. El resumen de las actividades posteriores al incidente determina las "conclusiones obtenidas".

Figura 5: Actividad posterior al incidente

2.4.1. Retención de pruebas

La retención de pruebas es el proceso de preservar datos y pruebas relacionados con el incidente para el procesamiento o la investigación potenciales en el futuro, lo cual es especialmente importante para la FBI. Como parte de la preparación, las organizaciones deben tener un proceso bien definido para preservar datos y pruebas relacionados con incidentes cibernéticos. Este proceso debe incluir pautas claras para la recopilación y el almacenamiento de datos, así como el acceso a estos. La CISA y sus socios interinstitucionales instan encarecidamente a las empresas de servicios públicos a implementar este proceso en su planificación. Las oficinas regionales de la CISA o de la FBI pueden brindar orientación sobre la retención de datos.

2.4.2. Uso de datos de incidentes recopilados

De forma voluntaria, la CISA y sus socios interinstitucionales recopilan datos de las organizaciones afectadas, los anonimizan y los comparten ampliamente para apoyar a los defensores cibernéticos en todo el espacio de infraestructura fundamental. Estos datos pueden incluir TTP relevantes, IOC y otros datos técnicos que puedan apoyar la defensa colectiva.

2.4.3. Conclusiones obtenidas

La CISA y sus socios recopilarán las conclusiones obtenidas del esfuerzo de respuesta. Un análisis de conclusiones obtenidas permite a todos los socios revisar la efectividad y eficiencia del manejo de incidentes. A menudo, este proceso puede ser tan simple como una reunión de todos los intervinientes para revisar el incidente de forma cronológica. La evaluación de la información obtenida mediante la retención de pruebas puede generar soluciones prácticas y no técnicas. Por ejemplo, los registros bien mantenidos del incidente pueden revelar la cantidad de horas que el personal dedicó a realizar tareas específicas, lo que puede determinar la forma en que una organización manejará los incidentes futuros. Consolidar las conclusiones en un informe formal es una manera efectiva de conmemorar los factores clave, capacitar al personal nuevo y aumentar la conciencia situacional en toda la organización.

Anexo I: Una respuesta colectiva más avanzada

El sector de agua y aguas residuales es grande y complejo. Los niveles de madurez de ciberseguridad en todo el sector son dispares. A menudo, las empresas de servicios públicos de WWS deben priorizar los recursos limitados para la funcionalidad de sus sistemas de agua sobre la ciberseguridad. Por lo tanto, la CISA no espera que las empresas de servicios públicos participen en acciones colectivas para responder a un incidente cibernético más allá de administrar su propia respuesta organizacional. Sin embargo, en la medida de lo posible, la CISA agradece y alienta la participación en sus esfuerzos de respuesta colectiva de socios relevantes de todo el sector. En este caso, la CISA también agradece la participación de las empresas de servicios públicos del WWS que no sean las víctimas específicas del incidente. El siguiente anexo describe las actividades de coordinación que las empresas de servicios públicos pueden experimentar si optan por realizar actividades colectivas.

A. Análisis colectivo

Como coordinadora nacional para la resiliencia y seguridad de la infraestructura fundamental, la CISA participa en la revisión y clasificación federal de los incidentes del sector informados, mediante análisis colectivos para determinar la magnitud y el alcance del incidente. La CISA se coordina con socios federales para descubrir el impacto total y cualquier impacto cruzado o en cascada en otros sectores de infraestructura fundamental. Según corresponda, la CISA interactúa con socios externos relevantes para recopilar información adicional, evaluar la gravedad del incidente y generar conciencia situacional común.

La evaluación colectiva de un incidente cibernético tiene dos propósitos. Primero, fomenta el intercambio de información que servirá de base para las actividades de mitigación o corrección. Segundo, ayuda a los socios a determinar si se justifica la acción colectiva.

