

AUTOR: YANIR LAUBSSTEIN

PROTEGER LAS INFRAESTRUCTURAS DE AGUA Y SANEAMIENTO DE AMENAZAS CIBERNÉTICAS

UN ESTUDIO DE CIBERSEGURIDAD
PARA AMÉRICA LATINA Y EL CARIBE

EDITORES:

ARIEL NOWERSZTERN • MARCELLO BASANI • FERNANDO MELEAN • HILA COHEN MIZRAV



Proteger las infraestructuras de agua y saneamiento de amenazas cibernéticas

Un estudio de ciberseguridad
para América Latina y el Caribe

Autor:

Yanir Laubshtein

Editores:

Ariel Nowersztern

Marcello Basani

Fernando Melean

Hila Cohen Mizrav





CON LA COLABORACIÓN DE

FUENTE DE INNOVACIÓN

Esta publicación se enmarca en Fuente de Innovación, una alianza promovida y cofinanciada por la División de Agua y Saneamiento del Banco Interamericano de Desarrollo (BID) y BID Lab en coordinación con socios claves como el Gobierno de Suiza, a través de la Secretaría de Estado para Asuntos Económicos (SECO), la Fundación FEMSA, el Gobierno de Corea, a través de su Ministerio de Ambiente, y el Gobierno de Israel.

Códigos JEL:

H12, K24, L95, M15, N56, O32, O33, Q25.

Palabras clave:

agua, saneamiento, aguas residuales, tratamiento de aguas, infraestructura crítica, tecnología operativa, sistemas de control industrial, industria 4.0, ciberseguridad, políticas cibernéticas, ciberespacio, ciberataques, amenazas cibernéticas, respuesta a incidentes, planificación estratégica, protección de datos.

Copyright © 2023 Banco Interamericano de Desarrollo (BID). Esta obra se encuentra sujeta a una licencia Creative Commons CC BY 3.0 IGO (<https://creativecommons.org/licenses/by/3.0/igo/legalcode>). Se deberá cumplir los términos y condiciones señalados en el enlace URL y otorgar el respectivo reconocimiento al BID.

En alcance a la sección 8 de la licencia indicada, cualquier mediación relacionada con disputas que surjan bajo esta licencia será llevada a cabo de conformidad con el Reglamento de Mediación de la OMPI. Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la Comisión de las Naciones Unidas para el Derecho Mercantil (CNUDMI). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones que forman parte integral de esta licencia.

Las opiniones expresadas en esta obra son exclusivamente de los autores y no necesariamente reflejan el punto de vista del BID, de su Directorio Ejecutivo ni de los países que representa.



Índice



Índice de cuadros y gráficos

Página 8



Agradecimientos

Página 9



Listado de siglas

Página 10



Prefacio

Página 11



Resumen ejecutivo

Página 14

1

Introducción



Marco conceptual • Página 17

¿Qué son las amenazas cibernéticas? • Página 17

¿Qué es un ataque cibernético o ciberataque? • Página 18

Definición de las infraestructuras críticas • Página 19

El surgimiento de los sistemas de tecnología de operación • Página 20

Relación entre la TO, los SCI y los sistemas SCADA • Página 21

La importancia de proteger los SCI • Página 22

Tipos de ataques cibernéticos • Página 23

Agentes de amenaza • Página 24

2

Protección del sector de agua y saneamiento en la era cibernética



La importancia de proteger las infraestructuras críticas • Página 27

Predicciones sobre ciberseguridad de IC como premisas para la planificación estratégica • Página 27

Interdependencias y seguridad de las infraestructuras • Página 28

Ejemplos de interdependencias entre infraestructuras • Página 29

Interdependencias del agua y aguas residuales • Página 30

- ➔ **Ciberseguridad en el sector de agua y saneamiento** • Página 31
 - Industria 4.0 y la paradoja de la hiperconectividad • Página 31
 - ¿Por qué la industria 4.0 es importante para el sector de AyS? • Página 32
 - Impacto de los ataques cibernéticos en la infraestructura del sector de AyS • Página 34
 - La tríada de confidencialidad, integridad y disponibilidad para la seguridad de los datos • Página 34
 - Elementos clave para mejorar la situación del sector en materia de ciberseguridad • Página 35
 - Daños potenciales y su impacto en la infraestructura del sector de AyS • Página 38
-

3 Preparación del sector de agua y saneamiento en América Latina y el Caribe

- ➔ **Ciberseguridad regional en ALC** • Página 41
 - Tendencias regionales • Página 41
 - Protección de las IC en la región • Página 42
 - ¿Por qué ALC es más vulnerable a los ataques cibernéticos? • Página 46
 - ¿Por qué las empresas prestadoras de servicios de suministro de agua en ALC no son blanco de más ataques cibernéticos? • Página 47
 - Cooperación regional en ciberseguridad • Página 47
 - Falta de incentivos • Página 48
 - Entrevistas: metodología y perspectivas • Página 50
 - Ciberseguridad en el sector de agua y el saneamiento en ALC • Página 51
 - Descripción del estado de la ciberseguridad en cinco países • Página 53
 - Argentina • Página 53
 - Brasil • Página 54
 - Chile • Página 54
 - Colombia • Página 54
 - República Dominicana • Página 54

4 Desafíos y respuestas a nivel internacional

→ **Entendimiento de la importancia de las APP** • Página 56

→ **Estudios de casos internacionales** • Página 57

Estudio de caso No. 1: el modelo israelí • Página 57

Estudio de caso No. 2: el modelo británico • Página 59

5 Recomendaciones clave para el sector de agua y saneamiento en América Latina y el Caribe

→ **Recomendaciones clave de ciberseguridad** • Página 62

→ **Cuestionario de autoevaluación para analizar el escenario de ciberseguridad de una infraestructura** • Página 67

→ **Referencias**

Página 68

→ **Anexo A. Cuestionario para entrevistar al personal de empresas prestadoras de servicios públicos**

Página 76

→ **Anexo B. Cuestionario para entrevistar al personal de entidades reguladoras y agencias federales**

Página 78

Índice de cuadros y gráficos

Cuadro 1: Lista de agentes de amenaza • Página 24

Cuadro 2: Importancia de la industria 4.0 para el sector de AyS • Página 32

Cuadro 3: Posibles escenarios de daños • Página 39

Cuadro 4: Madurez del país según el CMM con respecto a la protección de las IC en ALC • Página 44

Gráfico 1: Relación entre TO, SCI y sistemas SCADA • Página 21

Gráfico 2: Tipos de ataques cibernéticos • Página 23

Gráfico 3: Modelo de interdependencias de infraestructuras • Página 29

Gráfico 4: Dependencias de la infraestructura • Página 30

Gráfico 5: Etapas del tratamiento del agua • Página 33

Gráfico 6: Cinco etapas de madurez • Página 43

Gráfico 7: Cronología de políticas en materia de ciberseguridad en la región de ALC, 1999-2019 • Página 49

Gráfico 8: Prioridades de la Estrategia de Ciberseguridad de Belice 2020-2030 • Página 50

Gráfico 9: Estrategia Nacional de Ciberseguridad del Reino Unido • Página 60

Agradecimientos

Esta publicación se enmarca en Fuente de Innovación, una alianza promovida y cofinanciada por la División de Agua y Saneamiento (INE/WSA) del Banco Interamericano de Desarrollo (BID) y BID Lab en coordinación con socios claves, como el Gobierno de Suiza, a través de la Secretaría de Estado para Asuntos Económicos (SECO), la Fundación FEMSA, el Gobierno de Corea, a través de su Ministerio de Ambiente, y el Gobierno de Israel. En colaboración con esta alianza, el estudio también fue codesarrollado con la ayuda del equipo de ciberseguridad de la División de Innovación para Servir al Ciudadano (IFD/ICS) del BID.

El producto de conocimiento generado busca mostrar a los lectores las tendencias, desafíos y oportunidades en ciberseguridad dentro del sector de agua y saneamiento de América Latina y el Caribe (ALC), evaluando la preparación en seguridad informática de las infraestructuras de agua y aguas residuales de ALC y presentando recomendaciones clave para los actores del sector público y privado que buscan aumentar la resiliencia cibernética general de su organización.

Los autores desean agradecer a todas las personas que participaron en la revisión y enriquecimiento de este documento, en particular a María Donoso, James Pichardo e Iván Rodríguez. También se hace un reconocimiento especial a Ricardo Poppi, Kim Olson y Clara Sarcone por sus contribuciones y su encomiable trabajo en la corrección y edición del texto. Por último, pero no por ello menos importante, el BID también quisiera agradecer a todas aquellas organizaciones y profesionales que amablemente participaron en nuestras entrevistas y consultas, proporcionando información valiosa necesaria para la terminación de esta publicación.

Listado de siglas

ALC: América Latina y el Caribe

APP: Asociaciones público-privadas

APT: Amenaza avanzada persistente (siglas en inglés)

AyS: Agua y saneamiento

BID: Banco Interamericano de Desarrollo

CERT.br: Equipo de respuesta a emergencias informáticas de Brasil (siglas en inglés)

CID: Confidencialidad, integridad y disponibilidad

CLP: Controlador lógico programable

CMM: Modelo de madurez de capacidades de ciberseguridad de las naciones (siglas en inglés)

CSO: Desbordamientos combinados del alcantarillado (siglas en inglés)

IC: Infraestructura crítica

IESUE: Instituto de Estudios de Seguridad de la Unión Europea

IIoT: Internet industrial de las cosas (siglas en inglés)

IoT: Internet de las cosas (siglas en inglés)

NCSC: Centro Nacional de Ciberseguridad del Reino Unido (siglas en inglés)

NCSS: Estrategia Nacional de Ciberseguridad (siglas en inglés)

NIST: Instituto Nacional de Estándares y Tecnología de los Estados Unidos (siglas en inglés)

OEA: Organización de Estados Americanos

SCADA: Control de supervisión y adquisición de datos (sigla en inglés)

SCF: Sistemas ciberfísicos

SCI: Sistemas de control industrial

SSO: Desbordamientos sanitarios del alcantarillado (siglas en inglés)

TI: Tecnología de la información

TIC: Tecnologías de la información y las comunicaciones

TO: Tecnología de operación

Prefacio

La digitalización es un elemento fundamental para la gobernanza del siglo XXI, dado que contribuye a que los Estados mejoren la calidad y cobertura de los servicios públicos que proporcionan, e incrementen la integridad de sus actividades en favor de la sociedad.

Si bien la pandemia del COVID-19 ha sido un reciente acelerador de la digitalización, tanto el sector público como el privado iniciaron el siglo XXI con esfuerzos de inversión importantes en infraestructura tecnológica, sistemas digitales y talento humano con el objetivo de mejorar su gestión y sus servicios. Los ciudadanos han podido contar con acceso fácil y eficiente a más servicios e información, a través de canales novedosos de comunicación con los gobiernos y las empresas.

Conscientes de que la digitalización es una herramienta que impulsa la eficiencia, agilidad y transparencia en el funcionamiento del sector público, y que contribuye a mejorar la calidad de vida de la población de América Latina y el Caribe (ALC), desde el Banco Interamericano de Desarrollo (BID) promovemos la implementación de tecnologías digitales en los países de la región.

Junto con las oportunidades descritas, el proceso de digitalización trae consigo complejidades y desafíos. A medida que aumenta la digitalización de las infraestructuras y los servicios urbanos, se incrementa también su exposición a los riesgos y vulnerabilidades inherentes al ciberespacio, lo que abre la puerta a actores maliciosos y ciberataques que buscan damnificar áreas críticas, como los sectores de agua y saneamiento (AyS) (Guillaume, 2022), salud, energía y transporte, entre muchos otros.

En el ámbito de las infraestructuras críticas, los sistemas digitalizados en el sector de AyS se consideran unos de los más sensibles (IWA, 2022), debido a su intrínseca relación con la salud de la población y los controles de higiene, ya que este sector engloba responsabilidades como la producción y suministro continuo de agua potable para los ciudadanos y la recolección, transporte y tratamiento de aguas residuales, entre otros procesos fundamentales para las condiciones de salubridad de áreas residenciales y públicas. Teniendo en cuenta la criticidad de estas operaciones, no sorprende que un reporte de la American Water Works Association haya considerado el riesgo cibernético como la amenaza número uno que enfrenta el sector de AyS (Germano, 2019).

Un ataque cibernético dirigido a dependencias del sector de AyS tiene la capacidad de entorpecer o hasta interrumpir las operaciones de ciudades completas, lo que puede producir daños significativos y, en determinados casos, irreparables o catastróficos a los sistemas de tecnología estatales. Esto puede dejar a la población sin suministro de agua por periodos de varias horas o hasta días, y aumentar el riesgo de contraer enfermedades asociadas a la ingesta de agua no tratada o contaminada, todo lo cual pone en peligro la vida de las personas.

Al mismo tiempo, ciertas prácticas tradicionales de las infraestructuras digitalizadas, como el monitoreo, recolección de datos y creación de registros extensos, pueden ser explotadas por ciberdelincuentes que busquen hacerse con la información confidencial de dichas instalaciones de tratamiento de agua para fines ilícitos, divulgar datos de clientes y proveedores, encontrar puntos vulnerables en la gestión de la empresa o el Estado, quebrantar la cadena de suministro o incluso vender la información a competidores en el mercado negro. Los motivos por los cuales la infraestructura en AyS se enfrenta a este tipo de amenazas a diario son tan variados como los métodos de ataque empleados por los ciberdelincuentes. Intereses personales, políticos, económicos, entre otros, impulsan a los criminales a desarrollar nuevas herramientas y métodos para estudiar los sistemas y hallar vulnerabilidades que les permitan aumentar la frecuencia y sofisticación de estos incidentes.

Para enfrentar estas amenazas, es responsabilidad de las administraciones planificar e invertir de forma proactiva a fin de garantizar que los ciberataques no causen interrupciones en su gestión y pongan en peligro a la población. La inversión en ciberseguridad es el mecanismo fundamental para cumplir con el objetivo de defender y respaldar la digitalización de las infraestructuras críticas para la salud de sus usuarios y los servicios digitales de los que disponen.

Esta publicación tiene como objetivo ofrecer una visión general de la protección cibernética que los países de la región implementan en las entidades destinadas a la recolección, tratamiento y distribución de agua que operan dentro de su territorio nacional. Se ofrece información recopilada de diversas fuentes, expertos y publicaciones, a partir de la cual se presenta un análisis integral del nivel de preparación del sector, con énfasis en la importancia de la protección de estas infraestructuras críticas dentro del entorno de la cuarta revolución industrial (Stankovic, Hasanbeigi y Neftenov, 2020).

A partir de la presentación de argumentos, como el costo del cibercrimen, las tendencias de la región, los principales incentivos y retos a nivel internacional, entre otros, se aprovecha la experiencia de países con políticas de ciberseguridad reconocidas, como Israel y Reino Unido, para exponer casos de estudio que detallan los resultados de una gestión sólida y comprometida con la seguridad de la información en el sector. Sobre la base del análisis de todas estas experiencias y recomendaciones, esta publicación se plantea como una herramienta para promover el conocimiento y las acciones de ciberdefensa claves para asegurar el futuro del sector de AyS.

Desde el BID, somos muy conscientes de estos desafíos y, por ese motivo, trabajamos estrechamente con los proveedores de AyS y los gobiernos de la región para apoyar una digitalización segura que fortalezca sus capacidades de ciberseguridad. La puesta en práctica de políticas integrales de ciberseguridad permitirá disfrutar de los beneficios de la cuarta revolución industrial a la vez que se garantiza el bienestar de la población. Los invitamos a unirse a nosotros en este esfuerzo.



Roberto de Michele

Jefe de División de Innovación para Servir al Ciudadano
Sector de Instituciones para el Desarrollo
Banco Interamericano de Desarrollo



Sergio Campos

Jefe de División de Agua y Saneamiento
Sector de Infraestructura y Energía
Banco Interamericano de Desarrollo

Resumen ejecutivo

El sector de agua y saneamiento es esencial para el sustento y, por lo tanto, la mayoría de los países reconocen que se trata de una infraestructura crítica (OMS, 2019). Aunque la creciente tendencia a la automatización y digitalización de las instalaciones del sector de AyS mejora la eficiencia y ayuda a reducir los costos operativos, también expone las instalaciones y operaciones del sector a riesgos cibernéticos cada vez mayores. El número y variedad de amenazas cibernéticas y agentes maliciosos que atacan a las empresas de servicios públicos aumentan rápidamente: desde agentes de estados nacionales que desean provocar el caos político y social e interferir en las economías, delincuentes cibernéticos en busca de beneficios pecuniarios y *hacktivistas* motivados por agendas ideológicas o personales hasta personas de las propias empresas que están descontentas y particulares que intentan obtener una reducción en sus facturas.

A medida que las tecnologías digitales se expanden y añaden mayor valor a las infraestructuras del sector de AyS, los delincuentes cibernéticos intentan aprovecharse de la infraestructura interconectada y atacan los sistemas de control industrial (SCI), las computadoras especializadas que gestionan las operaciones de control de caudal, el tratamiento de aguas residuales y otros sistemas. Los ataques cibernéticos aumentan en frecuencia, volumen y sofisticación. Sin embargo, la escasa concientización y reticencia a invertir en ciberseguridad debido a sus costos, junto con la falta de atención y de requisitos normativos, hacen que las empresas de servicios públicos no inviertan lo suficiente en ciberseguridad, con el consecuente aumento de su vulnerabilidad a sufrir ataques cibernéticos, lo que puede generar terribles consecuencias.

Las empresas prestadoras de servicios de suministro de agua de todo el mundo ya enfrentaron una amplia gama de ataques, desde el secuestro de datos (*ransomware*) y la interferencia en los SCI hasta la manipulación de la operación de válvulas y caudales, la alteración de las fórmulas de tratamientos químicos, además de otros intentos por dañar potencialmente la maquinaria e interferir en las operaciones. Entrevistas realizadas durante la preparación de esta publicación revelaron que algunas entidades de América Latina y el Caribe ya sufrieron un ataque cibernético que afectó sus operaciones, aunque la recuperación se logró rápidamente. No obstante, la propia capacidad de una entidad para clasificar un evento operativo como incidente cibernético depende en gran medida de su infraestructura digital, sus capacidades forenses y su conciencia cibernética.

Los ataques cibernéticos dirigidos contra los sistemas del sector de AyS podrían poner en peligro el suministro de agua potable, la calidad del agua o la recolección y tratamiento de aguas residuales al interferir en la continuidad y confiabilidad de las actividades o procesos. Tales ataques también podrían manipular la información sobre el consumo, interferir en la facturación y poner en riesgo los datos de los clientes. Los ataques cibernéticos a entidades responsables por la gestión del agua o aguas residuales pueden tener efectos devastadores para la salud pública, el medioambiente y la economía. Además, los ataques cibernéticos que provocan contaminación, mal funcionamiento operativo o interrupciones del servicio pueden acabar desgastando la confianza de los clientes e incluso derivar en responsabilidades financieras y legales.

Esta publicación es la primera de su tipo que el Banco Interamericano de Desarrollo presenta para analizar un motivo de creciente preocupación: las amenazas cibernéticas en el sector de AyS de ALC. En 2020 el BID y la Organización de Estados Americanos (OEA) realizaron estudios de amplio alcance para evaluar la madurez cibernética de cada país de ALC, en los que utilizaron el modelo de madurez de capacidades de ciberseguridad de las naciones (CMM, por sus siglas en inglés). Además, el BID publica guías de ciberseguridad de interés general y guías de mejores prácticas en materia de ciberseguridad para otros sectores críticos, como el de energía, salud y ciudades inteligentes. Esta publicación se suma a la información más actualizada que el BID pone a disposición del público sobre el sector de AyS de ALC y aborda temas de amplio alcance, entre ellos, la transformación digital del sector.

En esta publicación se analizan las tecnologías del sector de AyS y se explican las amenazas cibernéticas a las que se enfrenta la tecnología de la infraestructura de este sector. Además, se evalúa la preparación del sector de AyS de ALC en materia de ciberseguridad a través de documentos y entrevistas con representantes clave de instituciones del ámbito público y otras empresas prestadoras de servicios de suministro de agua en ALC. Asimismo, se presenta una serie de recomendaciones para los responsables tanto del sector público como del privado. Finalmente, se incluye un cuestionario gratuito de autoevaluación en línea que permite que las organizaciones evalúen su situación actual en materia de ciberseguridad e identifiquen las brechas existentes, y que además contiene recomendaciones.

