Revista de Ciencias Ambientales
ISSN: 1409-2158
ISSN: 2215-3896
Universidad Nacional

Concepción Donoso, María
¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica?
Revista de Ciencias Ambientales, vol. 56, núm. 1, 2022, Enero-Junio, pp. 284-297
Universidad Nacional

DOI: https://doi.org/10.15359/rca.56/1.15

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

FORO
¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica?

How important is cybersecurity to achieving water security?

María Concepción Donoso[1]

Resumen

Alcanzar la seguridad hídrica es indispensable para lograr un desarrollo sostenible. La seguridad hídrica implica tener acceso a *cantidades adecuadas de agua de calidad aceptable*, pero también exige salvaguardar el recurso hídrico y disponer de un sector de agua eficiente y sostenible. Hoy, la seguridad de este sector se ve afectada por ataques cibernéticos, los cuales han aumentado exponencialmente en los últimos cinco años. Se estima que cada 39 segundos ocurre un nuevo ataque en algún sitio de la red global. Sin embargo, la ciberseguridad en el sector del agua en América Latina y el Caribe se encuentra en una fase incipiente. Esta vulnerabilidad del sector pone en peligro la seguridad hídrica de cada país. El presente artículo expone una visión amplia del concepto de seguridad hídrica e ilustra la amenaza real de ataques cibernéticos, identificando los diversos elementos que pueden ser objeto de los ciberdelincuentes. Las consideraciones finales apuntan a sugerir acciones de sensibilización del sector del agua ante los peligros de agresiones cibernéticas y adelantar gestiones tendientes a consolidar la ciberseguridad para propiciar o fortalecer una seguridad hídrica sostenible.

Palabras clave: Ataques cibernéticos; sector del agua; seguridad cibernética; seguridad hídrica

Abstract

Attaining Water Security is essential to achieve sustainable development. Water Security implies having access to adequate amounts of water of acceptable quality, but it also requires safeguarding the water resource and having an efficient and sustainable water sector. Today, the security of this sector is affected by cyberattacks. Cyber threats have increased exponentially in the last five years. It is estimated that every 39 seconds a new attack occurs somewhere on the world wide web. However, cybersecurity in the Latin America and the Caribbean water sector is in an incipient stage. This vulnerability of the sector endangers the country's Water Security. This article presents a broad vision of the concept of water security and illustrates the real threat of cyberattacks, identifying the various elements that can be targeted by cybercriminals. The final considerations aim to suggest actions to raise awareness of the water sector in the face of the dangers of cybernetic attacks and to take steps to consolidate cybersecurity to facilitate or strengthen Sustainable Water Security.

Keywords: Cyberattacks; cybersecurity; water sector; water security.

1 Catedrática Fundadora de la Cátedra UNESCO en Seguridad Hídrica Sostenible de la Universidad Internacional de la Florida, Florida, EE. UU. mcdonoso@fiu.edu

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

1. Introducción

Cada día aparece en diferentes medios de comunicación una mayor cantidad de noticias relacionadas con ataques o crímenes cibernéticos. Se estima que el 64 % de las compañías del mundo han experimentado por lo menos un ataque cibernético (Bulao, 2021). De acuerdo con el Centro de Estudios Estratégicos e Internacionales (CSIS, por sus siglas en inglés) entre junio y agosto de 2021 se registraron 26 incidentes significativos de violación de la seguridad cibernética a nivel mundial (CSIS, 2021). Si bien estos están dirigidos a sectores como la banca, empresas varias o secciones específicas de diferentes gobiernos, con mayor frecuencia se observa cómo los sectores productivos y de servicio ven afectados sus sistemas computacionales por incursiones externas de individuos, organizaciones u otros Estados, con fines adversos para la entidad objeto.