Según los resultados del período de evaluación, los socios relevantes (agencias federales, autoridades SLTT, MSP/MSSP, proveedores de ICS, etc.) trabajarán juntos en los próximos pasos para la mitigación o corrección. Los socios deben basarse en sus propios planes y políticas de IR para determinar actividades específicas de mitigación o corrección, pero pueden tener oportunidades para alinear y coordinar esas actividades en el futuro. Entre las medidas de coordinación que la CISA puede adoptar en esta etapa, se incluyen las siguientes:

- **Canales de comunicación**. La CISA puede establecer un chat en tiempo real (p. ej., Slack) dedicado a un incidente específico e incluir los puntos de contacto técnicos, legales, de políticas y comunicaciones relevantes de las organizaciones asociadas.
- **Reglas de interacción**. La CISA y sus socios determinarán de manera colectiva la frecuencia de las reuniones de las partes interesadas y los medios de comunicación (principales, alternativos y de emergencia).
- **Criterios colectivos**. La CISA y sus socios se esforzarán por establecer criterios de éxito para determinar cuándo las operaciones pueden volver a la cadencia de operaciones anterior al incidente.

Para invitarla a participar en actividades de respuesta colectiva, la CISA puede comunicarse con una empresa de servicios públicos de manera proactiva, por ejemplo, directamente, a través de otra agencia federal o mediante un socio SLTT, del ISAC o de una asociación. Cualquier participación en la respuesta colectiva que lidere la CISA se lleva a cabo de forma estrictamente voluntaria.

B. Respuesta colectiva

Una vez completado el análisis colectivo inicial, la CISA y sus socios pueden decidir coordinarse y colaborar continuamente en una respuesta. A continuación, se detallan algunas de las formas en que esta colaboración puede manifestarse:

- **Reuniones rápidas y periódicas específicas de incidentes**. La CISA puede organizar una reunión rápida para los socios relevantes, incluidas las entidades relevantes del WWS, con el propósito de 1) proporcionar información de referencia sobre los incidentes para los socios y 2) solicitar actualizaciones o recomendaciones sobre los próximos pasos a los socios.

- **Coordinación técnica**. La CISA y sus socios pueden coordinarse para brindar servicios técnicos a las víctimas, según la gravedad del incidente.

- **Coordinación de comunicaciones externas**. La CISA y sus socios pueden coordinar mensajes externos según corresponda. Por lo general, los socios apoyan el desarrollo, la distribución o la amplificación de las orientaciones, las alertas y los avisos públicos de mitigación para las partes afectadas.

- **Intercambio continuo de información**. Una IR colectiva efectiva depende de una estrecha colaboración operativa y del intercambio de información técnica entre los socios relevantes. Este intercambio de información generalmente ocurre a través de canales de comunicación previamente establecidos (como se describe en la sección "Análisis colectivo"), intercambios técnicos directos entre organizaciones o mediante procesos automatizados de intercambio de información técnica. El tipo de información que se comparte de forma continua suele incluir detalles técnicos (p. ej., IOC, TTP) y estrategias de mitigación (p. ej., respuestas físicas, registros mejorados).

C. Actividades colectivas posteriores al incidente

Normalmente, la CISA llevará a cabo una revisión después de un incidente para recopilar observaciones, conclusiones obtenidas, prácticas recomendadas y áreas de mejora relacionadas con la planificación y las operaciones de la CISA asociadas con el incidente cibernético.

- **Evaluación de conclusiones obtenidas**. Antes de la desmovilización, la CISA puede solicitar aportes a todas las partes involucradas en el proceso para evaluar la respuesta. Esta es una oportunidad para que los socios proporcionen comentarios sobre el proceso de respuesta, así como para considerar retrospectivamente los aspectos más destacados de la colaboración, los desafíos de la colaboración y la reflexión sobre las consideraciones del ancho de banda y las actividades de preparación adicionales que pueden mejorar la colaboración con la comunidad operativa relevante en el futuro.

Anexo II: Recursos de preparación

La siguiente lista proporciona recursos para implementar las recomendaciones en la sección *2.1: Preparación* de este documento.

A. Creación de un plan de IR a nivel organizacional:

- NIST SP 800-61. Guía para el manejo de incidentes de seguridad informática: Esta guía es fundamental para crear planes de IR a nivel organizacional. La guía es universal y aplicable para cualquier organización, independientemente del sector. Muchas otras guías de IR se asignan a esta publicación o hacen referencia a esta.