Una ciberseguridad eficaz en el sector de AyS requiere no solo la aplicación de medidas técnicas e implementación de metodologías de protección, sino también la priorización e integración de la ciberseguridad en la gestión y cultura corporativas. Esto reforzaría la ciberseguridad del sector y permitiría la prestación segura e ininterrumpida de servicios esenciales de agua y saneamiento a la población de ALC.



Introducción



Marco conceptual

¿Qué son las amenazas cibernéticas?

En los últimos años, como consecuencia del rápido y continuo desarrollo de la tecnología, de la cual las personas son cada vez más dependientes, surge una amenaza creciente sobre todos los ámbitos de la vida: la amenaza cibernética o cibamenaza. En la actualidad, los sistemas de tecnología de la información (TI) controlan y dan apoyo a muchos procesos críticos para el bienestar de las personas. Entre los ejemplos, se pueden mencionar los sistemas de agua y electricidad, telecomunicaciones y servicios de transporte. Esta nueva amenaza desafía a los gobiernos, empresas, organizaciones y ciudadanos de todo el mundo.

Estos procesos y la amenaza creciente se desarrollan en un ámbito conocido como ciberespacio. El Centro de Investigación de Seguridad Informática (CSRC, por sus siglas en inglés) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos describe al ciberespacio como la red interdependiente de infraestructuras de TI, entre las que se encuentran Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados en industrias críticas (CSRC, 2022a).

¿Qué es un ataque cibernético o ciberataque?

El CSRC (2022b) define el ciberataque como un ataque a través del ciberespacio, cuyo objetivo es el uso del ciberespacio por parte de una empresa con el fin de interferir, inutilizar, destruir o controlar maliciosamente un entorno o infraestructura informática, destruir la integridad de los datos o robar información controlada.

Algunos ataques cibernéticos se llevan a cabo aprovechando las vulnerabilidades de las plataformas tecnológicas. Una vulnerabilidad de ciberseguridad es una debilidad tecnológica o un comportamiento involuntario en un sistema informático que permite que posibles atacantes accedan a él o realicen acciones que no tienen permitidas. Las vulnerabilidades posibilitan el ingreso no autorizado a diferentes niveles de un sistema de información y, como resultado, los atacantes pueden utilizar tal acceso para realizar una serie de acciones en función de sus objetivos e intenciones. Existe una distinción entre las vulnerabilidades conocidas, que son aquellas que han sido expuestas y para las que los desarrolladores de *software* ya publicaron una actualización de seguridad que impide que sean utilizadas, y las vulnerabilidades de “día cero”, las cuales han sido expuestas por los investigadores pero carecen de una actualización de seguridad que impida su uso. En el caso de estas últimas, los desarrolladores de *software* disponen de prácticamente cero días para desarrollar una actualización de seguridad antes de que la vulnerabilidad pueda ser utilizada con fines maliciosos (Ablon y Bogart, 2017).



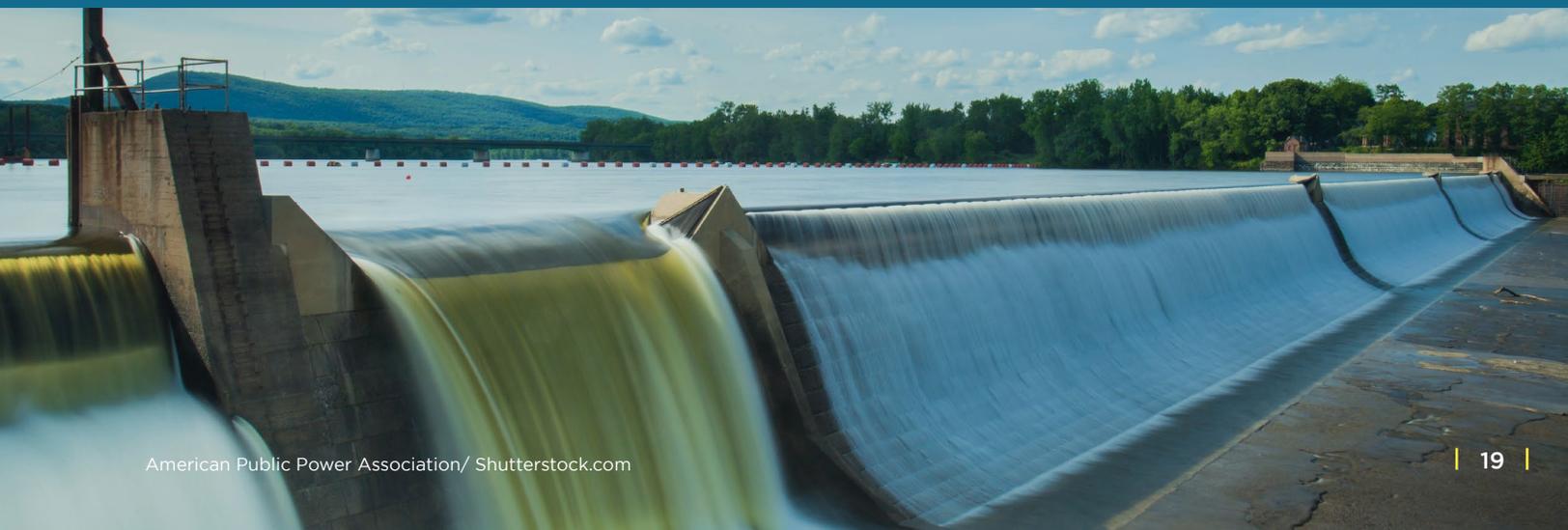


Definición de las infraestructuras críticas

A escala nacional, una infraestructura se califica como crítica cuando se considera que su falla provocará una crisis socioeconómica considerable, que podría desestabilizar a la sociedad y acarrear ramificaciones políticas, estratégicas o de seguridad. Los distintos países definen las infraestructuras críticas (IC) de manera diferente, sin embargo, en el contexto de la ciberseguridad todos coinciden en que se trata de una infraestructura con una dimensión informática de la que dependen otros sistemas físicos y cuya falla de funcionamiento puede dañar significativamente la esfera física (Tabansky, 2011). En el caso de la infraestructura del sector de AyS, esos daños pueden traspasar el sistema sociopolítico y afectar las estructuras físicas reales (represas, sistemas de distribución, etc.) y el medioambiente.

En algunos países la definición de IC se basa en la designación formal de la infraestructura, mientras que en otros se consideran las consecuencias sociales de los daños que esta pueda sufrir. Por ejemplo, la Unión Europea (UE) define las IC como sistemas necesarios para la seguridad nacional y transfronteriza de servicios esenciales pertenecientes a sectores como las tecnologías de la información y las comunicaciones (TIC), energía, finanzas, sanidad y transporte (ENISA, 2023). En los Estados Unidos la IC se refiere a sistemas, activos o redes (físicos o virtuales) de importancia fundamental, por lo cual su destrucción tendría graves consecuencias para la seguridad nacional en general y económica en particular, así como para la salud pública (CISA, 2023). Dado que los países definen las IC de manera diferente, los sectores en los que pueden encontrarse también varían. Según la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) de los Estados Unidos, los sistemas de IC se encuentran, entre otros, en los sectores energéticos, agroalimentario, de las comunicaciones, de sistemas de transporte y de sistemas de suministro de agua y tratamiento de aguas residuales (CISA, 2022).

Muchos sistemas de IC se gestionan y operan mediante sistemas digitales de control y supervisión, conocidos como sistemas de control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés), que median entre el mundo físico y el ciberespacio a través de controladores lógicos programables (CLP). En algunos casos, los sistemas SCADA permiten el acceso remoto. En cuanto a los sistemas de suministro de agua, a menudo es posible controlar a distancia el funcionamiento y detención de las bombas que extraen agua de los embalses en función de las necesidades y cantidad de agua en dicha estructura, además de controlar el caudal de agua en las represas y, si es necesario, su cierre (Stouffer et al., 2015).



El surgimiento de los sistemas de tecnología de operación

Se utiliza el término tecnología de operación (TO) para designar el *hardware* y *software* utilizados en los sistemas de control de automatización dentro de la infraestructura (Murray, Johnstone y Valli, 2017). Los sistemas de TO se emplean en todo el mundo para controlar y supervisar procesos industriales en infraestructura y servicios públicos críticos, como centrales eléctricas, centrales nucleares e infraestructuras de agua y alcantarillado.

En la última década, el surgimiento de Internet industrial de las cosas (IIoT, por sus siglas en inglés) resultó en la convergencia de la TI y la TO. Las industrias conectaron los sistemas de TI y TO en un esfuerzo por mejorar la funcionalidad de las infraestructuras y, de ese modo, eliminaron las llamadas brechas de aire que habían protegido sus sistemas de TO de los *hackers* y *software* malicioso (*malware*) procedente de Internet. Debido a la eliminación de las brechas de aire, los agentes hostiles aumentaron sus esfuerzos de piratería contra los sistemas de TO para obtener datos, interferir en las operaciones o lanzar ataques cibernéticos terroristas contra IC (Siboni, Cohen y Rotbart, 2013). Estos riesgos aumentan con el creciente número de dispositivos conectados, muchos de los cuales no están protegidos por sus fabricantes o usuarios. También se observa un incremento de los ataques de interferencia del servicio en sistemas públicos y privados, junto con los casos de extorsión y de pedidos de rescate (Siboni, Cohen y Rotbart, 2013). El *malware* existente es eficaz contra los sistemas obsoletos instalados en las redes de TO que carecen de controles de ciberseguridad y de protección cibernética adicional, como la protección de ciberseguridad de punto final (*software* antivirus) (Stouffer et al., 2015).

Los ataques contra los sistemas que controlan y supervisan las infraestructuras civiles críticas ocupan un lugar destacado en la escala de gravedad de los ataques cibernéticos. Entre los más graves se encuentran los ataques que ponen en peligro la vida de civiles, incluida la contaminación del agua o daños ambientales causados por el vertido de aguas residuales o productos químicos, también conocidos como desbordamientos del alcantarillado sanitario (SSO, por sus siglas en inglés). Asimismo, en años recientes se observa un aumento significativo de ataques cibernéticos contra IC por parte de diversos agentes, entre ellos, estados nacionales, terroristas, anarquistas, entidades comerciales competidoras, delincuentes y personas de las propias organizaciones que actúan maliciosa o inadvertidamente, entre otros (Bigelow y Lutkevich, 2021). Los ataques a organizaciones en sectores de IC aumentaron drásticamente, ya que pasaron de menos de 10 en 2013 a casi 400 en 2020, valor que representa un crecimiento del 3.900% (Thielemann et al., 2021).

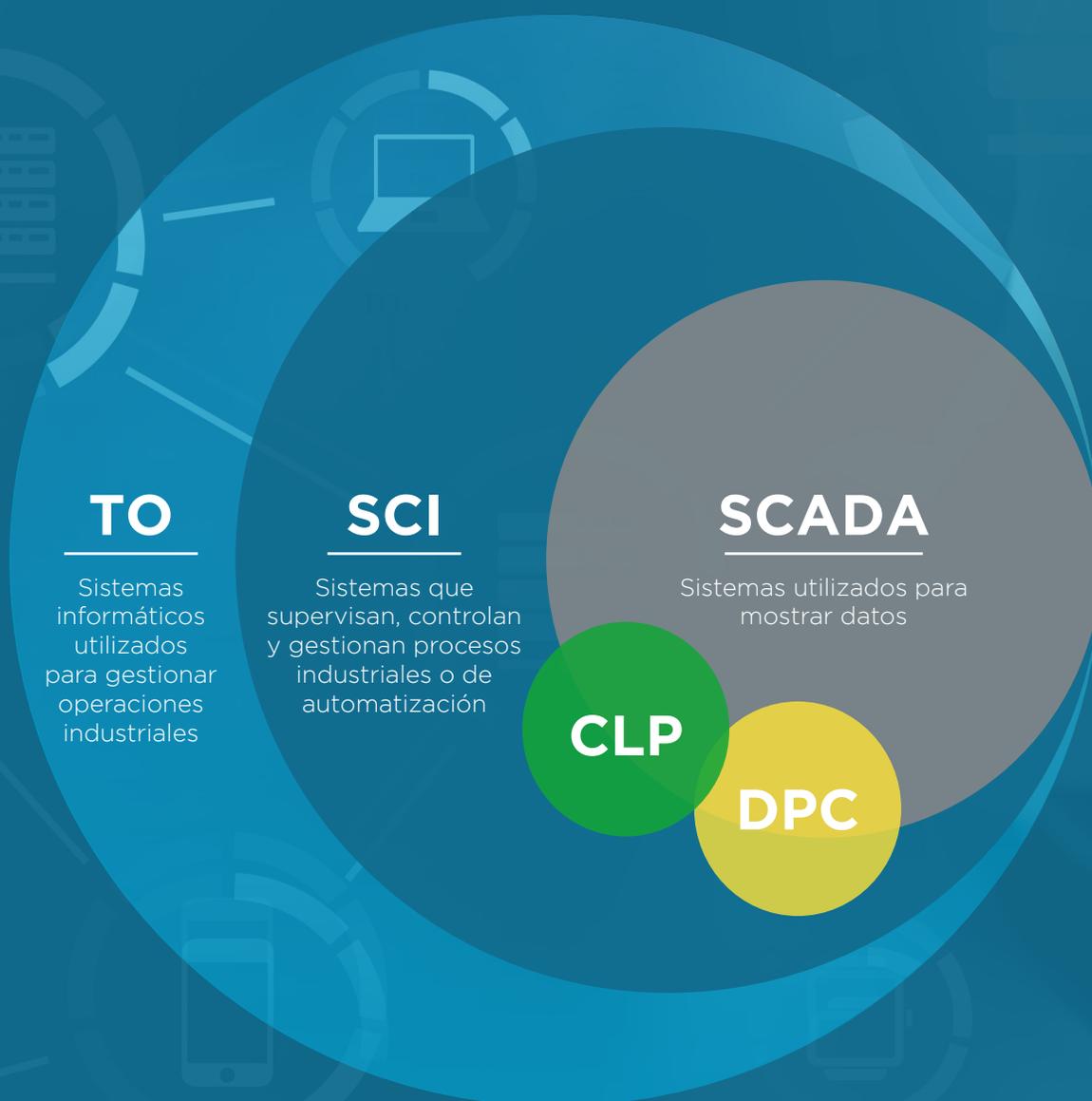
En general, muchas organizaciones consideran que la TO está a salvo de los ataques cibernéticos porque se ocupa de las máquinas y del mundo físico. Las organizaciones se esfuerzan enormemente por fortalecer su perímetro, pero no presupuestan ni invierten lo suficiente en seguridad interna, específicamente, en la seguridad de los sistemas de TO. Estas discrepancias en la inversión dejan a la TO menos vigilada y susceptible a ataques. Una vez que los atacantes consiguen acceder a los sistemas de una organización, pueden desplazarse y operar fácilmente dentro de ellos. En 2017 los ataques cibernéticos de NotPetya y WannaCry demostraron en la práctica que trabajar siguiendo ese modelo tradicional ya no es suficiente (Bigelow y Lutkevich, 2021).



Relación entre la TO, los SCI y los sistemas SCADA

Es importante diferenciar entre las funciones de la TO, los SCI y los sistemas SCADA. La TO hace referencia a los sistemas informáticos utilizados para gestionar las operaciones industriales. Los sistemas SCADA se utilizan para visualizar datos, mientras que los SCI —los sistemas que supervisan, controlan y gestionan los procesos industriales o de automatización— forman el nivel intermedio entre los dos anteriores. La mayoría de los SCI se consideran sistemas de control de procesos continuos gestionados por CLP o sistemas de control de procesos en tiempo discreto (DPC, por sus siglas en inglés) que podrían utilizar un CLP o algún otro dispositivo de control de procesos por lotes. Básicamente, la TO indica al sistema qué debe hacer, el SCI verifica el resultado de los sistemas (cómo lo hizo) y el sistema SCADA procesa los datos recolectados por el SCI y los pone a disposición de los usuarios (Williamson, 2015). El Gráfico 1 ilustra este proceso.

Gráfico 1: Relación entre TO, SCI y sistemas SCADA



Fuente: Williamson (2015).



La importancia de proteger los SCI

Los SCI son esenciales para las organizaciones industriales, ya que ayudan a mantener la eficiencia, evalúan los datos para que se puedan tomar decisiones informadas e identifican fallas en los sistemas que permiten garantizar la calidad y reducir el tiempo de inactividad (Stouffer et al., 2015). Los SCI pueden encontrarse en todas las instalaciones operativas y en una diversidad de otras entidades, sin embargo, a pesar de su ubicuidad, muchos siguen siendo vulnerables a los ataques cibernéticos.

Muchos de los protocolos de comunicación utilizados en los SCI suman décadas de antigüedad y no se diseñaron para hacer frente a los riesgos cibernéticos actuales. Algunos dispositivos, protocolos y programas de los SCI, por ejemplo, pueden modificarse sin autenticar el usuario y algunos están expuestos a Internet. Además, si bien por cuestiones de confiabilidad los SCI se diseñaron para ser totalmente independientes de cualquier otro sistema, cuestiones relacionadas con los costos y la eficiencia obligan a los operadores a conectar los SCI a las redes industriales e, incluso, a Internet, aunque no hayan sido pensados para ese entorno. Al hacerlo, aumenta el riesgo de un ataque cibernético, ya que quedan expuestos al mundo exterior sin la seguridad adecuada (Stouffer et al., 2015).

Según el informe bianual sobre riesgos y puntos débiles publicado por una empresa de ciberseguridad que trabaja en el ámbito de los SCI, la concientización en el área de la seguridad de los SCI aumentó después de ataques cibernéticos de gran repercusión en IC y plantas industriales. Como consecuencia, junto con el aumento de la concientización pública y gubernamental sobre la seguridad de los SCI, hubo un crecimiento drástico en la detección de vulnerabilidades de seguridad en los mismos. De las 637 vulnerabilidades de SCI que afectan a 76 proveedores, publicadas por Claroty en la primera mitad de 2021, el 65% tiene una alta probabilidad de causar una pérdida total de disponibilidad del sistema (Claroty Team82, 2021).

Stouffer et al. (2015) informan que las dos dinámicas de ataque más comunes contra los sistemas de los SCI son:



1. Ataques que buscan detener una función operativa y causar daños inmediatos.



2. Ataques lentos y sigilosos que se basan en cambios lógicos en los sistemas de control o en un profundo conocimiento del proceso para manipularlo deliberadamente.

Tipos de ataques cibernéticos

En el ciberespacio el factor humano es responsable de la mayoría de las fallas y disfunciones. En 2017 aproximadamente el 52% de los propietarios de empresas estadounidenses reconocieron el riesgo de un ciberataque debido al factor humano, resultado de la acción u omisión por parte de los empleados de una organización (Kaspersky, 2017b). En el Gráfico 2 se describen brevemente varios tipos de ataques cibernéticos.

Gráfico 2: Tipos de ataques cibernéticos

Ataques de intermediario (MitM, por sus siglas en inglés)

Ataques en los que el atacante se sitúa entre las partes legítimas de una transacción. De este modo, puede eludir las protecciones del protocolo (a menudo aplicadas por medios criptográficos) y acceder a datos secretos o corromper la transacción.



Ataques de ransomware

Ataques que niegan el acceso a operaciones o datos críticos de una entidad hasta que se pague un rescate.



Phishing

Ataques de ingeniería social que engañan a las víctimas para que revelen información sensible o permitan el acceso a los sistemas. Estos incluyen el *spear phishing* (envío de correos electrónicos desde lo que parece ser una fuente confiable para inducir a los usuarios a hacer clic, y, de esa manera, instalar alguna forma de *malware* en un sistema informático), y el *whaling* (ataques dirigidos a altos ejecutivos para obtener información sensible de alto nivel).



Ataques de denegación de servicios (DoS, por sus siglas en inglés)

Ataques diseñados para denegar el acceso a servicios críticos aprovechando la vulnerabilidad de una aplicación o inundando un sistema con más datos o pedidos de los que puede gestionar.