El sector vinculado a los recursos hídricos no es inmune a la tendencia observada a nivel mundial, caracterizada por el incremento de ataques cibernéticos de diferente índole. Cabe destacar que los atentados cibernéticos contra este sector pueden afectar no solo sus bancos de información o bases de datos, sino también sus sistemas de alerta temprana, así como las infraestructuras hidráulicas. Por consiguiente, las instituciones vinculadas al sector del agua pueden ser muy vulnerables ante ciber-ataques, si no tienen las políticas necesarias o no cuentan con los sistemas adecuados de seguridad cibernética.

Con base en lo anterior, es importante destacar que, a fin de garantizar la seguridad hídrica de una comunidad, región o país, es necesario que se cuente con mecanismos adecuados y regulaciones idóneas para contrarrestar, o como mínimo disminuir, el impacto de atentados de origen cibernético. Para ello, es necesario que los planes de seguridad hídrica contemplen no solo los aspectos de la cantidad y calidad del recurso, sino que incluyan lineamientos referentes a la seguridad del recurso en sí y de los sistemas e infraestructura propios del sector.

En el presente artículo, se pretende dar una visión ampliada del concepto de seguridad y mostrar la importancia de considerar la seguridad del recurso *per se,* como elemento significativo para alcanzar y mantener la seguridad hídrica. A su vez, se ilustra la amenaza real de ataques cibernéticos y la necesidad de considerar estos incidentes en la planificación de acciones para salvaguardar el capital hídrico, así como para fortalecer la seguridad intrínseca de las entidades del sector del agua en beneficio de las comunidades y diferentes actores; cabe acotar que el sector del agua se refiere a los niveles local y nacional, e incluso transnacional, en el caso de cuencas transfronterizas. Los casos citados como ejemplos para ilustrar planteamientos y conceptos abordados han sido reportados por diversos medios de comunicación.

2. Seguridad hídrica

La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), en el Plan Estratégico del Programa Hidrológico Intergubernamental (PHI) para el periodo 2014-2021 define la seguridad hídrica como

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

> La capacidad de una determinada población para salvaguardar el acceso a cantidades adecuadas de agua de calidad aceptable, que permita sustentar tanto la salud humana como la del ecosistema, basándose en las cuencas hidrográficas, así como garantizar la protección de la vida y la propiedad contra riesgos relacionados con el agua – inundaciones, derrumbes, subsidencia de suelos y sequías" (UNESCO, 2012, p. 5).

En la implementación de esta estrategia, los diferentes actores dentro del sector del agua han focalizado sus esfuerzos en los aspectos relacionados con la cantidad y calidad de agua, principalmente. Durante los últimos años, la Cátedra UNESCO de Seguridad Hídrica Sostenible en el Instituto de Ambiente de la Universidad Internacional de la Florida (FIU, por sus siglas en inglés) (FIU, 2021) dedica esfuerzos dirigidos a llamar la atención de la importancia de salvaguardar el recurso como parte de los planes de seguridad hídrica presentes o en desarrollo, a diferentes niveles.

Para alcanzar la seguridad hídrica es transcendental tomar en consideración que los sistemas hídricos se encuentran expuestos a varios desafíos. Estos retos son de carácter técnico, institucional, político, financiero y relacionados con la información.

Abordar estos desafíos es fundamental para alcanzar los Objetivos de Desarrollo Sostenible (ODS) delineados en la Agenda 2030 de las Naciones Unidas (UN, 2015), en particular el Objetivo No. 6, específicamente dedicado al agua y al saneamiento.

Alcanzar dicho objetivo implica garantizar la disponibilidad de agua y su gestión sostenible, además del saneamiento para todos. Aun cuando ha habido progreso considerable en América Latina y el mundo en relación con el incremento del acceso al agua potable y los servicios de saneamiento, todavía hay 2 400 millones de personas siguen sin acceso a un saneamiento mejorado, y casi 700 millones carecen de fuentes mejoradas de agua potable (Lombana *et al.*, 2021). En respuesta a esta situación, en la última sesión del Consejo Intergubernamental del PHI, reiterando que la seguridad hídrica es reto clave del siglo XXI para alcanzar el desarrollo sostenible, los representantes de los Estados Miembros de esta organización adoptaron el Plan Estratégico "*La ciencia para un mundo con seguridad hídrica en un entorno cambiante*" (UNESCO, 2021). Este Plan Estratégico guiará las acciones de la UNESCO en recursos hídricos a lo largo de la Novena Fase del PHI (2022-2029).