- Lista de cotejo de acciones en caso de incidentes de ciberseguridad de la Agencia de Protección Ambiental (EPA): La lista de cotejo cubre las medidas que se deben tomar para **prepararse** para un incidente, **responder** a un incidente y **recuperarse** de un incidente.

- Orientación de administración de riesgos de ciberseguridad del sector de agua de la Asociación Americana de Obras Hidráulicas (AWWA): Esta orientación brinda un enfoque voluntario y específico del sector para adoptar el Marco de ciberseguridad del NIST.

- Manuales de respuesta a vulnerabilidades e incidentes de ciberseguridad del Gobierno federal de la CISA: Estos manuales, adaptados a las agencias del Poder Ejecutivo Civil Federal (FCEB, por sus siglas en inglés), proporcionan un conjunto estándar de procedimientos para identificar, coordinar, corregir, recuperar y monitorear las medidas de mitigación exitosas de incidentes y vulnerabilidades que afectan a los sistemas, los datos y las redes del FCEB. Si bien los manuales son para el FCEB, a las empresas de servicios públicos del WWS pueden resultarles útiles para crear sus propios planes.

- Agencia Federal para el Manejo de Emergencias (FEMA). Sistema Nacional de Administración de Incidentes (NIMS, por sus siglas en inglés): Este sistema guía a todos los niveles de gobierno, a las organizaciones no gubernamentales y al sector privado sobre cómo trabajar juntos para prevenir y mitigar incidentes, protegerse y recuperarse de estos, y responder a ellos. Aunque los incidentes a los que se hace referencia *no* se limitan a incidentes cibernéticos, la guía proporciona información fundamental que se debe considerar al crear planes de IR individuales.

    - Consideraciones de planificación para incidentes cibernéticos. Orientación para administradores de emergencias: La FEMA desarrolló esta guía en coordinación con la CISA para ayudar al personal de administración de emergencias SLTT a prepararse de manera colaborativa para un incidente cibernético y apoyar el desarrollo de un plan o anexo de respuesta a incidentes cibernéticos. Si bien se centran en las funciones y responsabilidades que pueden tener los administradores de emergencias gubernamentales, a los administradores de emergencias en el mundo académico, las organizaciones sin fines de lucro o el sector privado también deberían resultarles útiles los conceptos.

    - El Sistema de Mando de Incidentes (ICS) es un sistema de administración diseñado para permitir la administración de incidentes nacionales efectiva y eficiente a través de la integración de una combinación de instalaciones, equipos, personal, procedimientos y comunicaciones que operan dentro de una estructura

organizacional común. El Centro de Recursos del ICS (fema.gov) incluye capacitación, ayudas laborales y materiales de referencia.

- Para obtener más ayuda para comprender e implementar el ICS de la FEMA, consulte la serie informativa de la AWWA: Facilitación del ICS para sistemas de agua y aguas residuales de cualquier tamaño.

- **Recursos específicos del proveedor:** Los proveedores de productos con los que trabajan las empresas de servicios públicos pueden tener recursos y recomendaciones adicionales para los planes de IR a nivel organizacional. Por ejemplo, los proveedores pueden recomendar el establecimiento de un marco de administración de la recopilación: un componente clave para acelerar la investigación de incidentes y la respuesta a estos es comprender la información clave que las empresas de servicios públicos deben recopilar, así como durante cuánto tiempo y dónde almacenarla. Establecer un marco de administración de la recopilación ayuda a una organización a convertir rápidamente la actividad sospechosa en un conjunto de hipótesis y a saber qué datos están disponibles para ayudar a diferenciar entre un incidente cibernético y un evento benigno. Un proveedor de productos debería poder brindar instrucciones sobre qué datos se registran y el método para acceder a esos registros.