Ataques de “días cero”

Ataques que aprovechan vulnerabilidades en el *software* previamente expuestas por investigadores o ciberatacantes pero que carecen de una actualización de seguridad que impida su uso.



Ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés)

Ataques donde se utilizan varias computadoras para enviar muchos pedidos a un servidor y así desbordar su capacidad de funcionamiento.



Fuente: Elaboración propia con base en Check Point Software (s.f.).

Agentes de amenaza

El Centro Canadiense de Seguridad Cibernética (2018) informa que varios agentes de amenaza podrían estar interesados en interferir en el correcto funcionamiento de la infraestructura del sector de AyS por intereses ideológicos, económicos, políticos, personales o de otro tipo (Tabansky, 2011). El Cuadro 1 enumera los principales tipos de agentes de amenaza.

Cuadro 1: Lista de agentes de amenaza



Agentes de estados nacionales

Los estados soberanos atacan numerosos objetivos en el ciberespacio y causan efectos variados, desde la desfiguración de sitios web hasta grandes daños a las infraestructuras. Su objetivo suele ser geopolítico.



Delincuentes cibernéticos (agentes de amenazas con motivación financiera)

El lucro es uno de los motivos más comunes de los delincuentes cibernéticos. Suelen atacar organizaciones poco protegidas, vulnerables a las perturbaciones y con capacidad de pago, o cuyos activos de valor, como datos, propiedad intelectual o fondos, se puedan robar en línea.



Atacantes patrocinados por estados nacionales y grupos de amenazas avanzadas persistentes

Las amenazas avanzadas persistentes (APT, por sus siglas en inglés) constituyen agentes de amenaza con gran capacidad técnica. Algunas APT están patrocinadas por un estado nacional, pero mantienen una negación plausible, ya que no suelen formar parte de un gobierno abiertamente. Las APT persiguen los objetivos estratégicos de los países y pueden utilizar capacidades avanzadas de forma sostenida para atacar a grandes entidades, posiblemente mejor protegidas. Sus objetivos pueden incluir instituciones estatales, IC y empresas que posean activos clave. El objetivo común de estos atacantes es alcanzar una meta estratégica para su patrocinador, en forma de interrupción u obtención de información sensible. Algunos ejemplos recientes son el ciberataque a SolarWinds, que aprovechó las vulnerabilidades de la cadena de suministro de *software*.



Terroristas

Estos agentes están interesados en manifestar su ideología mediante la violencia contra la población civil. En algunas ocasiones, los terroristas utilizan métodos poco sofisticados y recurren a herramientas ampliamente disponibles que requieren poca habilidad técnica para su instalación.



Agentes de amenaza internos

Cualquier empleado, proveedor o contratista actual o anterior de una organización, que tenga acceso legítimo a sus sistemas e instalaciones, puede representar una potencial amenaza cibernética. Estas personas pueden tener profundos conocimientos de los sistemas y controles de seguridad de la organización. Quienes deciden utilizar sus conocimientos contra la organización en la que trabajan suelen hacerlo por venganza (empleados insatisfechos), razones psicológicas, ideológicas o financieras. Suelen querer dañar la reputación de la organización o robar información confidencial, por ejemplo, propiedad intelectual.



Hactivistas

Individuos o grupos, como Anonymous, que utilizan la piratería informática para promover sus objetivos sociales o ideológicos. En la mayoría de los casos, su principal objetivo es concientizar sobre la causa más que causar daños específicos a IC.

Fuente: Elaboración propia a partir de Flashpoint (2021).

En ALC las amenazas más destacadas suelen tener motivaciones financieras, como los ataques de FIN11 y UNC2053 (dos grupos de delincuencia financiera bien establecidos), y con frecuencia adoptan la forma de *ransomware* y ataques de *malware*. Según Mandiant, los anuncios de datos robados a organizaciones de ALC durante incidentes de *ransomware* aumentaron un 550% en solo un año (de 2020 a 2021). Esta actividad afectó a varios países, con mayor frecuencia a Brasil, Colombia y México, e implicó instalaciones industriales, incluidos proveedores de energía y otros servicios públicos (Caparros, 2021).



Protección del sector de agua y saneamiento en la era cibernética



La importancia de proteger las infraestructuras críticas

Como se describió en la sección 1, las IC se definen como tales por el impacto que causa su falla, la cual podría desencadenar una crisis sustancial. Es importante planificar y aplicar estratégicamente las protecciones de las IC teniendo en cuenta una serie de predicciones que se describen con más detalle en esta sección.

Predicciones sobre ciberseguridad de IC como premisas para la planificación estratégica

Aunque es posible que las siguientes predicciones no se apliquen totalmente a ALC, proporcionan un punto de partida general para una planificación estratégica.

Para 2024, un ciberataque dañará las IC, de forma tal que un miembro del Grupo de los Veinte (G20) reaccionará con un ataque físico declarado. Asimismo, el 80% de las organizaciones de IC abandonarán a sus actuales proveedores de soluciones de seguridad aisladas para cerrar la brecha entre los riesgos ciberfísicos y de TI mediante la adopción de soluciones hiperconvergentes (Snow, 2022).

Para 2025, los atacantes habrán utilizado como arma un sistema ciberfísico (SCF) de IC para dañar o matar seres humanos con éxito y de forma deliberada.

Durante 2025, el 30% de las organizaciones de IC enfrentarán una vulneración de seguridad que provocará la interrupción de las operaciones o de un SCF esencial para una misión (Moore, 2021).

Durante 2026, menos del 30% de los propietarios y operadores de IC de los Estados Unidos cumplirá con los requisitos de seguridad de los SCF exigidos por el gobierno (Snow, 2022).

Interdependencias y seguridad de las infraestructuras

El uso cada vez mayor de TI, junto con la creciente dependencia del mercado libre en los productos y servicios proporcionados por las infraestructuras, aumenta la prevalencia de la interdependencia de las infraestructuras y la importancia del fenómeno por el que los daños causados a un sistema de infraestructuras afectan a otro. La interrupción del sistema de una infraestructura puede tener un impacto significativo en la capacidad de funcionamiento de otras infraestructuras y, en muchos casos, puede provocar el colapso de otras infraestructuras conectadas a la infraestructura afectada (Menashri y Baram, 2015). Por este motivo, a menudo al definir la IC de los Estados Unidos se afirma que se trata de un sistema de sistemas (Stouffer et al., 2015).

La capacidad de identificar y analizar las interdependencias es claramente un aspecto importante de la protección de las IC. Aunque las interdependencias son una característica común de los sistemas de IC y muchas veces se materializan mediante conexiones digitales a través de las TIC, la mayoría están determinadas regionalmente, es decir, están estrechamente relacionadas con la proximidad geográfica y las redes regionales integradas. Esto es especialmente cierto, por ejemplo, en la región del mar Báltico y, sobre todo, en los países nórdicos, donde las IC de muchos sectores forman parte del mismo sistema nórdico de infraestructuras (Pursiainen et al., 2007).

Los agentes que participan en la ciberprotección de la infraestructura deben estudiar y examinar las conexiones y dependencias entre las distintas infraestructuras, crear redundancias y diseñar sistemas que sean resilientes a los efectos dominó que afectan a otras infraestructuras muy dependientes en caso de pérdida o daño de una de ellas (Menashri y Baram, 2015). A la hora de evaluar la vulnerabilidad, establecer planes de respuesta y recuperación y gestionar otras cuestiones de seguridad y protección, los sistemas de suministro de agua y tratamiento de aguas residuales presentan distintas interdependencias con otras infraestructuras que deben tenerse en cuenta (Gillette et al., 2002).



Ejemplos de interdependencias entre infraestructuras

Según un modelo sugerido por Rinaldi en un estudio realizado con otros investigadores (Rinaldi, Peerenboom y Kelly, 2001), se pueden identificar cuatro tipos de interdependencias:

Interdependencia física: cuando un sistema depende del resultado físico de otro u otros sistemas.

Interdependencia geográfica: cuando uno o varios sistemas pueden verse afectados por un cambio en el entorno cercano.

Interdependencia cibernética: cuando los sistemas se comunican a través del ciberespacio.

Interdependencia lógica: cuando los sistemas dependen unos de otros en cualquier otra forma de interdependencia, no especificada anteriormente.

El Gráfico 3 muestra una representación de las interdependencias descritas anteriormente.

Gráfico 3: Modelo de interdependencias de infraestructuras



Fuente: Rinaldi, Peerenboom y Kelly (2001).





Interdependencias del agua y aguas residuales

Al estudiar las vulnerabilidades cibernéticas y diseñar su protección de ciberseguridad, debe examinarse la interdependencia específica de las infraestructuras de aguas residuales y de agua, ya que estas se vinculan a los principales proveedores de agua limpia de un país o región (Gillette et al., 2002). Como ejemplo, se puede considerar el terremoto de Cinchona en Costa Rica (2009), que causó fuertes deslizamientos de tierra y flujos de lodo que provocaron daños en los sistemas de agua y alcantarillado, los cuales tuvieron importantes repercusiones en la disponibilidad de agua potable. Este ejemplo muestra cómo los desastres naturales pueden influir en las instalaciones de aguas residuales y, en consecuencia, afectar la disponibilidad de agua limpia (Deubelli, 2019). El Gráfico 4 ilustra las dependencias de las infraestructuras, incluidas sus dependencias con otros tipos de infraestructuras (transporte, gas, etcétera).

Gráfico 4: Dependencias de la infraestructura



Notas: H₂O: sector de AyS; EE: energía eléctrica; GN: gas natural; LP: líquidos derivados del petróleo; TRANS: transporte; TC: telecomunicaciones.

Fuente: Gillette et al. (2002).



En las entrevistas realizadas para la elaboración de esta publicación, se identificó que en la mayoría de los países, incluidos los de ALC, las infraestructuras de agua y aguas residuales son antiguas y no tan eficientes como podrían ser. Por lo tanto, el sector debe pasar por una transformación digital para ampliar el acceso al agua potable y garantizar su continuidad. La digitalización está mejorando las operaciones de las empresas de servicios públicos mediante el aumento de su eficiencia, mejora de los servicios y actualización de sus tecnologías. Además de ampliar la cobertura de servicios a más personas, la digitalización tiene beneficios financieros: las empresas que tienen una mayor madurez digital registran un 30% más de crecimiento de los ingresos en comparación con las empresas de menor madurez (Deloitte Insights, 2020).

Sin embargo, a medida que el sector de AyS se digitaliza, también se hace más vulnerable a los ataques cibernéticos. El desconocimiento de los riesgos cibernéticos, que se traduce en una falta de inversiones para su mitigación, aumenta su daño potencial. Como proponen Mirjana et al. (2020), la ciberseguridad en el sector industrial, que depende de las tecnologías de IIoT y es vulnerable a ataques cibernéticos especializados, debe gestionarse utilizando marcos adecuados a fin de reforzar la ciberresiliencia de estas infraestructuras.

Ciberseguridad en el sector de agua y saneamiento

Industria 4.0 y la paradoja de la hiperconectividad

La industria 4.0 se refiere a la cuarta revolución industrial, en la que el sector industrial se digitaliza y automatiza más y adopta nuevas tecnologías en los procesos industriales, como la inteligencia artificial (IA), macrodatos (*big data*), cadena de bloques (*blockchain*), drones y realidad virtual y realidad aumentada (RV/RA). El sector de AyS se está transformando de acuerdo con la visión de la industria 4.0, que introducirá desafíos totalmente nuevos debido a la compleja hiperconectividad y al mayor abanico de amenazas. La incorporación de dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) introduce preocupaciones sobre la pérdida de datos, robo de información, privacidad y debilitamiento de la protección de la red, entre otros. A medida que se conectan más dispositivos a las redes operativas, las empresas de servicios públicos se enfrentan a una mayor vulnerabilidad y los *hackers* tienen más oportunidades de acceder a las redes y utilizar vectores de ataque adicionales.

Las soluciones de telemedida (*smart metering*) son un claro ejemplo del avance del sector hacia la industria 4.0. La evolución de las tecnologías de la comunicación implica que los sistemas funcionan a distancia y se gestionan de forma centralizada. Gracias a una captura de datos más frecuente y de mayor calidad, las empresas pueden ofrecer servicios nuevos y mejorados a sus clientes, como la comunicación proactiva de problemas, avisos sobre consumos inusuales de agua y recomendaciones para un consumo responsable. Además de las mejoras cualitativas en los servicios directos al ciudadano, la medición remota ofrece la posibilidad de mejorar la gestión inteligente de la red, detectar precozmente las fugas, mejorar la eficiencia energética y, en última instancia, optimizar los procesos y la gestión eficiente del ciclo integral del agua (Mirjana et al., 2020).

¿Por qué la industria 4.0 es importante para el sector de AyS?

Mirjana et al. (2020) afirman que en el sector de AyS la industria 4.0 es especialmente importante por las razones que se señalan en el Cuadro 2.

Cuadro 2: Importancia de la industria 4.0 para el sector de AyS

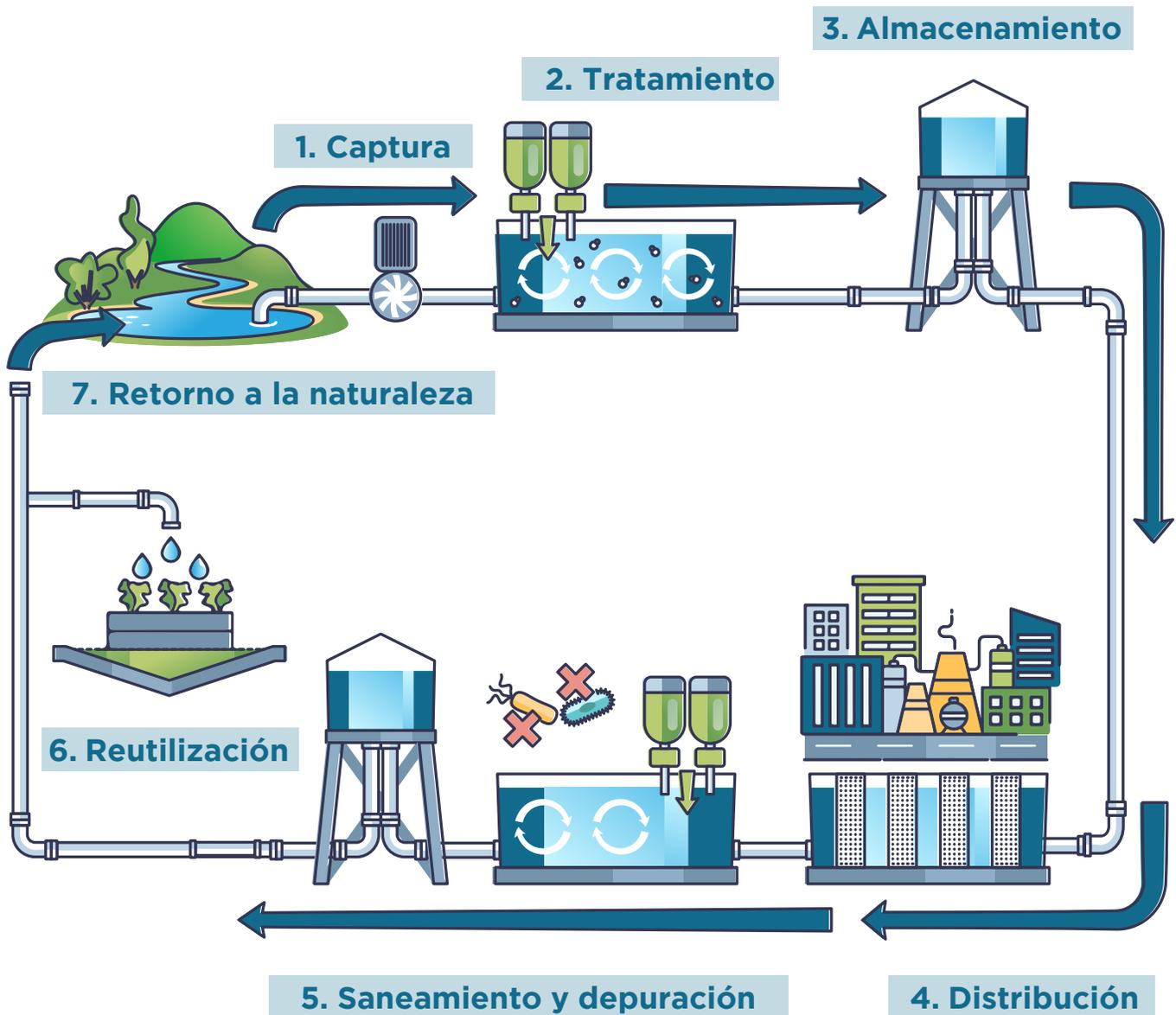
Factores	Descripción
<p>Envejecimiento de la fuerza laboral</p> 	<p>La mano de obra de la industria del agua está atravesando un cambio generacional. Muchas personas se aproximan a la edad de jubilación, se retiran o abandonan el sector en busca de mejores oportunidades. Su alejamiento reduce la mano de obra. Sin embargo, el aspecto más preocupante es la pérdida de los conocimientos y experiencia indocumentada. Debido a la disminución de la recaudación, presupuestos ajustados e inmadurez tecnológica, muchos de los mejores y más brillantes profesionales no se sienten atraídos por el sector de AyS, por lo que los puestos vacantes podrían cubrirse con recursos subóptimos o quedar vacíos.</p>
<p>Gestión de activos</p> 	<p>Los activos de muchas empresas prestadoras de servicios de suministro de agua son antiguos y necesitan rehabilitación o sustitución. Se prevé que los presupuestos de capital disminuyan en los próximos años. Los costos operativos se disparan debido a que los activos se averían con frecuencia y requieren reparaciones de urgencia. Además, las prácticas de gestión de activos son anticuadas en comparación con sectores como el del petróleo y gas, el químico y el de los servicios eléctricos.</p>
<p>Riesgo climático</p> 	<p>Las tres primeras revoluciones industriales, apalancadas por la máquina de vapor, la era de la ciencia y la producción en masa y el surgimiento de la tecnología digital, transformaron la sociedad moderna y cambiaron el mundo por completo. Como consecuencia, el planeta y su clima también se modificaron. Asimismo, aumentan los riesgos para los aspectos medioambientales, económicos y sociales de la civilización, lo que desafía a la sociedad a encontrar nuevas formas de vivir más resistentes y sostenibles. Las empresas prestadoras de servicios de suministro de agua y las comunidades a las que atienden se enfrentan a la disminución de las reservas de agua, a precipitaciones más frecuentes e intensas que agravan los desbordamientos combinados del alcantarillado (CSO, por sus siglas en inglés) y SSO, y a la subida del nivel del mar y la intrusión de agua salada.</p>
<p>Contaminantes emergentes</p> 	<p>Se detectaron microplásticos, compuestos farmacéuticos y otros compuestos refractarios en fuentes de agua potable, aguas residuales, lodos de aguas residuales y biosólidos. Estos contaminantes son nocivos para los seres humanos y la vida acuática. La Agencia de Protección Ambiental de los Estados Unidos y sus agencias de protección medioambiental en los estados pronto exigirán que las empresas prestadoras de servicios de suministro de agua controlen activamente y traten estos contaminantes de acuerdo con los límites normativos.</p>
<p>Cuestiones sociales</p> 	<p>Estas cuestiones incluyen el crecimiento demográfico y la migración, tanto interna (del campo a la ciudad) como externa.</p>

Fuente: Mirjana et al. (2020).



La industria 4.0 es necesaria para la evolución del sector de AyS y su mayor eficiencia. Pasar a la industria 4.0 exige el uso de nuevas tecnologías digitalizadas en la infraestructura del sector de AyS, lo que la expone más que nunca a los ataques cibernéticos. El Gráfico 5 presenta una ilustración de las diferentes etapas del tratamiento del agua.

Gráfico 5: Etapas del tratamiento del agua





Impacto de los ataques cibernéticos en la infraestructura del sector de AyS

Desde hace algún tiempo la prestación de servicios de agua y aguas residuales se considera un componente esencial del desarrollo económico. El agua es un recurso vital para la supervivencia de las personas y del planeta. Las interrupciones en los sistemas de producción, transmisión y distribución de agua pueden provocar enfermedades y morbilidad, dañar la agricultura y la industria, amenazar la seguridad hídrica de los ciudadanos e, incluso, socavar la resiliencia nacional. Por lo tanto, los proveedores de agua deben garantizar siempre un suministro de agua estable y constante para minimizar los posibles daños a la calidad de vida de los ciudadanos (Daigger et al., 2019).