En los últimos 50 años, los avances de la Gestión de los Recursos Hídricos han ido de la mano del progreso cibernético. La transformación digital, conocida hoy como la Cuarta Revolución Industrial, es uno de los procesos clave en las agendas de desarrollo de los países. Al mismo tiempo, la presión ejercida sobre el sector del agua a incursionar cada vez más en la gestión inteligente del agua ha aumentado de manera exponencial, en parte porque el uso de tecnologías inteligentes puede mejorar los servicios brindados y aportar ahorros considerables al sector. Cabe acotar que

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

> la gestión inteligente del agua es una forma de gestión basada en el análisis de la información registrada en tiempo real por distintos tipos de equipos inteligentes, a través de la Internet de las Cosas (*Internet of Things* – IoT) y mediante sensores remotos, combinando esta información/datos con algoritmos. (Donoso, 2021a, p. 5).

Se considera que el uso de estas tecnologías podría ahorrarles a las empresas de servicios públicos de agua hasta US$15 000 millones al año**.**

Aun cuando en el sector del agua los ciber-ataques han sido escasos e incipientes, en comparación con aquellos infligidos a otros sectores, la seguridad del recurso hídrico, así como la del sector, en general, se ve cada vez más amenazada. Estas amenazas, que en un inicio tenían como objetivo principal obtener la información, últimamente se vierten sobre la calidad y disponibilidad del recurso, extendiéndose también a las infraestructuras y procesos operativos del sector. En este contexto, como indicáramos en varias oportunidades, la seguridad hídrica, que incluye la seguridad del recurso hídrico y del sector de aguas, debe considerarse parte integral de la seguridad nacional (Donoso, 2021b, c). Luego, es esencial entender en qué sentido la seguridad cibernética incide en la seguridad hídrica. A su vez, es importante poder establecer como se traducen las amenazas cibernéticas en el contexto de la seguridad hídrica.

3. Seguridad cibernética

A nivel global, el avance de las ciencias computacionales, la tecnología digital y los sistemas de informática implica el aumento de los casos y la sofisticación de los ataques cibernéticos. Innovaciones tales como el Internet de las Cosas, transacciones financieras y pagos móviles usando equipos inteligentes y la computación en la Nube (reconocida en informática por su expresión en inglés, *cloud computing*) dan lugar al incremento del tipo y número de delitos informáticos (Finances Online, 2021). El Foro Económico Mundial reportó que el delito de más rápido crecimiento en el mundo es el ciberdelito (World Economic Forum, 2020). La **Figura 1** muestra el número de incidentes de ciber-ataques, según el ya citado CSIS (2021).

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

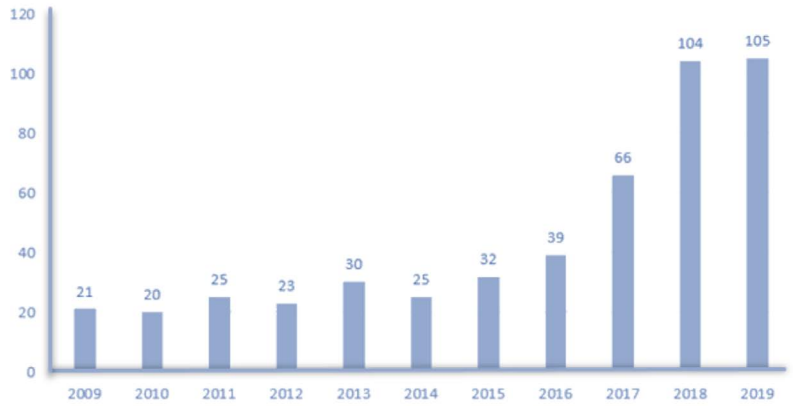

Figura 1. Registro de incidentes de ataques cibernéticos con más de US$1 000 000 de pérdidas. Fuente: CSIS (2021).
Figure 1. Cyber attack incident log with more than $ 1 000 000 in losses. Source: CSIS (2021).