B. Recursos para elevar la referencia cibernética:

Existe una variedad de recursos destinados a comprender la referencia cibernética de una organización y mejorar la higiene cibernética:

- **Objetivos de Desempeño de Ciberseguridad (CPG):** Los CPG de la CISA son un subconjunto de prácticas voluntarias de ciberseguridad para ayudar a las organizaciones pequeñas y medianas a impulsar sus esfuerzos de ciberseguridad priorizando la inversión en una cantidad limitada de medidas esenciales con resultados de seguridad de alto impacto.

- **15 fundamentos de ciberseguridad para servicios de agua y aguas residuales:** La guía 15 fundamentos de ciberseguridad para servicios de agua y aguas residuales de WaterISAC contiene las prácticas recomendadas, agrupadas en 15 categorías principales, que los sistemas de agua y aguas residuales pueden implementar para reducir los riesgos de seguridad de sus sistemas informáticos y de OT. Cada recomendación contiene enlaces a los recursos técnicos correspondientes, que brindan información para profundizar en cada tema.

- **Realizar una evaluación de riesgos de ciberseguridad:** Realizar una evaluación de riesgos ayuda a una organización a comprender los riesgos cibernéticos para sus operaciones, activos organizacionales e individuos. Las oficinas regionales de la CISA pueden ayudar a establecer evaluaciones de riesgos para las empresas de servicios públicos del WWS.

- **Realizar una evaluación de revisión validada del diseño de la arquitectura (VADR):** Una VADR es una evaluación basada en estándares, pautas y prácticas recomendadas federales y de la industria. Las evaluaciones se pueden realizar en infraestructuras informáticas o de OT (ICS-SCADA). Estas se centran en 1) la evaluación de la arquitectura, 2) el análisis del tráfico de la red y 3) la revisión y el análisis de registros de sistemas. Las oficinas regionales de la CISA pueden ayudar a establecer las VADR para las empresas de servicios públicos del WWS.

- **Análisis de vulnerabilidades:** La CISA utiliza herramientas automatizadas para llevar a cabo análisis de vulnerabilidades en redes externas. Estas herramientas buscan vulnerabilidades y configuraciones débiles que los adversarios podrían utilizar para realizar actividades cibernéticas maliciosas. El análisis proporciona una revisión externa y no intrusiva de los sistemas accesibles a través de Internet. El análisis no llega a la red privada de la organización y no puede realizar ningún cambio. La CISA envía a los participantes informes semanales con información sobre las vulnerabilidades conocidas que se detectaron en activos accesibles a través de Internet, comparaciones semanales y las medidas de mitigación recomendadas.

    - Envíe un correo electrónico a vulnerability@cisa.dhs.gov con el asunto "Requesting Vulnerability Scanning Services" (Solicitud de servicios de análisis de vulnerabilidades). Incluya el nombre de su empresa de servicios públicos, un punto de contacto con una dirección de correo electrónico y la dirección física de la oficina central de su empresa de servicios públicos.

    La CISA responderá con un formulario de solicitud de servicios y una carta de aceptación del análisis de vulnerabilidades para obtener la información necesaria sobre su empresa de servicios públicos y su autorización para analizar sus redes públicas.

- **Herramientas y servicios gratuitos de la CISA:** La CISA ha compilado una lista de herramientas y servicios de ciberseguridad gratuitos para ayudar a las organizaciones a potenciar aún más sus capacidades de seguridad. Este repositorio activo incluye los servicios de ciberseguridad que brinda la CISA, herramientas de código abierto ampliamente utilizadas y herramientas y servicios gratuitos que ofrecen las organizaciones del sector privado y público en toda la comunidad de ciberseguridad.[14]

- **NIST SP 800-82, revisión 3, Guía para la seguridad de la tecnología operativa (OT):** Este documento brinda orientación sobre cómo asegurar la OT y, al mismo tiempo, aborda sus requisitos únicos de seguridad, confiabilidad y desempeño. Incluye una descripción general de las topologías típicas del sistema y de la OT, identifica amenazas y vulnerabilidades comunes de estos sistemas y proporciona respuestas de seguridad recomendadas para mitigar los riesgos asociados.