La tríada CID para la seguridad de los datos

La tríada compuesta por la confidencialidad, integridad y disponibilidad (CID) se creó para orientar las políticas de seguridad digital de las organizaciones en torno a los principales riesgos cibernéticos. La confidencialidad limita el acceso a los sistemas o datos restringidos únicamente a usuarios autorizados. La integridad garantiza la confiabilidad, exactitud y exhaustividad de los sistemas, procesos o datos. La disponibilidad garantiza un acceso confiable a los sistemas o datos (Wesley, 2023). En general, en muchos contextos informáticos la confidencialidad puede ser más importante que su integridad, la cual puede ser más importante que su disponibilidad. Sin embargo, en los entornos centrados en los SCI, este orden de importancia suele invertirse (Pe, s.f.): una disponibilidad extremadamente alta del sistema y del servicio puede ser más importante que su integridad, y puede suceder que la confidencialidad sea relativamente menos importante, ya que los contextos de los SCI suelen tratar con datos menos sensibles.

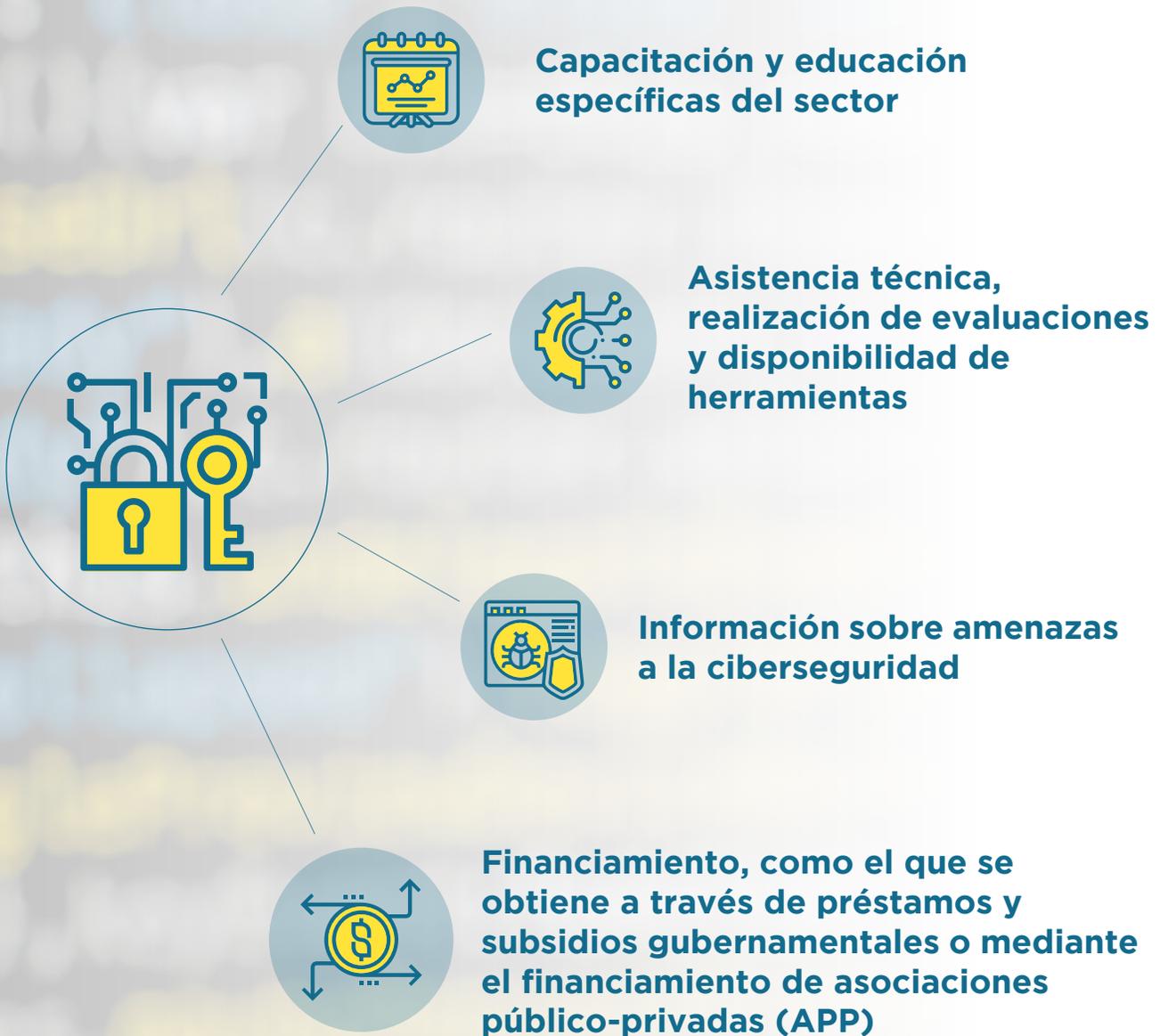
Para ilustrar los principios básicos de la seguridad de la información esbozados por la tríada CID, algunos ejemplos de riesgos para los sistemas de infraestructuras podrían ser los siguientes (Pe, s.f.):

1. Deterioro de la disponibilidad del sistema crítico, por ejemplo, la capacidad de utilizar el sistema informático crítico según se indique en cualquier momento y desde cualquier lugar designado a tal efecto.
2. Deterioro de la capacidad de producción de sistemas críticos.
3. Deterioro de la confiabilidad e integridad de la información o los procesos de sistemas críticos, con resultados contrarios a la finalidad prevista de los sistemas. La alteración o destrucción no autorizada de información puede perjudicar el correcto funcionamiento de sistemas informáticos críticos.
4. Violación de la confidencialidad de la información almacenada en estos sistemas, que podría afectar los sistemas informáticos críticos o los activos de información de la organización. Un ejemplo puede ser la divulgación de datos utilizados por las divisiones comerciales de las empresas de servicios públicos.



Elementos clave para mejorar la situación del sector en materia de ciberseguridad

Según el *Informe sobre el estado de la ciberseguridad en el sector para 2021*, publicado por el Consejo Coordinador del Sector del Agua de Estados Unidos (WSCC, 2021), las cuatro principales áreas de preocupación que afectan a la ciberseguridad para el sector de AyS son las brechas en:





Una publicación del Departamento de Energía de Estados Unidos (Clark et al., 2017) revela las cinco principales áreas técnicas del sector de AyS que sufren frecuentes brechas de seguridad:

1. Configuraciones de la red
2. Protección de los medios de comunicación y plataformas de *streaming*
3. Acceso remoto a los sistemas operativos del agua
4. Políticas y procedimientos documentados
5. Personal con capacitación inadecuada

Una encuesta realizada por el WSCC (2021) sobre el estado de la ciberseguridad de la infraestructura del sector de AyS en los Estados Unidos identificó las necesidades del sector y las ordenó de más a menos indispensables, tal como se muestra a continuación:

1. Asistencia técnica
2. Subsidios o préstamos federales para equipos o servicios de ciberseguridad
3. Capacitación y educación dirigidas al sector
4. Garantía de la integridad de la cadena de suministro de *hardware* y *software* de TI y TO
5. Financiamiento para contratar personal de ciberseguridad
6. Información sobre amenazas a la ciberseguridad



Una encuesta realizada por el Water Information and Sharing Analysis Center (WaterISAC, 2021) sobre el estado de la ciberseguridad de la infraestructura del sector de AyS en los Estados Unidos, que incluye una muestra representativa de los sistemas de todos los tamaños, concluye que en 2021 se realizaron las siguientes asignaciones presupuestarias para ciberseguridad:

- El **38%** de los sistemas asigna menos del 1% del presupuesto a la ciberseguridad de la TI.

- El **22,1%** de los sistemas asigna entre el 1% y el 5% del presupuesto a la ciberseguridad de la TI.

- El **6,3%** de los sistemas asigna entre el 6% y el 10% del presupuesto a la ciberseguridad de la TI.

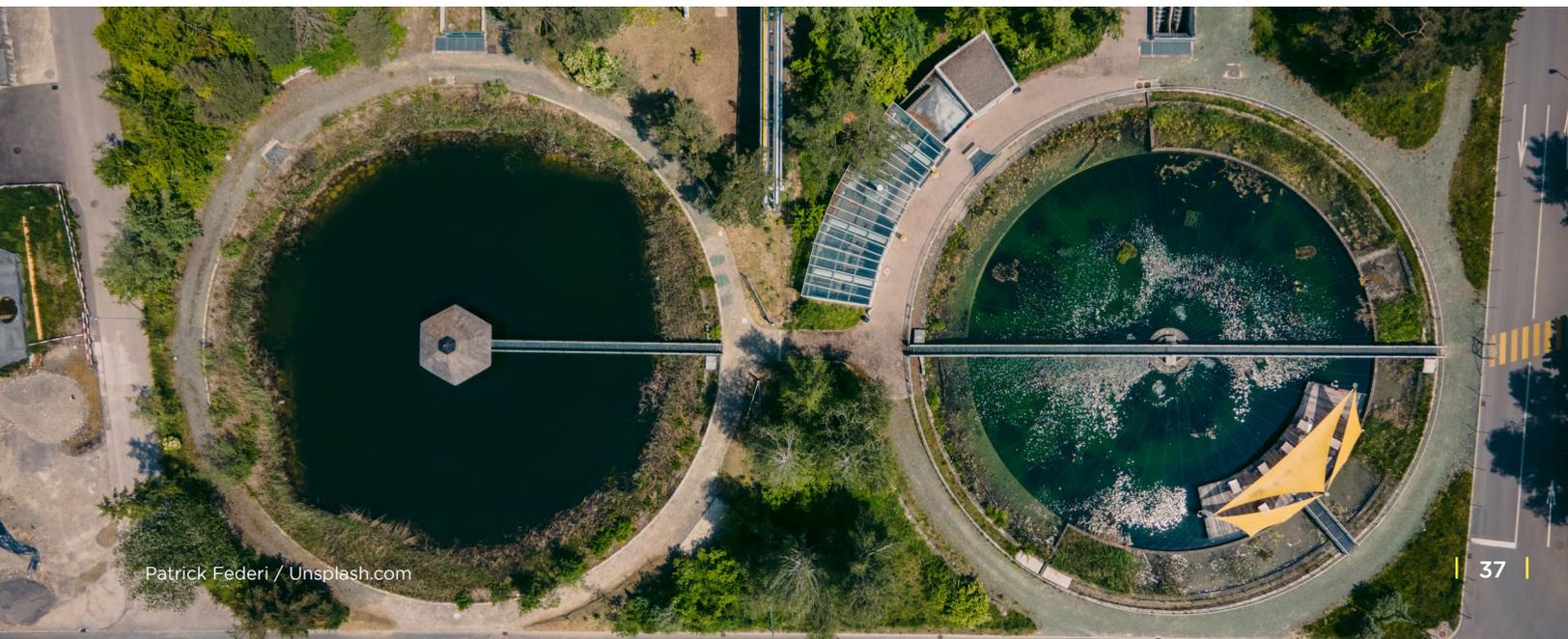
- El **4,1%** de los sistemas asigna más del 10% del presupuesto a la ciberseguridad de la TI.

- El **44,8%** de los sistemas asigna menos del 1% del presupuesto a la ciberseguridad de la TO.

- El **20,95%** de los sistemas asigna entre el 1% y el 5% del presupuesto a la ciberseguridad de la TO.

- El **4,9%** de los sistemas asigna entre el 6% y el 10% del presupuesto a la ciberseguridad de la TO.

- El **1,7%** de los sistemas asigna más del 10% del presupuesto a la ciberseguridad de la TO.





Las cifras anteriores analizan los informes sobre asignaciones presupuestarias en la práctica. Por lo tanto, no indican necesariamente una asignación óptima del presupuesto de ciberseguridad, sino que de hecho, pueden documentar la asignación de un presupuesto insuficiente para mitigar los riesgos cibernéticos en los servicios públicos críticos y, específicamente, en el ámbito de la TO.

Daños potenciales y su impacto en la infraestructura del sector de AyS

El impacto potencial sobre la producción de agua potable o el tratamiento de aguas residuales puede incluir los siguientes escenarios (Thielemann et al., 2021):



Los ciudadanos se verían privados de agua potable segura y saneamiento



Los hospitales no podrían funcionar



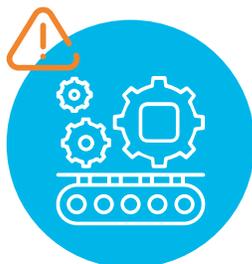
Las mangueras contra incendios no funcionarían



Las escuelas, oficinas e instalaciones gubernamentales permanecerían cerradas



Los cultivos agrícolas sufrirían daños



Se paralizarían varios segmentos de fabricación



Se interrumpiría el suministro de agua a las instalaciones nucleares que dependen de la refrigeración por agua



Todos los sistemas relacionados con el suministro de agua, calidad del agua, reducción del riesgo de inundaciones, electricidad, producción agrícola y aguas residuales son potencialmente vulnerables a los ataques cibernéticos, con consecuencias devastadoras para la salud, el medioambiente y la economía (Misión de Israel ante Naciones Unidas, 2021). El Cuadro 3 presenta posibles escenarios en los que las amenazas cibernéticas a las instalaciones de agua dedicadas a la producción, transmisión y purificación pueden producir daños significativos (OCDE Agua, s.f.):

Cuadro 3: Posibles escenarios de daños

Daños potenciales	Área(s) de impacto	Escenario No. 1	Escenario No. 2
Deterioro del caudal operativo para la producción y transmisión de agua	<ul style="list-style-type: none"> • Uso urbano y doméstico • Productividad industrial • Productividad agrícola • Salud humana 	(a) Un chorro de agua a alta presión puede hacer que varias piedras y objetos que están por encima y alrededor de la tubería dañada sean expulsados, pudiendo dañar a las personas y al medioambiente.	(b) Las fugas de una tubería de agua subterránea provocan el desplazamiento de arena, que puede dañar los cimientos, infraestructuras subterráneas cercanas, carreteras y edificios, y resultar en su derrumbe e inundación.
Contaminación de las fuentes de agua	<ul style="list-style-type: none"> • Público en general 	Manipulación del proceso de depuración o desalinización del agua.	CSO o SSO que causan una contaminación masiva del agua de pozo.
Daños medioambientales y ecológicos que resultan del tratamiento de aguas residuales	<ul style="list-style-type: none"> • Productividad agrícola • Salud humana • Medioambiente 	Las líneas de alcantarillado están sometidas a presión hidráulica interna (líneas de drenaje) y, cuando se dañan, pueden dañar las líneas de agua. Normalmente, el caudal en las tuberías de alcantarillado depende de la gravedad. Por lo tanto, los principales riesgos derivados de los daños en las tuberías son la contaminación ambiental, la contaminación de las fuentes de agua subterránea y los efectos nocivos para la salud.	CSO o SSO que causan una contaminación masiva del agua de pozo y problemas medioambientales.

Fuente: Elaboración propia y OCDE Agua (s.f.). Los escenarios (a) y (b) se tomaron de Ali y Choi (2019).



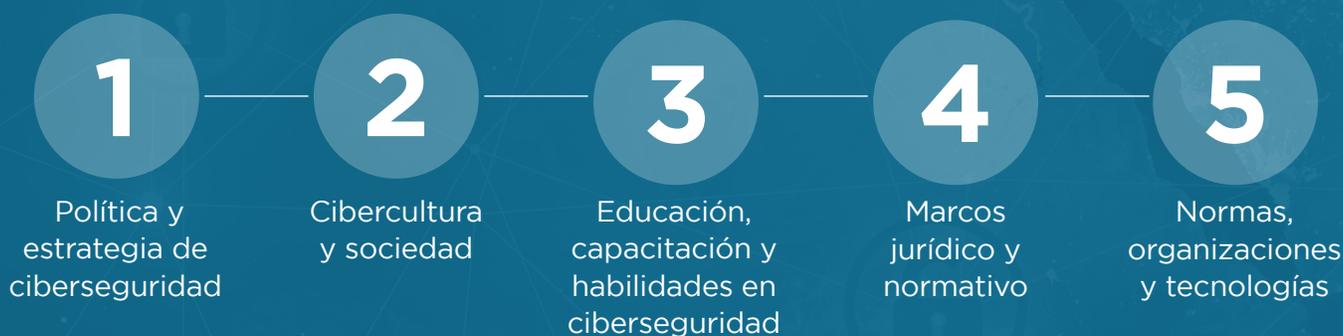
Preparación del sector de agua y saneamiento en América Latina y el Caribe

Ciberseguridad regional en ALC

Tendencias regionales

Los países difieren en su enfoque de la ciberseguridad, dependiendo de su panorama económico, político y cultural. Algunos consideran que la ciberseguridad es una cuestión de seguridad nacional, mientras que otros la ven como un reto para el desarrollo económico. Como se menciona en el informe sobre ciberseguridad de BID y OEA (2020), la región de ALC no está suficientemente preparada para hacer frente a los ataques cibernéticos. Solo siete de los 32 países cuentan con un plan de protección de IC, mientras que 20 han creado equipos de respuesta a incidentes de ciberseguridad. Esto limita su capacidad para identificar y responder a los ataques.

El CMM, desarrollado por el Centro Global de Capacidad de Ciberseguridad de la Universidad de Oxford (2021), es un marco metodológico diseñado para analizar la capacidad de ciberseguridad de un país. El CMM sigue un enfoque global que evalúa la madurez de las naciones en cinco dimensiones:





El BID y la OEA utilizaron el CMM para evaluar la madurez de los países de ALC en 2016 y 2020 (BID y OEA, 2016 y 2020). De acuerdo con estas evaluaciones, los países de ALC avanzaron en su postura con respecto a la ciberseguridad, dado que algunos alcanzaron niveles de madurez más altos en los indicadores de identificación, organización y gestión de riesgos y respuesta con respecto a la protección de IC, entre otras mejoras importantes. La principal tendencia observada en la región es el establecimiento de planes de protección de IC. En 2016 solo uno de cada cinco países contaba con una estrategia de ciberseguridad o un plan de protección de IC. Para 2020, 12 países de la región habían aprobado estrategias nacionales de ciberseguridad, siete contaban con planes de protección de IC, mientras que otros estaban mejorando sus capacidades en ese momento.

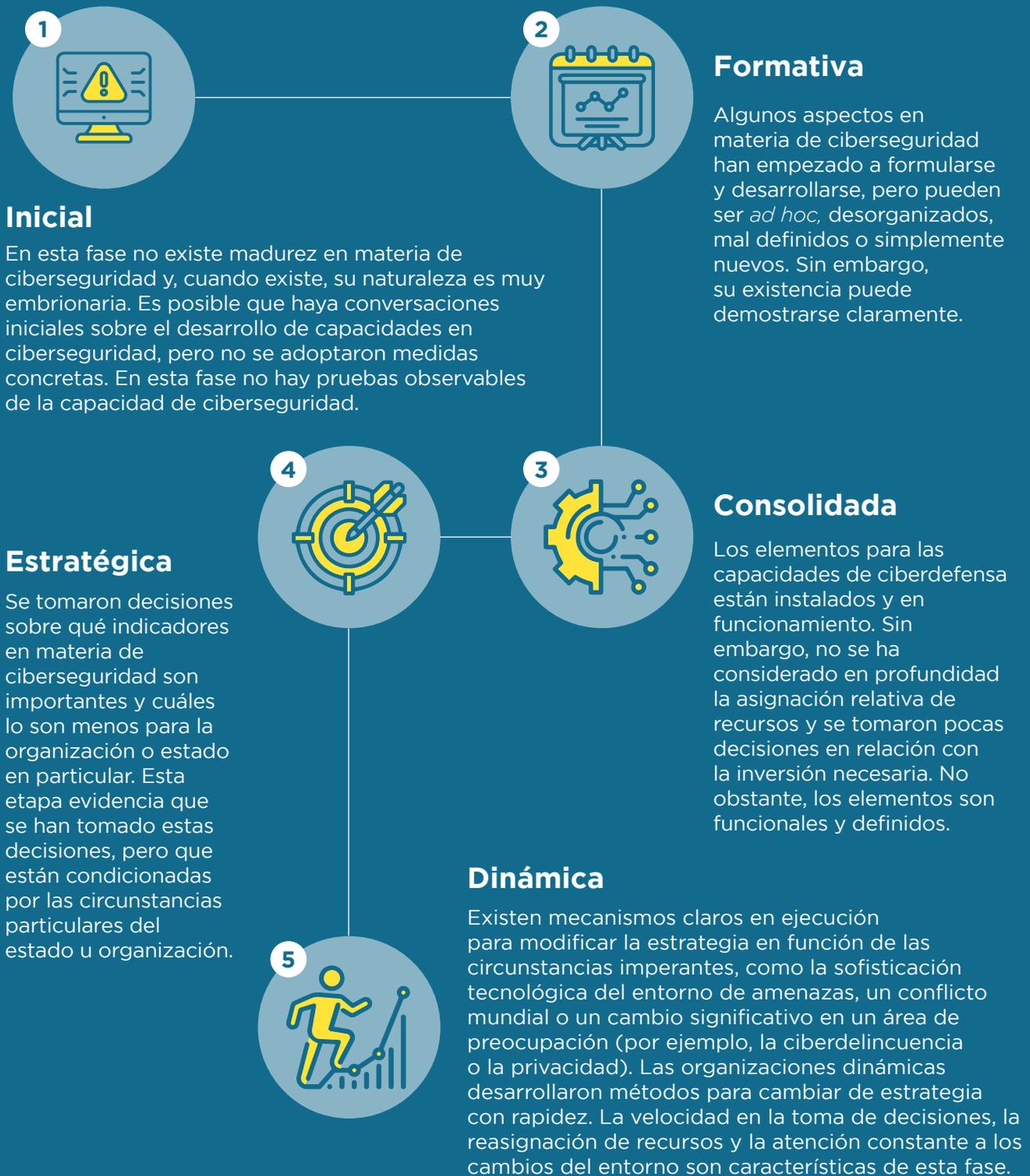
El costo de la ciberdelincuencia mundial aumentó de manera considerable. Tal como informa McAfee en su publicación *The Hidden Cost of Cybercrime* (Lewis, 2020), los costos aumentaron más de un 50% entre 2018 y 2020, ya que pasaron de US\$600.000 millones a más de US\$1 billón. Un informe publicado por IBM Security (2021) reveló que el costo promedio por incidente cibernético en grandes empresas en ALC aumentó un 52,4% entre 2020 y 2021 y estableció el costo promedio de violación de datos en US\$2.560.000 en la región, mientras que el costo promedio por incidente a nivel mundial fue de US\$4.240.000.

Argentina, Brasil, Colombia y México se encuentran entre las economías más grandes y más digitalizadas de ALC. En consecuencia, estos países tienen algunas de las mayores superficies de exposición a los ataques cibernéticos, es decir, tienen más activos digitales expuestos a ataques potenciales. El *ransomware* de cifrado se convirtió en una importante amenaza para las IC de la región. La mayoría de los sistemas de automatización industrial atacados se encuentran en Brasil (0,9%), México (0,5%) y Colombia (0,4%), cifras que representan el porcentaje de computadoras atacadas por *malware* en ese mismo país. Se registraron menos ataques en Argentina, Chile, Costa Rica, Ecuador, Panamá, Paraguay y República Dominicana (Kaspersky, 2017a).

Protección de las IC en la región

Las dimensiones consideradas en el CMM tratan de proporcionar una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país y le asignan una etapa específica que corresponde a su grado de logros en materia de ciberseguridad. Las cinco etapas de madurez, que se asignan mediante una evaluación, van de la más básica (inicial) a la más avanzada (dinámica) y se definen como muestra el Gráfico 6.

Gráfico 6: Cinco etapas de madurez



Cuando este marco se aplica para analizar la protección de las IC en los países de ALC, es posible evaluar la capacidad del gobierno para **identificar** sus activos de IC, los esfuerzos **organizativos** para regular la ciberseguridad de esas infraestructuras y las capacidades para la **gestión de riesgos y respuesta**, y de esta manera reconocer la capacidad del país para proteger sus IC de las amenazas cibernéticas.



El Cuadro 4 presenta la madurez de los países de ALC en materia de protección de IC según el estudio realizado por el BID y la OEA (2020).

Cuadro 4: Madurez del país según el CMM con respecto a la protección de las IC en ALC

País	Protección de las infraestructuras críticas														
	Identificación					Organización					Gestión de riesgos y respuesta				
Antigua y Barbuda		2					2				1				
Argentina		2					2					2			
Bahamas		2				1					1				
Barbados	1					1					1				
Belice	1						2				1				
Bolivia		2				1					1				
Brasil			3					3					3		
Chile		2					2					2			
Colombia			3						4					4	
Costa Rica	1					1					1				
Dominica	1					1					1				
Ecuador	1					1						2			
El Salvador	1					1					1				
Granada	1					1					1				
Guatemala	1					1					1				



Protección de las infraestructuras críticas

País	Identificación					Organización					Gestión de riesgos y respuesta				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Guyana		2				1					1				
Haití	1					1					1				
Honduras		2					2					2			
Jamaica		2				1					1				
México		2					2					2			
Nicaragua	1					1					1				
Panamá		2					2					2			
Paraguay	1					1					1				
Perú		2					2				1				
República Dominicana	1						2				1				
San Cristóbal y Nieves		2				1					1				
Santa Lucía	1					1					1				
San Vicente y las Granadinas	1					1					1				
Surinam	1					1					1				
Trinidad y Tobago		2					2					2			
Uruguay		2						3					3		
Venezuela	1					1						2			

Fuente: BID y OEA (2020).



El estudio de BID y OEA ofrece una visión crítica sobre la situación de los países de ALC y las oportunidades que la región puede capitalizar para mejorar su protección de las IC. Con base en esta información, se evidencia que el **nivel medio de madurez de la región sigue estando entre 1 y 2**, según el CMM. En otras palabras, la mayoría de los países de ALC empieza a formular algunas iniciativas de ciberseguridad que involucran a sus IC, mientras que algunas de estas estrategias ya están en marcha, aunque se están implementando de manera *ad hoc* y carecen de coordinación entre las partes interesadas clave. En este sentido, los riesgos asociados a la falta de un mecanismo institucionalizado para hacer frente a las vulnerabilidades de las IC exacerbando las capacidades internas de respuesta de la región, incluidas la organización de protección de IC, la gestión de crisis y la gestión de riesgos y respuesta, que como resultado promedian hacia la parte inferior de la escala (BID y OEA, 2020).

¿Por qué ALC es más vulnerable a los ataques cibernéticos?

Al igual que otras regiones del mundo, ALC está cada vez más digitalizada. En la última década, el acceso a Internet en ALC aumentó a un ritmo exponencial (Prado, 2011). Según la Unión Internacional de Telecomunicaciones (UIT), más de dos tercios de la población de ALC está en línea, en comparación con solo el 53,6% de los usuarios de Internet en todo el mundo (UIT, 2019). El aumento de la penetración de Internet en los hogares se produjo simultáneamente con el crecimiento de la digitalización de empresas, fábricas y proveedores de servicios, lo que exigió una estrategia de ciberseguridad más madura, integral y relevante para la región.

Al describir el panorama de las amenazas de la ciberdelincuencia en ALC, existe un factor especialmente destacado: el nexo entre desarrollo económico, digitalización, gobernanza y delincuencia. Si bien los países de ALC están incorporando cadenas de suministro mundiales y prosiguen su desarrollo económico, los avances institucionales aún son incipientes. Las fragilidades institucionales de algunos países se traducen en una deficiente gobernanza de ciberseguridad, dada por la falta de una legislación sólida en materia de ciberdelincuencia, de una aplicación adecuada de la ciberlegislación, de conocimientos técnicos y de cooperación jurídica internacional. Esto, a su vez, podría atraer a delincuentes cibernéticos que creen que la región es un objetivo fácil (Pimenta Klein y Boguslavskiy, 2020).

Al igual que otros tipos de delitos, las características específicas de la ciberdelincuencia en ALC están relacionadas principalmente con la vulnerabilidad socioeconómica de la región. Dada la disponibilidad de tecnologías digitales que permiten llevar a cabo delitos cibernéticos con facilidad, los grupos delictivos tradicionales decidieron recurrir a las actividades cibernéticas para obtener ganancias financieras potencialmente mayores en un ámbito digital poco regulado, lo que se traduce en menores riesgos para los delincuentes.

En otras palabras, la ciberdelincuencia en ALC es el resultado de las fragilidades del desarrollo regional, es decir, su rápida digitalización y adaptación a las nuevas tecnologías frente al retraso de la regulación y las políticas. Este vacío de aplicación y autoridad creado por la expansión y evolución del uso de la TIC atrae a agentes malintencionados, como los grupos delictivos tradicionales. Como resultado, los agentes de amenaza encuentran numerosas brechas en las infraestructuras tanto digitales como sociales y, por tanto, aumenta la motivación para participar en actividades de ciberdelincuencia casi sin reservas (Pimenta Klein y Boguslavskiy, 2020).



¿Por qué las empresas prestadoras de servicios de suministro de agua en ALC no son blanco de más ataques cibernéticos?

Tal como se mencionó previamente, la infraestructura del sector de AyS de la región de ALC suele ser antigua y aún no se hizo la transición a sistemas de tecnología de avanzada. Los sistemas de las infraestructuras que no están digitalizados ni conectados en línea permanecen aislados de muchos riesgos cibernéticos. Sin embargo, se deben tener en cuenta dos cuestiones importantes cuando se habla del número de ataques cibernéticos a las empresas prestadoras de servicios de suministro de agua en la región de ALC:



A medida que el sector de AyS realiza su transición hacia tecnologías más modernas, se prevé un número más alto de ataques cibernéticos contra las empresas prestadoras de servicios de suministro de agua en tanto no se implementen mecanismos adecuados de ciberseguridad.



La falta de vigilancia cibernética de las empresas prestadoras de servicios de suministro de agua modernizadas crea puntos ciegos en los que podrían producirse ataques cibernéticos que aún no se imaginan.

Cooperación regional en ciberseguridad

En las últimas décadas, ALC cooperó regionalmente en cuestiones de ciberseguridad y reforzó la capacidad de sus países para contrarrestar las amenazas digitales. Si bien esta cooperación regional podría fomentar una convergencia diplomática en el ámbito cibernético, los países de ALC aún no constituyen un bloque regional en las conversaciones con Naciones Unidas sobre la estabilidad del ciberespacio. Los países de ALC elaboran políticas de ciberseguridad y mecanismos de protección a un ritmo lento desde 2004, momento en que se convirtió en la primera región en articular una estrategia en materia de ciberseguridad (Van Raemdonck, 2020).

El Instituto de Estudios de Seguridad de la Unión Europea (IESUE) identificó los siguientes factores como causas de esta situación:

1. Niveles desiguales de penetración digital.
2. Escasa sensación de urgencia por parte de los formuladores de políticas a la hora de coordinar sus respuestas en materia de ciberseguridad debido a la falta de difusión pública de ataques de gran repercusión.
3. Ausencia de recursos financieros destinados a la inversión en seguridad digital nacional.
4. Falta de experiencia por parte de los formuladores de políticas y profesionales de las TI.





Otras razones que explican la lentitud de ALC a la hora de adaptarse a las amenazas cada vez mayores en torno a la ciberseguridad son su limitado conocimiento respecto de las medidas y riesgos relacionados, la falta de confianza entre países de la región y dentro de cada país, la desconexión entre el sector público y el privado, y las marcadas disparidades socioeconómicas que hacen que más personas caigan en la delincuencia y, dentro de ella, en el delito informático o ciberdelito. El IESUE reconoce que existen mecanismos eficaces de cooperación regional que pueden ayudar a ALC a hacer frente a las amenazas digitales. Organizaciones multilaterales, como el BID y la OEA, contribuyen a esta cooperación efectiva a través de diferentes programas gestionados por los grupos de ciberseguridad de cada entidad.

El desarrollo de la ciberseguridad en el sector privado se debe principalmente a la disponibilidad de recursos financieros, humanos y tecnológicos. Por lo tanto, la cooperación entre el sector público y el privado es una condición necesaria. Esta cooperación podría adoptar la forma de APP para la promoción de políticas de ciberseguridad en el ámbito nacional, regional e internacional. Este tipo de colaboración público-privada exige una buena coordinación y poder de decisión para hacer frente a las amenazas cibernéticas.

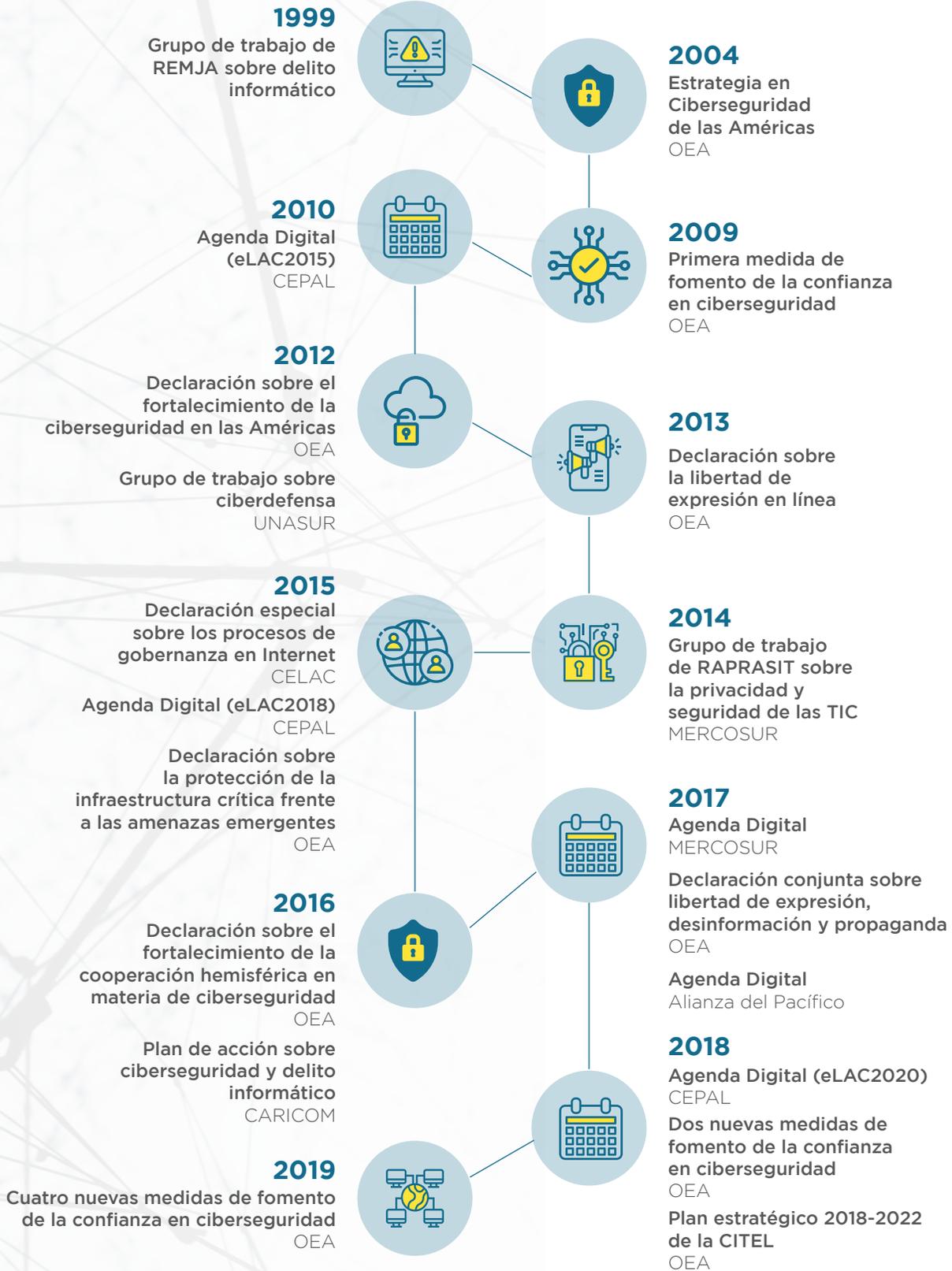
Dado que los ataques cibernéticos pueden cruzar fronteras, la cooperación transnacional es especialmente decisiva en el ámbito cibernético. Las políticas cibernéticas deberían actualizarse y coordinarse de manera regional, y los países deberían dedicar esfuerzos y recursos a este ámbito común (Saavedra, 2015). Organizaciones regionales y subregionales, como la OEA, la Unión de Naciones Suramericanas (UNASUR) y el Sistema de la Integración Centroamericana (SICA), entre otras, pueden ayudar a armonizar estrategias para la ciberseguridad regional común. Esta armonización promoverá la sanción de leyes y la cooperación de las naciones de la región, así como la elaboración de planes de acción coherentes (Saavedra, 2015).

Falta de incentivos

En los últimos años, a medida que el uso de sistemas digitales en el mundo registra un fuerte aumento, la crisis en materia de ciberdefensa se agrava y los ataques cibernéticos aumentan drásticamente. Sin embargo, el crecimiento del número de ataques cibernéticos también puede explicarse porque no se ha invertido en suficientes recursos para desarrollar productos y servicios de *hardware* y *software* seguros que operen en el ciberespacio. La mayoría de las empresas consideran que las inversiones destinadas a la ciberseguridad de sus productos podrían no ser viables desde el punto de vista financiero, dado que los costos pueden ser más altos que el potencial daño que sufrirían como consecuencia de los incidentes de ciberseguridad. A su vez, esto conduce a pocos incentivos para este tipo de inversión (Brangetto y Kert-Saint Aubyn, 2015). En 2018 la OEA y Microsoft encuestaron a propietarios y operadores de IC y concluyeron que muchos gobiernos de la región no habían establecido programas de incentivos para alentar la adopción voluntaria de medidas de ciberseguridad por parte de esos propietarios y operadores, ni habían comenzado a implementar marcos obligatorios para hacerlo (OEA, 2018). El Gráfico 7 ofrece una perspectiva general de 20 años de iniciativas en la región de ALC.



Gráfico 7: Cronología de políticas en materia de ciberseguridad en la región de ALC, 1999-2019



Fuente: Van Raemdonck (2020). **Notas:** REMJA: Reunión de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas; CITELE: Comisión Interamericana de Telecomunicaciones; RAPRASIT: Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica.



Entrevistas: metodología y perspectivas

Con el propósito de enriquecer esta publicación, se llevaron a cabo varias entrevistas en la región. Participaron en ellas representantes de instituciones estatales y de empresas pres-tadoras de servicios de suministro de agua de los siguientes siete países: Belice, Brasil, Chi-le, Jamaica, Panamá, Surinam y Trinidad y Tobago. Las entrevistas se realizaron mediante videollamadas y a cada entrevistado se le preguntó por la ciberseguridad en la región, en su país y en particular en el sector de AyS (véanse los [Anexos A y B](#)).

Si bien los países de la región de ALC realizan esfuerzos por mejorar la protección en ma-teria de ciberseguridad de su infraestructura del sector de AyS, las protecciones existentes no abordan los riesgos por completo. Este proceso exige reglamentaciones adicionales, financiamiento, además de un mayor conocimiento de las instalaciones de suministro de agua por parte de propietarios y operadores.

Como resultado de las entrevistas, se identificaron varias tendencias, entre ellas, una mayor inver-sión en materia de ciberseguridad, dado que los directivos reconocieron que los riesgos ciberné-ticos afectan diversas esferas de la operación, por ejemplo, el ámbito comercial, el tratamiento de aguas residuales, los recursos hídricos y la calidad de los servicios. Si bien existen numerosas reglamentaciones que cubren ciertos aspectos, como la calidad del suministro de agua, suelen existir brechas en lo que respecta a reglamentaciones en materia de ciberseguridad.

En algunos países de ALC, la mayoría de los procesos operativos aún continúan realizándose en forma manual; de hecho, las autoridades reguladoras del suministro de agua operan de forma remota solo el 15% de sus sistemas. En el caso de Belice, por ejemplo, se observan estas tenden-cias, que también se describen en el Gráfico 8 (Observatorio del Crimen de Belice, 2020).