C. Creación de la comunidad cibernética del sector de agua

Las comunidades operativas impulsan una respuesta colectiva. Las empresas de servicios públicos de cualquier nivel de madurez cibernética pueden interactuar con grupos, flujos de información y oficinas locales existentes para elevar la postura de ciberseguridad del sector de agua. La interacción puede costar tiempo y recursos a las empresas de servicios públicos individuales, pero, en definitiva, crea mejores condiciones para una respuesta colectiva a un incidente cibernético.

- **Interactúe con su Centro de Análisis e Intercambio de Información (ISAC) de Agua:** Por lo general, la mayoría de los sectores fundamentales cuentan con ISAC individuales que funcionan como un centro de intercambio de información gubernamental y privada que

[14] Consulte la página de la CISA Servicios y herramientas de ciberseguridad gratuitos | CISA.

ayuda a los miembros a identificar riesgos y prepararse para emergencias. WaterISAC es el ISAC del sector de agua. Únase a WaterISAC a través de su página web.

- **Conozca las oficinas estatales, locales, tribales y territoriales (SLTT):** Los Gobiernos SLTT son socios clave para ayudar a prepararse para un incidente cibernético y responder a este. Además de proporcionar orientación y recursos de ciberseguridad, las autoridades SLTT pueden proporcionar información sobre las leyes y regulaciones que puedan servir de base para la planificación de IR. Por ejemplo, los requisitos de notificación de filtración de datos varían según el estado. El riesgo de la información que permite la identificación personal (PII, por sus siglas en inglés), como las direcciones de facturación de clientes, puede requerir diferentes medidas por parte de la empresa de servicios públicos según el estado de residencia de los clientes afectados.

- **Conozca las oficinas regionales federales:** Las empresas de servicios públicos pueden acceder a la variedad de capacidades de desarrollo de resiliencia, mitigación de riesgos e IR de la CISA mediante 10 oficinas regionales, que comprenden las consideraciones de planificación exclusivas de comunidades, estados y regiones específicos. Considere programar una visita de asistencia mediante la oficina regional correspondiente a fin de explorar las oportunidades para mejorar el intercambio de información con socios gubernamentales, identificar vulnerabilidades y reducir el riesgo.

- **Explore las asociaciones sin fines de lucro:** Existe una amplia comunidad de organizaciones sin fines de lucro disponibles para apoyar la planificación de IR, la preparación y la respuesta de las empresas de servicios públicos del WWS. El Instituto de Preparación Cibernética (CRI), la Asociación Americana de Obras Hidráulicas (AWWA) y el Sistema de Mando de Incidentes para Sistemas de Control Industrial (ICS4ICS) son ejemplos de estas oportunidades de colaboración. Además de proporcionar capacitación y recursos directos, interactuar con socios sin fines de lucro desarrolla relaciones e impulsa la cooperación en todo el sector.

- **Únase a la WARN de su estado o a otras organizaciones de asistencia mutua:** Una Red de Respuesta de la Agencia de Agua y Aguas Residuales (WARN) es una red de empresas de servicios públicos que ayudan a otras a responder a emergencias y recuperarse de estas. El hecho de participar en una WARN permite que las empresas de servicios públicos que han sufrido o que anticipan daños de incidentes naturales o causados por humanos brinden y reciban ayuda y asistencia de emergencia en forma de personal, equipos, materiales y otros servicios asociados, según sea necesario, de otras empresas de servicios públicos del WWS.

- **Comprenda cómo aprovechar las capacidades de respuesta a incidentes de seguridad de productos (PSIR) de los proveedores:** La OT en sistemas de agua y aguas residuales suele comprender productos de varios proveedores de sistemas de control industrial. A su vez, estos proveedores, por lo general, cuentan con Equipos de Respuesta a Incidentes de Seguridad de Productos (PSIRT, por sus siglas en inglés) para manejar las respuestas a informes de vulnerabilidad e incidentes específicos de esos productos. Comprender e incluso ensayar los procesos de PSIR de los proveedores puede aumentar la planificación de IR de la empresa de servicios públicos (p. ej., ¿cómo un proveedor notifica a los clientes sobre una vulnerabilidad asociada con un dispositivo específico?).