Gráfico 8: Prioridades de la Estrategia de Ciberseguridad de Belice 2020-2030



Fuente: Observatorio del Crimen de Belice (2020).

El segundo objetivo que se describe en la Estrategia Nacional de Belice publicada en 2020 se refiere a las normas mínimas de seguridad para los sistemas de información de IC. Este objetivo, que incluye varias actividades, se espera lograr en el largo plazo. Algunas de estas actividades son las siguientes (Observatorio del Crimen de Belice, 2020):

1. Identificar normas mínimas para las IC de información.

2. Redactar normas mínimas de seguridad para los sistemas de IC de información.

3. Crear un grupo de trabajo destinado a analizar amenazas y recomendar normas acordes con la industria.

Ciberseguridad en el sector de agua y el saneamiento en ALC

Las entrevistas llevadas a cabo también permitieron identificar otras cuestiones:

Falta de designación oficial de la infraestructura del sector de AyS como crítica. La falta de una designación oficial de la infraestructura del sector de AyS como IC nacional dificulta la realización de mayores esfuerzos por parte de los organismos oficiales del Estado nacional en cuanto a la implementación de mejoras en la ciberseguridad de dicha infraestructura. En algunos países, esto se debe principalmente a la deficiente gestión nacional de los riesgos cibernéticos de las IC.

Escasez de equipos dedicados a la ciberseguridad en las empresas prestadoras de servicios de suministro de agua durante su digitalización. En la actualidad algunas empresas prestadoras de servicios de suministro de agua de ALC utilizan guías genéricas de mejores prácticas de la industria y proveedores en materia de ciberseguridad (por ejemplo, políticas de cortafuegos), pero aún no redactaron sus propios lineamientos. Esto podría deberse a que la digitalización de los sistemas de suministro de agua en esos países es relativamente reciente y se encuentra en proceso de implementación, aunque algunos de estos países comparten información y conocimiento en soluciones de ciberseguridad para las industrias relacionadas con el suministro de agua en el ámbito doméstico. En algunos casos, la digitalización podría llevarse a cabo de manera oficial y estructurada, mientras que en otros puede hacerse de manera informal con base en las relaciones personales.

Falta de entidades designadas para la ciberseguridad. Otro problema que impide que los países tengan una estrategia sólida en materia de ciberseguridad destinada a las IC del sector de AyS es la falta de designación de una entidad responsable del tema dentro de las agencias competentes del país. Por ejemplo, en uno de los países de ALC, una empresa estatal responsable por el suministro de agua carece de una función dedicada a la ciberseguridad. Allí, el departamento de TI ejecuta las operaciones cibernéticas diarias de la organización y, para hacerlo, cuenta con menos del 1% del total de empleados de la empresa prestadora de servicios de suministro de agua.



Amenazas nuevas y aún no conocidas. Algunos países de ALC disponen de mecanismos más avanzados para gestionar la ciberseguridad de la IC, pero no tienen una preparación adecuada ante un ataque grave contra sus instalaciones del sector de AyS. Entre los problemas que afectan a la preparación, se encuentran la escasa experiencia en hacer frente a grandes ataques y la limitada disponibilidad de profesionales altamente especializados. En uno de los países más maduros de ALC en términos de ciberseguridad, la empresa prestadora más grande de servicios de suministro de agua y alcantarillado reconoce que las áreas que más preocupan en el sector son la falta de conocimiento en torno a todo el inventario de dispositivos de TI y TO, infraestructura industrial no segura (es decir, activos digitales) y capacitación deficiente del personal. Desde su perspectiva, esto podría repercutir en:



Pérdida de información



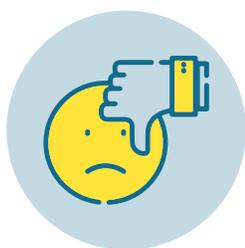
Robo de identidad



Actividades fraudulentas



Daños ambientales



Daños a la reputación



Daños a la salud pública



Daños a infraestructura pública

En otro ejemplo, una de las empresas prestadoras de servicios de suministro de agua que participó en las entrevistas está regulada por dos autoridades: una se ocupa de la calidad del servicio y otra de cuestiones tecnológicas. Si bien la reglamentación es un paso importante para el logro de una ciberdefensa robusta, la organización solo cuenta con un empleado a cargo de la ciberseguridad en el departamento de TI. De hecho, la organización no dispone de procedimientos de ciberseguridad aprobados, más allá de una lista de tareas y la necesidad de verificar controles básicos. Sin embargo, esos controles no están regulados y se revisan únicamente según su criticidad. La organización también carece de un plan de trabajo anual holístico en materia de ciberseguridad, por lo que solo gestiona una lista de proyectos de ciberseguridad que se evalúan anualmente. Si bien se realizó una prueba de penetración cuatro años antes de la entrevista, nunca se llevó a cabo una auditoría en materia de ciberseguridad. Además, se manifestó que utilizaban metodologías desarrolladas para proteger dispositivos de TO de otros sectores y las adaptaban a la industria del agua.



Descripción del estado de la ciberseguridad en cinco países

Medidas específicas por país

A continuación, se incluyen varios ejemplos de países de ALC y su enfoque para mejorar la resiliencia de la nación en materia de ciberseguridad.



Argentina

En los últimos años, Argentina adoptó múltiples medidas para implementar políticas, reglamentaciones y reformas en los sectores de telecomunicaciones, Internet y tecnología del país (BID y OEA, 2020). En 2008 el país modificó el Código Penal e incluyó el delito informático. En 2016 el Poder Ejecutivo promulgó un decreto por el que se creó el Ministerio de Modernización y que estableció la creación de la Subsecretaría de Tecnología y Ciberseguridad dentro del nuevo ministerio, bajo cuya dirección están la Oficina Nacional de Tecnologías de la Información, la Dirección Nacional de Infraestructura Tecnológica y Operaciones y la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (Privacy International, 2019). En 2017 se creó el Comité de Ciberseguridad, que depende del Gabinete de Ministros y del cual participan delegados de los ministerios de Defensa y Seguridad. Su misión era elaborar una estrategia nacional de ciberseguridad, que se publicó en 2019. El Decreto 50 de 2019 asignó responsabilidades en materia de protección de IC a la Secretaría de Innovación Pública de la Jefatura del Gabinete de Ministros. A principios de 2023, esa misma secretaría llevó a cabo consultas públicas para actualizar la estrategia nacional de ciberseguridad.

Argentina fue uno de los primeros países de ALC en disponer de un marco normativo destinado a proteger los datos personales y es uno de los pocos países de la región que participa en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales. El gobierno argentino recibió un préstamo basado en políticas (PBL) del BID en 2019 con el propósito de apuntalar la implementación de políticas relacionadas con la IC y las prácticas en el uso de TIC en sus esfuerzos por fortalecer las capacidades nacionales de ciberseguridad, y otro préstamo de inversión del BID en 2023 destinado a proteger las IC de información. Argentina también elaboró un Programa nacional de infraestructuras críticas de información y ciberseguridad (ICIC) a fin de establecer un marco normativo que defina y proteja las infraestructuras estratégicas y críticas pertenecientes tanto al sector público y al privado, como a organizaciones interjurisdiccionales. También cabe destacar que Argentina ofrece una variedad de oportunidades educativas relacionadas con la cibereducación en universidades tanto públicas como privadas y en organizaciones de la sociedad civil, y pertenece a grupos de trabajo sobre ciberseguridad con otros países (BID y OEA, 2020).





Brasil

Los operadores públicos y privados de IC en Brasil varían en cuanto a su madurez en la protección de la IC. Todas las instituciones federales deben evaluar anualmente los riesgos relacionados con la ciberseguridad en función de las lecciones aprendidas a partir de los principales incidentes en esta materia. En respuesta a la información proporcionada por la herramienta de conocimiento de la situación del equipo de respuesta a emergencias informáticas de Brasil (CERT.br, por sus siglas en inglés) todas las instituciones públicas cuentan con políticas y procedimientos claramente definidos (OEA, 2020). Alrededor del 54% de los ataques cibernéticos informados en Brasil se originan en el propio país (Lewis, 2018).



Chile

A diferencia de sus vecinos sudamericanos, el delito informático más común en Chile no es la estafa ni el *phishing*, sino la infección por *malware*. Esta tendencia es el resultado de una población con educación técnica en materia de ciberseguridad, que hace uso de las mejores prácticas para mantener a salvo sus dispositivos y datos. Sin embargo, los destinatarios de los ataques son los mismos que los de otros países latinoamericanos: el sector financiero, en especial, los bancos. A modo de ejemplo, el Banco de Chile, el segundo mayor banco del país, sufrió un importante ataque de *ransomware* en mayo de 2018 por el que perdió US\$10.000.000 (Pimenta Klein y Boguslavskiy, 2020). Chile publicó su Política nacional de ciberseguridad en 2017, la cual incluye medidas para proteger las IC. Se está redactando una versión actualizada en 2023.



Colombia

Colombia fue el primer país de América Latina en aprobar una estrategia nacional de ciberseguridad en 2011. Cinco años después, puso en marcha una estrategia actualizada conocida como Política nacional de seguridad digital. Esta nueva versión actualizó la visión de la primera política, ya que incluye la gestión del riesgo (Hernández, 2018). En 2023 el Plan nacional de desarrollo 2023-2026 resaltó la importancia de proteger la IC y determinó que la Dirección Nacional de Seguridad Digital coordinaría estos esfuerzos, tal como se estableció en el Decreto 338 de 2022.



República Dominicana

Según un estudio sobre el nivel de madurez de las estrategias nacionales de ciberseguridad, la estrategia de República Dominicana se considera una de las más maduras de ALC y por su modelo se califica como consolidada. En 2020 se determinó que la estrategia y la política de ciberseguridad del país presentaban debilidades relacionadas con la gestión de la crisis, ciberdefensa y redundancia de las comunicaciones, áreas en las que ahora se produjeron avances. En términos de protección de las IC, República Dominicana es el país más sólido en aspectos organizativos, mientras que avanza en la mejora de cuestiones relacionadas con la identificación y gestión no solo de los riesgos, sino también de las respuestas (BID y OEA, 2020).

Como se muestra en los ejemplos anteriores, los cinco estudios de caso sobre la estrategia y reglamentación a nivel nacional en materia de ciberseguridad no abordan específicamente la ciberseguridad en la infraestructura del sector de AyS. En la siguiente sección se analizarán los estudios de caso de Israel y Reino Unido, en los cuales se presenta la estrategia nacional de cada país en términos generales y, específicamente, la normativa en materia de ciberseguridad de la infraestructura del sector AyS.





Desafíos y respuestas a nivel internacional



Los países de todo el mundo conocen los diversos y potenciales riesgos de operar en el ciberespacio, que incluyen no solo los posibles daños que los ataques cibernéticos podrían provocar en la economía y la vida civil, sino también los casos en que los agentes de amenaza intentan alcanzar sus objetivos geoestratégicos a través de interrupciones en línea, lo cual representa riesgos significativos para la IC nacional. A medida que este entendimiento crece, los países invierten más recursos en la implementación de medidas nacionales de ciberseguridad y en controles de seguridad de los SCF, que respaldan los esfuerzos críticos y necesarios para el éxito (Thielemann et al., 2021).

Entendimiento de la importancia de las APP

Dado que los propietarios y operadores de IC son agentes tanto públicos como privados, los ataques podrían tener efectos de amplio alcance. La responsabilidad de proteger estas infraestructuras está en manos de entidades tanto del sector privado como público. Sin embargo, el enfoque principal de ambos sectores es diferente. El sector público considera las infraestructuras a escala nacional y tiende a dedicar mayores esfuerzos a los activos más estratégicos. Según este enfoque, los gobiernos abordan la protección de las IC como un conjunto de sistemas y servicios.

En cambio, el sector privado prioriza las ganancias, el prestigio y los clientes, por lo cual da más valor a la prestación de servicios, la innovación, la reducción de costos y la creación de participación de mercado. En el plano técnico, el sector privado dedica sus esfuerzos a los elementos básicos que están bajo su control directo o sus obligaciones contractuales para la prestación de servicios.

Estos distintos enfoques crean oportunidades para que las APP, tanto a nivel estratégico como técnico, salven estas diferencias y protejan las IC de forma holística. Las organizaciones privadas deberían esforzarse por comprender su función en la protección de las IC, mientras que los gobiernos deberían valorar el conocimiento de expertos que forman parte del sector privado (OEA, 2018).



Estudios de casos internacionales

A continuación, se presentan dos estudios de casos (Israel y Reino Unido) a fin de entender cómo los gobiernos pueden proteger sus IC de las amenazas cibernéticas, con foco en el sector de AyS. Los dos modelos descritos ilustran las reglamentaciones nacionales que abordan los riesgos relacionados con la ciberseguridad.



Estudio de caso No. 1: el modelo israelí

El gobierno de Israel lleva casi tres décadas abordando cuestiones relacionadas con la seguridad de la información y la protección de las infraestructuras informáticas. Desde 1996 aprueba medidas de defensa contra las amenazas cibernéticas (Tabansky, 2011). En Israel se hace mucho hincapié en la regulación y coordinación entre el sector público y el privado. Desde una etapa inicial, el país calificó al sector de AyS como IC y se mostró activo en la concientización sobre los riesgos asociados. Además, las autoridades en ciberseguridad del gobierno asignan recursos nacionales para llevar a cabo revisiones, ejercicios y capacitación de forma periódica, lo que promueve la importancia de centrarse en las capacidades para la protección de la infraestructura del sector de AyS. Estas iniciativas animan a las entidades correspondientes del sector privado a mejorar sus medidas de protección y respuesta.

Reglamentación

El modelo israelí de protección de las infraestructuras contra las amenazas cibernéticas es centralizado: un organismo de supervisión examina de cerca las actividades de seguridad de los operadores de infraestructuras al tiempo que imparte instrucciones directas para la adopción de las medidas necesarias. En 2002 el gobierno israelí trató de definir responsabilidades para los sistemas informáticos del país y, para ello, creó un comité directivo que determinó cuáles serían los organismos que se considerarían críticos y, por lo tanto, necesitaban ciberprotección y lineamientos (Benoliel, 2014). En 2010 el gobierno creó la Autoridad Nacional en Ciberseguridad, actualmente conocida como Dirección Nacional de Cibernética de Israel (INCD, por sus siglas en inglés). La misión de la INCD es formular una política integral de protección del ciberespacio de Israel mediante la supervisión y reglamentación de las actividades gubernamentales generales relacionadas con el ciberespacio desde los puntos de vista civil y de seguridad nacional (Benoliel, 2014).

Bajo su responsabilidad regulatoria, el Ministerio de Energía y Recursos Hídricos de Israel, oficina gubernamental responsable de las infraestructuras del sector del agua y energía, trabaja con empresas privadas de infraestructura para proteger los sistemas informáticos críticos. Los procedimientos redactados por este ministerio ofrecen orientación a las empresas privadas de infraestructura (por ejemplo, gas y electricidad) en la protección de los sistemas digitales críticos que operan.

La Autoridad de Agua y Alcantarillado, creada en 2007, tiene a su cargo la operación del sistema de suministro de agua en el ámbito nacional, local y de los condados. Su misión es preservar las fuentes de agua y mantener las operaciones de abastecimiento, así como responder ante emergencias en situaciones que podrían dañar las infraestructuras del sector de AyS.

La Unidad de Seguridad del Agua, que opera en nombre de la Autoridad de Agua y Alcantarillado en materia de ciberseguridad, se ocupa de las operaciones, gestión y control de los incidentes físicos y digitales causados por el agua, así como de las crisis hídricas. La unidad también se encarga de mejorar las capacidades de los ministerios, agencias nacionales y empresas prestadoras de servicios de suministro de agua (desalinizadoras, plantas potabilizadoras, empresas de suministro de



agua) y participa en la preparación para incidentes en el sector de AyS mediante la organización, suministro de equipos, redacción de procedimientos, práctica y mantenimiento de las normas necesarias para la operación.

La Autoridad del Agua y Alcantarillado de Israel estableció una escala para el nivel de ciberprotección que se exige a las empresas prestadoras de servicios de suministro de agua. El uso de esta escala permite que cada empresa prestadora establezca su propio nivel de sensibilidad y, a partir de eso, se determinan los controles de ciberseguridad necesarios, tal como se indica a continuación:



Instalación o infraestructura de nivel 1

- A. Instalaciones o infraestructuras para el suministro de agua cuyo daño interrumpirá la continuidad operativa del suministro de agua a una población de más de 250.000 residentes
- B. Planta desalinizadora.
- C. Plantas de tratamiento de aguas residuales cuya interrupción puede causar daños graves y duraderos al medioambiente.



Instalación o infraestructura de nivel 2

- A. Instalaciones o infraestructuras para el suministro de agua cuyo daño interrumpirá la continuidad operativa del suministro de agua a una población de menos de 250.000 residentes.
- B. Instalaciones con autoproducción de agua por perforación y cloración.



Instalación o infraestructura de nivel 3

- A. Instalación que no dispone de sistemas informáticos considerados esenciales para el desarrollo de las operaciones de agua y alcantarillado.

La Unidad de Seguridad del Agua es la única autoridad competente para elevar el nivel de criticidad establecido para una instalación después de ponderar las amenazas, la potencialidad de daños a la continuidad de la operación, la disponibilidad de la mano de obra, los costos, etcétera.

Estudio de caso de ataque y respuesta

En abril de 2020 *hackers* maliciosos afiliados a intereses iraníes supuestamente atacaron múltiples estaciones de bombeo e instalaciones de tratamiento de aguas residuales en Israel en un intento por manipular los sistemas de cloración para aumentar las cantidades de cloro en el agua destinada a la población israelí (Srivastava, 2020). Según la información publicada, el ataque iraní se llevó a cabo a través de servidores en los Estados Unidos y Europa a fin de ocultar su origen y reducir las sospechas y alcanzó a controladores de *software* comercial que estaban utilizando programas de CLP para operar las bombas de agua. El acceso a estos CLP se realizó a través de Internet, y de esta manera los atacantes pudieron ingresar y controlar las bombas de agua.

Se informó que el gobierno israelí reaccionó de inmediato y ordenó restablecer las contraseñas de todas las instalaciones de agua y energía del país de todos los sistemas SCADA a fin de evitar futuros ataques. Gracias a la rápida respuesta, no se materializó ningún daño significativo en la calidad del agua (Boubaker, 2021). Luego, se decidió reforzar los controles de seguridad que protegen a los sistemas SCADA —por ejemplo, la desconexión de estos sistemas de Internet— para garantizar el funcionamiento continuo de las instalaciones.



Estudio de caso No. 2: el modelo británico

Reglamentación

El Reino Unido tiene una larga historia del uso de la ciencia y la tecnología con fines de seguridad nacional, y el gobierno implementa una estrategia y política a largo plazo de apoyo a la innovación, la tecnología y las industrias intensivas en conocimiento. La Estrategia de Seguridad Nacional (NSS, por sus siglas en inglés) del Reino Unido (Gobierno del Reino Unido, 2015) definió las amenazas cibernéticas como una categoría de amenaza de primer orden y un riesgo de primer nivel para los intereses del país. Un año después, el Reino Unido publicó su Estrategia Cibernética Nacional para 2016-2021 y posteriormente la actualizó para 2022-2030 (Gobierno del Reino Unido, s.f.).

La estrategia para 2022 incluye cinco objetivos principales:

- Gestionar los riesgos de ciberseguridad.
- Brindar protección contra ataques cibernéticos.
- Detectar incidentes de ciberseguridad.
- Minimizar el impacto de los incidentes de ciberseguridad.
- Desarrollar competencias, conocimientos y cultura en materia de ciberseguridad.

El gobierno británico realiza importantes inversiones para la ejecución del plan de trabajo que le permita alcanzar las metas fijadas en la Estrategia Cibernética Nacional. Solo en 2021, el Reino Unido invirtió £2.600 millones en ciberseguridad. Esta atención prestada a la ciberseguridad se produce después de una serie de ciberataques contra instituciones políticas, partidos y organismos parlamentarios, y de ciberataques en los que se robaron datos de las infraestructuras nacionales.

Un paso más hacia la mejora en ciberseguridad es la reforma institucional cibernética británica que creó el Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés). El NCSC tiene a su cargo la implementación operativa gubernamental de toda la protección en materia de ciberseguridad en el Reino Unido, incluidas aquellas cuestiones que antes estaban bajo la responsabilidad del Centro para la Protección de la Infraestructura Nacional. En 2017 el Departamento de Medio Ambiente, Alimentación y Asuntos Rurales publicó la Estrategia de Ciberseguridad del Sector del Agua para 2017-2021. Los objetivos de esta estrategia se basan en la Estrategia Nacional de Ciberseguridad (NCSS, por sus siglas en inglés) presentada en el Gráfico 9.



Gráfico 9: Estrategia Nacional de Ciberseguridad del Reino Unido



Fuente: Departamento de Medio Ambiente, Alimentación y Asuntos Rurales (2017).

Estudio de caso de ataque y respuesta

Aproximadamente el 40% de los 777 incidentes gestionados por el NCSC entre septiembre de 2020 y agosto de 2021 en el Reino Unido tuvieron como objetivo entidades relacionadas con el gobierno. En mayo de 2021 el Irish Health Service Executive, el servicio público de atención sanitaria de Irlanda, sufrió un ciberataque. Se anunció que los costos de recuperación de ese ataque ascenderían a US\$600 millones (NCSC, 2021).

En estos casos, el NCSC desempeña varias funciones. En primer lugar, en colaboración con otras ramas del gobierno, identifica a los agentes de amenaza y les atribuye los ataques. En segundo lugar, después de detectar un incidente de ciberseguridad, lo analiza para evaluar sus características (evaluación del incidente, según el NCSC). Una vez evaluado el incidente, si se determina que se requiere una mayor intervención del NCSC, se proporciona apoyo tanto por parte de un equipo técnico como de un equipo jurídico. Luego, de ser necesario, el NCSC coordina con entidades internacionales los pasos a seguir. Después de los incidentes, se comparten las conclusiones y se implementan nuevos métodos para hacer frente a ataques similares (NCSC, 2021).





Recomendaciones clave para el sector de agua y saneamiento en América Latina y el Caribe

Recomendaciones clave de ciberseguridad

El direccionamiento hacia la industria 4.0 y la convergencia resultante de la TI y la TO conducen al surgimiento de nuevas amenazas cibernéticas en el sector de AyS. Varias de las organizaciones del sector de AyS, que participaron de las entrevistas durante la preparación de esta publicación, subrayaron que prevén una mayor automatización y digitalización de sus infraestructuras en los próximos 5 a 10 años. Con el aumento de la digitalización y automatización de procesos en el sector de AyS, es imperativo establecer controles de ciberseguridad adecuados para mejorar la resiliencia frente a los ataques cibernéticos y, de este modo, respaldar la fiabilidad, calidad y confianza en estos servicios.

A continuación, se incluye una serie de recomendaciones derivadas de los resultados de la investigación y de las entrevistas realizadas.



Garantizar que los responsables, tanto del ámbito nacional y subnacional como local, describan claramente su visión y definan las metas para alcanzarla

1. Se debe crear una **visión clara y viable de la ciberseguridad** y detallarla en una **estrategia** gubernamental de **ciberseguridad para las IC**. Esta visión debería incluir una gobernanza transparente e idónea, **objetivos** bien definidos y **mensurables**, y una hoja de ruta para alcanzarlos.
2. Es preciso **obtener el apoyo y compromiso del liderazgo nacional del gobierno** para reforzar la ciberseguridad del sector de AyS y otras IC, que incluya el liderazgo proactivo de la agencia nacional de ciberseguridad, el refuerzo de los recursos humanos y técnicos disponibles para el sector y el establecimiento de un sistema de gobierno transparente y capacidades operativas para reglamentar y proteger las IC.





Crear un marco jurídico en el que el sector de AyS sea reconocido como IC

1. El primer paso que debe darse es el **reconocimiento formal del sector de AyS como IC**. En la mayoría de los países de ALC, esto no sucede. Este reconocimiento suele ser un factor clave y necesario para que se asigne al sector la prioridad necesaria no solo en términos presupuestarios sino también de gestión en relación con los desafíos en materia de ciberseguridad. Sin este reconocimiento, el sector de AyS no recibirá la atención adecuada y, más concretamente, no se aplicarán suficientes controles en materia de ciberseguridad.
2. En los últimos años, varios países de ALC modernizaron sus marcos normativos en materia de ciberseguridad, gracias a una mayor concientización sobre la creciente importancia de este tema, en especial, con respecto a los sistemas de las IC. Sin embargo, los esfuerzos legislativos en el ámbito nacional y subnacional en muchos de los países de ALC aún no se tradujeron en una implementación congruente de estrategias y planes de acción en materia de ciberseguridad. Si bien se lograron mejoras en este aspecto, deberían acelerarse aún más las actividades al respecto. Por lo tanto, **se debe priorizar la implementación congruente de estrategias y planes de acción en materia de ciberseguridad, que se centren en las IC**.
3. Al mismo tiempo, varios países de ALC reforzaron sus estructuras institucionales tanto para reducir los riesgos cibernéticos como para mejorar la protección y resiliencia una vez que esos riesgos se materialicen, incluidas las inversiones en procesos, personas y recursos tecnológicos. **Estos esfuerzos y la coordinación interinstitucional son necesarios a escala nacional e internacional** (Saavedra, 2015).





Establecer y priorizar las APP para compartir conocimientos

1. La protección de las IC debe basarse en **asociaciones que reúnan a agentes privados y público-privados**. Gobiernos, propietarios y operadores de IC y proveedores de TIC deben colaborar de forma intersectorial y transfronteriza a fin de gestionar mejor el riesgo (OEA, 2018). Las estrategias eficaces de seguridad y resiliencia de las IC exigen la participación de APP que, a su vez y oportunamente, **intercambien información fiable entre las partes interesadas. Este aspecto es esencial para la protección de las IC** (CISA, 2022).
2. El intercambio de información también aumenta el potencial de respuestas colectivas a las amenazas cibernéticas. Las organizaciones están mejor preparadas para frustrar a los atacantes y métodos de ataque cuando se **comparte información sobre los delincuentes cibernéticos y sus métodos**. Sería prudente que los gobiernos consideren la posibilidad de implementar marcos e incentivos para alentar a las organizaciones de IC a participar en esta actividad (OEA, 2018).
3. Las APP son de extrema importancia en el sector de AyS, ya que se trata del sector que mejor se describe como conservador, debido a que cuenta con muchos profesionales empleados en el área del suministro de agua pero pocos vinculados con ciencias informáticas que puedan abordar los aspectos relacionados con la ciberseguridad que afecta a este campo. Por lo tanto, **la creación de asociaciones entre el conocimiento en ciberseguridad del sector privado y el conocimiento del sector de AyS puede exponer al sector de AyS a las mejores prácticas de la industria y al conocimiento técnico en ciberseguridad**.
4. La efectividad de las APP puede ir más allá de un simple intercambio de información práctica sobre amenazas. Los gobiernos pueden reunir a las distintas partes interesadas para mejorar la seguridad de sus servicios críticos **mediante la creación de grupos de trabajo o comités de consultoría**. Sus áreas de atención podrían incluir la creación de estructuras de coordinación eficaces, procesos y protocolos para el intercambio de información, identificación e intercambio de ideas, enfoques y mejores prácticas para mejorar la seguridad y coordinación internacional (OEA, 2018).





Comprender que las organizaciones públicas y privadas, así como los servicios públicos, deberían desarrollar culturas corporativas que hagan hincapié en la ciberseguridad

1. Se debe **reconocer la ciberseguridad como un riesgo**, al mismo nivel que la seguridad, calidad del servicio, protección del medio ambiente y otras prioridades operativas.
2. Es preciso aumentar la **concientización en ciberseguridad** mediante la creación de una cultura en la materia con la participación de la dirección (por ejemplo, capacitación, ejercicios de simulación, cursos sobre ciberseguridad, etc.).
3. Es necesario **incorporar directivas de seguridad** para las IC en la gobernanza corporativa.
4. Es preciso **adaptarse continuamente a los cambios**. El ámbito del ciberespacio, incluidas las tecnologías, amenazas y vulnerabilidades, cambia rápidamente. Reconocer y adoptar los cambios aumentará el reconocimiento y aceptación del sector público y del privado sobre los esfuerzos a escala nacional para crear ciberresiliencia.



Comprender que las organizaciones públicas y privadas, así como las empresas de servicios públicos, deben establecer y adaptar los pasos prácticos a seguir dentro de la organización antes de implementar los controles de ciberseguridad

1. Se deben **trazar mapas de los riesgos y realizar evaluaciones de impacto** mediante la modelación de los posibles efectos de los ataques cibernéticos, incluidos los que afectan a la vida humana. En ellos se basarán los planes corporativos de continuidad de las actividades y clasificación de datos.
2. Es preciso **trazar mapas e identificar activos, dispositivos y sistemas** que participan en la red de TO/SCI.
3. Es necesario elaborar un **plan anual de ciberseguridad ajustado a un presupuesto** donde se incluya la concientización, capacitación específica de los equipos pertinentes, ejercicios sobre ciberseguridad en toda la empresa, así como el mantenimiento y actualización de las soluciones de seguridad necesarias.
4. Es preciso **prepararse y capacitarse para la gestión de incidentes y la recuperación en caso de desastre** mediante la actualización continua de un plan de respuesta ante incidentes de ciberseguridad.
5. Se deben **implementar requisitos de ciberseguridad** en todos los procesos empresariales y técnicos, adquisiciones, cadena de suministro y contratistas.





Desarrollar soluciones de ciberseguridad para la convergencia de TI y TO de organizaciones y servicios públicos y privados

1. Es preciso **desarrollar una estrategia de seguridad de normas y procedimientos de ciberseguridad pertinentes para los sistemas de TI y TO** (ISO 27001, IEC 64223, etc.), aprobada por la dirección de nivel C, mediante la puesta en marcha de un enfoque holístico en el que la seguridad de la TO, TI, IoT e IIoT se gestione a través de un esfuerzo coordinado.
2. Se deben **controlar y minimizar las interfaces de la red de TO/SCI** con redes externas y terceros. Además, hay que supervisar y controlar periódicamente las interfaces necesarias.
3. Es necesario atribuir **funciones exclusivas al personal de ciberseguridad** que supervisará la ciberseguridad de TI y TO.
4. Se debe **acelerar la convergencia de los métodos de seguridad mediante la compilación de un inventario de todas las soluciones de seguridad de IoT (TO/SCI)** utilizadas en la organización y evaluar la creciente lista de opciones independientes o multifuncionales basadas en plataformas para la interoperabilidad con las herramientas de seguridad de TI de la empresa. Además, es preciso segmentar la red de TO/SCI en diferentes zonas (capa 0, 1, etc.) mediante la implementación de controles de seguridad adecuados (cortafuegos, diodos de comunicación unidireccionales, red de área local virtual [VLAN, por sus siglas en inglés], etc.).



Restringir el acceso a los sistemas en organizaciones y servicios públicos y privados

1. Se deben implementar la **autenticación de usuarios y control de acceso basado en funciones** en los sistemas de procesos críticos.
2. Es preciso **implementar, controlar y restringir el acceso remoto** cuando lo requieran empleados y terceros. Además, hay que limitar el acceso físico a las instalaciones y sistemas al personal autorizado.
3. Es necesario **implementar sistemas de supervisión cibernética y capacidades de detección de amenazas** (por ejemplo, gestión de eventos e información de seguridad [SIEM, por sus siglas en inglés], sistema de detección de intrusiones [IDS, por sus siglas en inglés], etc.).

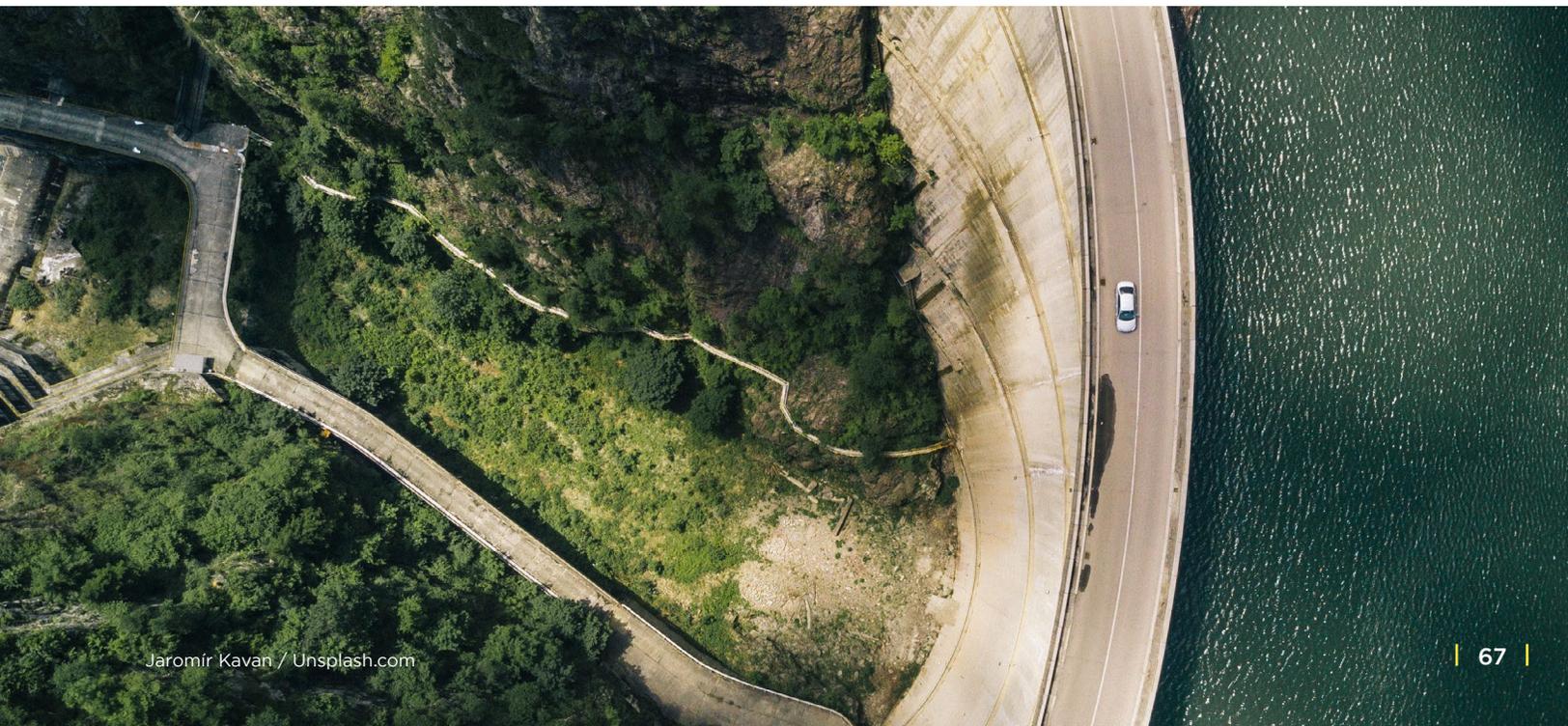


Cuestionario de autoevaluación para analizar el escenario de ciberseguridad de una infraestructura

En cuanto a la medición de la ciberseguridad y formulación de recomendaciones específicas para las distintas entidades, el BID implementó [una herramienta](#) que permitirá a las empresas prestadoras de servicios de suministro de agua y a los gobiernos elaborar una hoja de ruta para la acción. Ofrece una perspectiva general y las medidas que deben adoptarse para mejorar el nivel de madurez de las organizaciones, considerando las diferencias entre la situación actual en materia de ciberseguridad y las mejores prácticas del sector.

La herramienta, que consiste en un **cuestionario de autoevaluación**, permite que las organizaciones evalúen la situación actual de la infraestructura en materia de ciberseguridad, al señalar brechas existentes, y ofrece recomendaciones que sirven de base para la elaboración de un plan de acción concreto a fin de enfrentar las amenazas.

En primer lugar, la herramienta clasifica a la organización para definir tres posibles niveles de riesgo (básico, medio y avanzado), en función de los cuales establece los requisitos de seguridad de la información correspondiente. A continuación, se realiza una **autoevaluación**: se presentan las preguntas correspondientes según el nivel de riesgo elegido y se evalúa la preparación actual de la organización en materia de ciberseguridad con base en el Marco de Ciberseguridad del NIST. Por último, la herramienta calcula una puntuación según las respuestas obtenidas para cada función y categoría del Marco de Ciberseguridad del NIST y ofrece recomendaciones para mejorar el nivel de madurez de la organización.





Referencias





Referencias

- Ablon, L. y A. Bogart. 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Mónica, CA: RAND Corporation. Disponible en: <https://doi.org/10.7249/RR1751>.
- Ali, H. y J. Choi. 2019. A Review of Underground Pipeline Leakage and Sinkhole Monitoring Methods Based on Wireless Sensor Networking. *MDPI Sustainability* 11(15), 4007. Disponible en: <https://doi.org/10.3390/su11154007>.
- Aqualia Group. 2019. The New Reality of Water Management: Industry 4.0. Disponible en: <https://smartwatermagazine.com/news/aqualia/new-reality-water-management-industry-40>.
- Benoliel, D. 2014. Towards a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study. Global Network of Interdisciplinary Internet & Society Research Centers. Haifa Center of Law and Technology (HCLT). The University of Haifa Faculty of Law, julio de 2014. Disponible en: <https://law.haifa.ac.il/wp-content/uploads/2021/10/TOWARDS-A-CYBER-SECURITY-POLICY-MODEL-ISRAEL-NATIONAL-CYBER-BUREAU-CASE-STUDY-Daniel-Benoliel-reviewed-version.pdf>.
- BID (Banco Interamericano de Desarrollo) y OEA (Organización de Estados Americanos). 2016. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. Washington, D. C.: BID y OEA. Disponible en: <https://publications.iadb.org/publications/spanish/viewer/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf>.
- _____. 2020. Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Informe Ciberseguridad 2020. Washington, D. C.: BID y OEA. Disponible en: <https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>.
- Bigelow, S. y B. Lutkevich. 2021. What Is IT/OT Convergence? Everything You Need to Know. *Search IT Operations*. Disponible en: <https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence>.
- Boubaker, K. B. 2021. Water Industry: A Look Back at Twenty Years of Cyber Attacks. *Stormshield*. Disponible en: <https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water>.



- Brangetto, P. y M. Kert-Saint Aubyn. 2015. Economic Aspects of National Cyber Security Strategies. NATO Cooperative Cyber Defence Centre of Excellence. Disponible en: <https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf>.
- Caparros, J. 2021. Top Cyber Threats to Latin America and the Caribbean. *Mandiant*. Disponible en: <https://www.mandiant.com/resources/top-cyber-threats-to-latin-america-and-the-caribbean> (consultado el 21 de mayo de 2022).
- Centro Canadiense de Seguridad Cibernética. 2018. An Introduction to the Cyber Threat Environment. Disponible en: <https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors>.
- Centro Global de Capacidad de Ciberseguridad. 2021. The Cybersecurity Maturity Model for Nations (CMM). Universidad de Oxford. Disponible en: <https://gcscc.ox.ac.uk/the-cmm>.
- Check Point Software. s.f. Top 8 Types of Cyber Attacks. Disponible en: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/> (consultado el 21 de mayo de 2022).
- CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad). 2022. Critical Infrastructure Partnerships and Information Sharing. Disponible en: <https://www.cisa.gov/critical-infrastructure-partnerships-and-information-sharing>.
- _____. 2023. Critical Infrastructure Sectors. Disponible en: <https://www.cisa.gov/critical-infrastructure-sectors>.
- Clark, R., S. Panguluri, T. Nelson y R. Wyman. 2017. Protecting Drinking Water Utilities from Cyberthreats. *Journal of the American Water Works Association* 109. Disponible en: <https://doi.org/10.5942/jawwa.2017.109.0021>.
- Claroty Team82. 2021. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021. Disponible en: https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf.
- CSRC (Centro de Investigación de Seguridad Informática). 2022a. Cyberspace – Glossary. Disponible en: <https://csrc.nist.gov/glossary/term/cyberspace>.
- _____. 2022b. Cyber Attack – Glossary. Disponible en: https://csrc.nist.gov/glossary/term/Cyber_Attack.
- Daigger, G. T., N. Voutchkov, U. Lall y W. Sarni. 2019. The Future of Water: A Collection of Essays on ‘Disruptive’ Technologies That May Transform the Water Sector in the Next 10 Years. Documento para discusión No. IDB-DP-657. Washington, D. C.: BID. Disponible en: <http://dx.doi.org/10.18235/0001666>.
- Deloitte Insights. 2020. Uncovering the Connection between Digital Maturity and Financial Performance. Disponible en: https://www2.deloitte.com/content/dam/insights/us/articles/6561_digital-transformation/DI_Digital-transformation.pdf.
- Departamento de Medio Ambiente, Alimentación y Asuntos Rurales. 2017. Water Sector Security Strategy. Londres: Departamento de Medio Ambiente, Alimentación y Asuntos Rurales. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602379/water-sector-cyber-security-strategy-170322.pdf.
- Deubelli, T. 2019. Hacia una infraestructura resiliente y sustentable: Un estudio de caso sobre la gobernanza de la resiliencia en la infraestructura crítica en Costa Rica. Washington, D. C.: BID. Disponible en: https://publications.iadb.org/publications/spanish/viewer/Hacia_una_infraestructura_resiliente_y_sustentable_Un_estudio_de_caso_sobre_la_gobernanza_de_la_resiliencia_en_la_infraestructura_cr%C3%ADtica_en_Costa_Rica_es_es.pdf.



- ENISA (Agencia de la Unión Europea para la Ciberseguridad). 2023. Critical Infrastructure. Disponible en: <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services>.
- Flashpoint. 2021. From Ransomware to DDoS: Guide to Cyber Threat Actors—How, Why, and Who They Choose to Attack. *Flashpoint*. Disponible en: <https://www.flashpoint-intel.com/blog/guide-to-cyber-threat-actors/>.
- Germano, J. 2019. Cybersecurity Risk & Responsibility in the Water Sector. American Water Works Association. Disponible en: <https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf>.
- Gillette, J., R. Fisher, J. Peerenboom y R. Whitfield. 2002. Analyzing Water/Wastewater Infrastructure Interdependencies. Argonne, IL: Infrastructure Assurance Center, Argonne National Laboratory. Disponible en: <https://publications.anl.gov/anlpubs/2002/03/42598.pdf>.
- Gobierno del Reino Unido. s.f. Government Cyber Security Strategy: Building a Cyber Resilient Public Sector. Londres: Cabinet Office. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf.
- _____. 2015. National Security Strategy and Strategic Defense and Security Review 2015: Third Annual Report. Londres: Cabinet Office. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819613/NSS_and_SDSR_2015_Third_Annual_Report_-_FINAL_2_.pdf.
- Guillaume, F. 2022. The Digital Journey of Water and Sanitation Utilities in Latin America and The Caribbean: What is at Stake and How to Begin. Washington, D.C.: BID. Disponible en: <https://publications.iadb.org/en/digital-journey-water-and-sanitation-utilities-latin-america-and-caribbean-what-stake-and-how-begin>.
- Hernández, J. 2018. Estrategias Nacionales de Ciberseguridad en América Latina. *Global Strategy*. Universidad de Granada. Disponible en: <https://global-strategy.org/estrategias-nacionales-de-ciberseguridad-en-america-latina/>.
- IBM Security. 2021. Cost of a Data Breach Report 2021. Disponible en: <https://www.ibm.com/downloads/cas/OJDVQGRY>.
- IWA (International Water Association). 2022. Global Trends & Challenges in Water Science, Research and Management. Disponible en: <https://iwa-network.org/publications/global-trends-and-challenges-in-water-science-research-and-management/>.
- Kaspersky ICS CERT. 2017a. Península Ibérica y Latinoamérica: estadística de las amenazas para sistemas de automatización industrial, primer semestre de 2017. *SecureList*. Disponible en: <https://securelist.lat/threat-landscape-for-industrial-automation-systems-in-h1-2017/85531/>.
- Kaspersky. 2017b. The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within. *Kaspersky Daily*. Disponible en: <https://www.kaspersky.com/blog/the-human-factor-in-it-security/> (consultado el 26 de septiembre de 2022).
- Lewis, J. 2018. Economic Impact of Cybercrime—No Slowing Down Report. McAfee and the Center for Strategic and International Studies (CSIS). Disponible en: <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf>.



- _____. 2020. The Hidden Cost of Cyber-crime. McAfee and the Center for Strategic and International Studies (CSIS). Disponible en: <https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf>.
- Menashri, H. y G. Baram. 2015. Critical Infrastructures and Their Interdependence in a Cyber Attack – The Case of the U.S. *Military and Strategic Affairs* 7(1). Disponible en: https://www.inss.org.il/wp-content/uploads/systemfiles/5_Menashri_Baram.pdf.
- Mirjana, S., A. Hasanbeigi, N. Neftenov y Tambourine Innovation Ventures. 2020. Uso de tecnologías de la 4RI en agua y saneamiento en América Latina y el Caribe. Nota técnica No. IDB-TN-1910. Washington, D. C.: BID. Disponible en: <https://publications.iadb.org/publications/spanish/viewer/Uso-de-tecnologias-de-la-4RI-en-agua-y-saneamiento-en-America-Latina-y-el-Caribe.pdf>.
- Misión de Israel ante Naciones Unidas en Ginebra. 2021. Water and Cyber Security – Part II. Protection of Critical Water Related Infrastructure. Disponible en: <https://embassies.gov.il/UnGeneva/NewsAndEvents/Events/Pages/20210413-Water-and-Cyber-Security-Part-II.aspx>.
- Moore, S. 2021. Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans. Disponible en: <https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we>.
- Murray, G., M. Johnstone y C. Valli. 2017. The Convergence of IT and OT in Critical Infrastructure. *The Proceedings of the 15th Australian Information Security Management Conference*. Universidad Edith Cowan, Perth, Australia Occidental, 5 y 6 de diciembre de 2017, 149-155. Disponible en: <https://doi.org/10.4225/75/5A84F7B-595B4E>.
- NCSC (Centro Nacional de Ciberseguridad). 2021. NCSC Annual Review 2021. Disponible en: <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021> (consultado el 9 de julio de 2022).
- Observatorio del Crimen de Belice. 2020. National Cybersecurity Strategy 2020-2023. Belice: Gobierno de Belice, 5 de noviembre. Disponible en: <https://bco.gov.bz/download/national-cybersecurity-strategy-2020-2023/>.
- OCDE (Organización para la Cooperación y el Desarrollo Económicos) Agua. s. f. Infographic – What Are the Impacts of Water Pollution? Disponible en: <https://www.oecd.org/fr/sites/oecdwater/infographic-impacts-of-water-pollution.htm>.
- OEA (Organización de Estados Americanos). 2018. Critical Infrastructure Protection in Latin America and the Caribbean 2018. Disponible en: <https://www.oas.org/es/sms/cicte/cipreport.pdf>.
- _____. 2020. Cybersecurity Capacity Review Brazil 2020. Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford. Disponible en: <https://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf>.
- OMS (Organización Mundial de la Salud). 2019. Water, Sanitation, and Hygiene in Health Care Facilities. Seventy-Second World Health Assembly Agenda item 12.5. Disponible en: https://apps.who.int/iris/bitstream/handle/10665/329290/A72_R7-en.pdf?sequence=1&isAllowed=y.
- Pe, J. W. s.f. Assuring Industrial Control System (ICS) Cyber Security. Applied Control Solutions, LLC, p. 14.



- Pimenta Klein, B. e Y. Boguslavskiy. 2020. Latin America Threat Landscape: The Paradox of Interconnectivity. AdvIntel. Disponible en: <https://web.archive.org/web/20230126221027/https://www.advintel.io/post/latin-america-threat-landscape-the-paradox-of-interconnectivity>.
- Prado, P. 2011. The Impact of the Internet in Six Latin American Countries. *Western Hemisphere Security Analysis Center* 6. Disponible en: <https://digitalcommons.fiu.edu/whemsac/6/>.
- Privacy International. 2019. State of Privacy Argentina. 23 de enero. Disponible en: <http://privacyinternational.org/state-privacy/57/state-privacy-argentina>.
- Pursiainen, C., P. Lindblom, P. Francke y Nordregio. 2007. Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection. Estocolmo: Nordregio. Disponible en: <https://www.diva-portal.org/smash/get/diva2:700420/FULLTEXT01.pdf>.
- Rinaldi, S. M., J. Peerenboom y T. Kelly. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 21(6): 11-25. Doi: 10.1109/37.969131.
- Saavedra, B. 2015. Cybersecurity in Latin America and The Caribbean: The State of Readiness for the Defense of Cyberspace. Washington, D. C.: William J. Perry, Centro de Estudios Hemisféricos de Defensa. Disponible en: https://bco.wimp.bz/file_directory/files/cybersecurity/20150730LatinAmericaCaribbeanCybersecurityStateofReadiness.pdf.
- Siboni, G., D. Cohen y A. Rotbart. 2013. The Threat of Terrorist Organizations in Cyberspace. *Military and Strategic Affairs*, 5(3).
- Snow, R. 2022. 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure. Gartner Research. Disponible en: <https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure>.
- Srivastava, M. 2020. Israel-Iran Attacks: 'Cyber Winter Is Coming.' *Financial Times*, 31 de mayo. Disponible en: <https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967>.
- Stankovic, M., A. Hasanbeigi y N. Neftenov. 2020. Uso de tecnologías de la 4RI en agua y saneamiento en América Latina y el Caribe. Washington, DC: BID. Disponible en: <https://publications.iadb.org/es/uso-de-tecnologias-de-la-4ri-en-agua-y-saneamiento-en-america-latina-y-el-caribe>.
- Stouffer, K., V. Pillitteri, S. Lightman, M. Abrams y A. Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82. Gaithersburg, MD: NIST. Disponible en: <https://doi.org/10.6028/NIST.SP.800-82r2>.
- Tabansky, L. 2011. Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs*, 3(2). Noviembre. Disponible en: <https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf>.
- Thielemann, K., W. Voster, B. Pace, R. Contu y R. Hunter. 2021. Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus. *Gartner Research*, 17 de noviembre. Disponible en: <https://www.gartner.com/en/documents/4008351>.
- UIT (Unión Internacional de Telecomunicaciones). 2019. ICT Facts and Figures. Disponible en: <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>.
- Van Raemdonck, N. 2020. Cyber Diplomacy in Latin America. *EU Cyber Direct*. EU Institute for Security Studies. Disponible en: <https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america>.

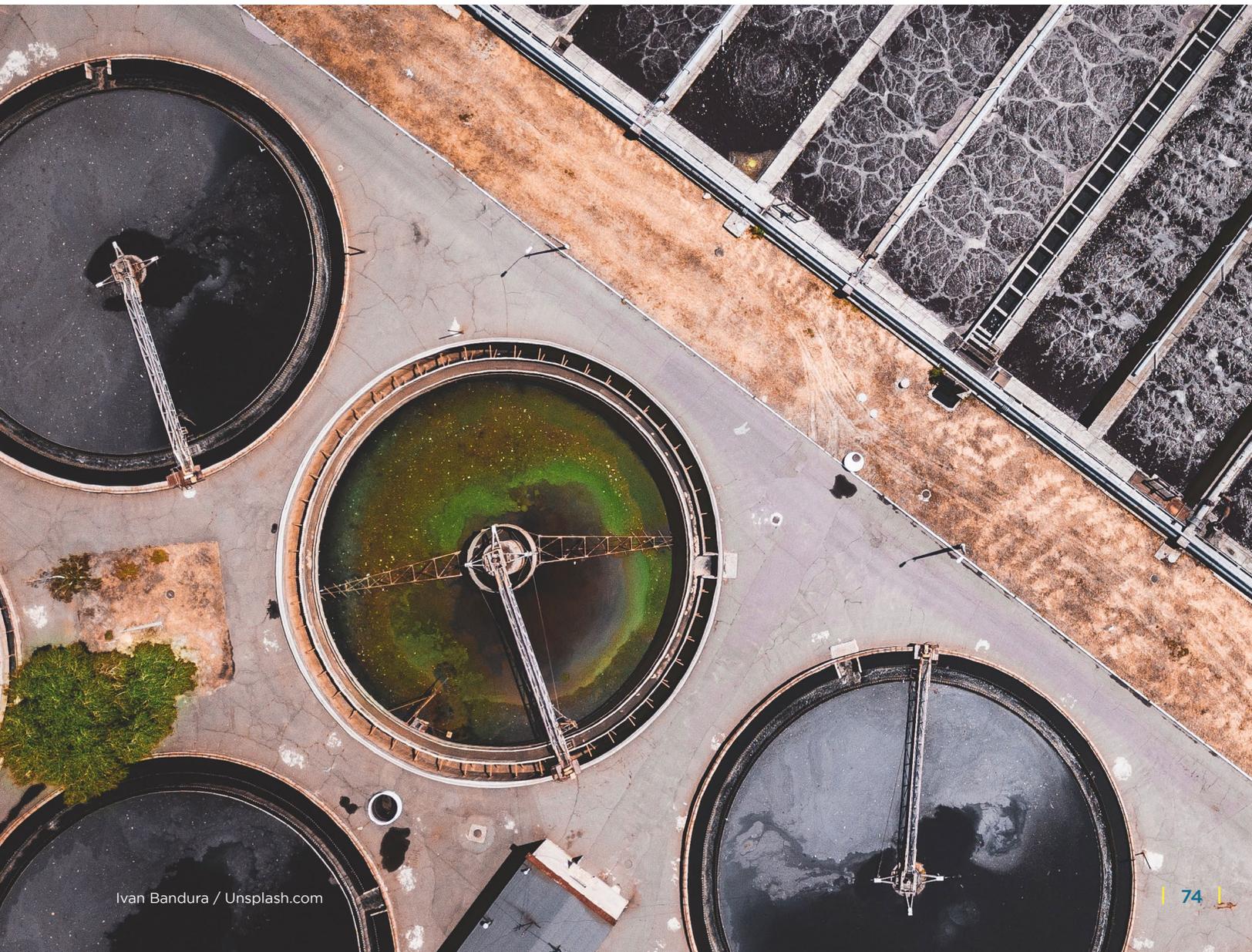


WaterISAC (Water Information Sharing and Analysis Center). 2021. WaterISAC 2021 Survey. Disponible en: <https://www.waterisac.org/2021survey>.

Wesley, C. 2023. What is the CIA Triad? Definition, Explanation and Examples. *TechTarget*. Disponible en: <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>.

Williamson, G. 2015. OT, ICS, SCADA – What’s the Difference? *KuppingerCole Analysts*. Disponible en: <https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference> (consultado el 21 de mayo de 2022).

WSCC (Consejo Coordinador del Sector del Agua de Estados Unidos). 2021. Water and Wastewater Systems, Cybersecurity 2021, State of the Sector. Disponible en: https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinating-Council_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf.





Anexos





Anexo A

Cuestionario para entrevistar al personal de empresas prestadoras de servicios públicos

1. ¿Cómo describiría la organización donde trabaja?
2. Indique el tamaño de la organización donde trabaja en términos de:
 - i. número de instalaciones
 - ii. número de empleados
 - iii. nivel de producción
 - iv. ingresos anuales
3. ¿La organización está reconocida como IC? ¿Infraestructura esencial?
¿Ninguna de las dos opciones?
4. ¿Cuál es la autoridad que regula la actividad de la organización donde trabaja?
5. ¿Cuántas personas trabajan en el departamento de TI? ¿Y en ciberseguridad?
6. ¿Existe un responsable por la ciberseguridad en la organización donde trabaja?
7. ¿Cuál es el presupuesto aproximado (en porcentaje) del departamento de TI de la organización donde trabaja? ¿Y del departamento de ciberseguridad?
8. ¿Se reconoce que la amenaza cibernética es un riesgo?
9. ¿El Estado nacional establece reglamentaciones, lineamientos o requisitos en relación con la ciberseguridad?
10. ¿Conoce algún programa de ciberseguridad para el sector a nivel de políticas o reglamentaciones? Descríbalos.



11. ¿Existen requisitos internos en materia de ciberseguridad?
12. ¿El sector de AyS está reconocido como IC?
13. ¿Sufrió un incidente de ciberseguridad/ataque cibernético? ¿Y un evento operativo/de mantenimiento sin explicación?
14. ¿Con qué frecuencia revisa los controles y procedimientos de ciberseguridad?
15. ¿Dispone de un plan anual en materia de ciberseguridad? En caso afirmativo, ¿qué incluye? (Por ejemplo, capacitación, concientización, *hacking* ético, actualización del inventario de dispositivos, etc.).
16. ¿Cuál es el daño potencial que podría provocar un incidente de ciberseguridad (que no sea un ataque)? (Consecuencias financieras, ambientales, de seguridad pública o de otro tipo).
17. ¿Cuándo se realizó la última auditoría en ciberseguridad? ¿Hay actividades pendientes?
18. ¿Dispone de un programa de capacitación en ciberseguridad para los empleados?
19. ¿Su empresa utiliza métodos seguros de acceso remoto?
20. ¿Cómo describiría los riesgos cibernéticos actuales y futuros a los que se enfrenta el sector de AyS en ALC?
21. ¿Cómo evaluaría el nivel de preparación de su Estado en caso de ataques cibernéticos contra IC? ¿Y en el sector de AyS específicamente? ¿Cómo evaluaría el nivel de preparación de la organización donde trabaja?
22. A su entender, ¿qué país de la región de ALC cuenta con las capacidades más sólidas de gestión de la ciberdefensa en el sector de AyS?
23. ¿Existen herramientas de ciberseguridad desarrolladas para otros sectores (por ejemplo, red eléctrica, oleoductos o gasoductos) que la empresa de servicios públicos donde trabaja haya adaptado para aplicar en el sector de AyS?
24. Si un agente de amenaza comprometiera su activo, ¿cuáles serían los peores escenarios realistas posibles?
25. ¿Qué interconexiones necesitan sus sistemas para funcionar?
26. ¿Desarrolló e implementó procedimientos de respuesta a incidentes que combinen procesos de respuesta de TI y TO?

Anexo B



Cuestionario para entrevistar al personal de entidades reguladoras y agencias federales

1. ¿Cómo describiría la organización donde trabaja?
2. ¿Cuál es el tamaño y los recursos de la unidad de ciberseguridad a cargo de la supervisión del sector de AyS?
3. ¿Cómo describiría los riesgos cibernéticos actuales y futuros a los que se enfrenta el sector de AyS en ALC?
4. ¿Se reconoce que la amenaza cibernética es un riesgo?
5. ¿Cómo evaluaría el nivel de preparación de su país en caso de ataques cibernéticos contra IC y, específicamente, en el sector de AyS?
6. ¿Cómo describiría los riesgos cibernéticos actuales y futuros a los que se enfrenta el sector de AyS en ALC?
7. ¿El gobierno federal implementó reglamentaciones, lineamientos o requisitos en materia de ciberseguridad?
8. ¿Conoce algún programa de ciberseguridad para el sector a nivel de políticas o reglamentaciones? Descríbalo.
9. A su entender, ¿qué país de la región de ALC cuenta con las capacidades más sólidas de gestión de la ciberdefensa en el sector de AyS?
10. ¿El sector de AyS está reconocido oficialmente como IC?
11. ¿Sufrió (o gestionó) un incidente de ciberseguridad/ataque cibernético?
12. ¿Con qué frecuencia revisa los procedimientos y requisitos en materia de ciberseguridad?
13. ¿Dispone de un plan anual en materia de ciberseguridad? En caso afirmativo, ¿qué incluye? (Por ejemplo, capacitación, concientización, ejercicio nacional, etc.).
14. ¿Cuál es el daño potencial de un incidente de ciberseguridad en el sector de AyS (no necesariamente un ataque)? (Consecuencias financieras, ambientales, de seguridad pública o de otro tipo).
15. ¿Existen herramientas de ciberseguridad desarrolladas para otros sectores (por ejemplo, red eléctrica, oleoductos y gasoductos) que la organización donde trabaja haya adaptado para usar en el sector de AyS?