El tipo de ataque informático predilecto de los ciber-delincuentes o "hackers" está relacionado con la demanda de rescate, usando software diseñado para este fin (*ransomware*). El costo del daño por *ransomware* para el año 2021 se estima en US$ 20 mil millones, suma que viene a ser 57 veces mayor que el costo reportado en 2015 (Morgan, 2021). Es interesante observar que más del 50 % de todos los ciber-ataques están dirigidos a pequeñas y medianas empresas. Igualmente, en el sector del agua, se ve que los ataques registrados que presentaremos más adelante también han ocurrido sobre todo en pequeñas y medianas empresas, ya sean públicas o privadas.

La pandemia de COVID-19 forzó la migración casi instantánea de un alto porcentaje de empleados de todo nivel, desde las sedes cotidianas de trabajo a sus hogares. Igualmente, se trasladaron las aulas a las casas. Aun cuando en las residencias de profesionales y ejecutivos se cuenta con cierto grado de sistema de seguridad cibernética, en la gran mayoría de los hogares no solo no se tienen sistemas de seguridad informática, sino que los equipos existentes son compartidos por miembros de la unidad familiar y en muchas ocasiones con vecinos, amigos, o compañeros. Por consiguiente, las organizaciones de todo el mundo debieron, y deben aun, responder de manera proactiva a las amenazas cibernéticas que experimentaron un aumento desde el inicio de la pandemia (Mordor Intelligence, 2020b).

El escenario de la pandemia del COVID-19 se ha convertido en uno de los factores que inducen y modulan no solo el mercado de sistemas y tecnología computacionales, sino también el mercado de la ciberseguridad. En 2020, el valor del mercado de la ciberseguridad fue de US$ 156.24 mil millones, y se proyecta que para 2026 éste será US$ 352.25 mil millones, registrando una tasa de crecimiento anual del 14.5 % durante el periodo de pronóstico de 2021 a 2026 (Mordor Intelligence, 2020a). Un análisis similar desarrollado para el mercado latinoamericano de ciberseguridad cotizó a éste en US$ 4 840 millones en 2020, y para 2026 lo estima en US$

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences
Desde Since 1980

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

9 570 millones, siendo 10.8 % la tasa prevista de crecimiento anual para el período 2021-2026 (Mordor Intelligence, 2020b).

Analizando las estadísticas observadas (Trend Micro, 2020; APWG, 2021; Sophos, 2021; entre otros) se concluye que el escenario particular ligado a la pandemia ha servido de llamado de alerta. Además, se reafirma lo importante que es alcanzar la seguridad hídrica, pero no solo en el contexto del *acceso a cantidades adecuadas de agua de calidad aceptable*, sino también destacando la necesidad de tener un enfoque que apunte a salvaguardar el recurso hídrico y la seguridad del sector del agua, reconociendo la vulnerabilidad ante las amenazas cibernéticas presentes y futuras.

4. Seguridad cibernética para la seguridad hídrica

A fin de evaluar el valor de la seguridad cibernética para la seguridad hídrica es fundamental identificar qué elementos dentro del sector de aguas pueden ser objetivos en peligro.

4.1 Bases de datos

Las bases de datos, así como los repositorios de información, son de particular interés para distintos grupos de agresores cibernéticos. Ratificando el dicho "la información es poder", la incursión no autorizada a bases de datos e información no necesariamente puede ser hecha por delincuentes con intenciones de obtener algún tipo de lucro, sino también puede ser ejecutada por personas pertenecientes a empresas o sectores competidores o grupos políticos de oposición, así como por estados antagónicos o rivales diplomáticos en la búsqueda de hegemonía geopolítica o financiera. Sin embargo, el acceso no autorizado o la extracción de datos y/o información realizada por *hackers* curiosos o ciber-bromistas puede ser tan dañino para el sector del agua como los ciber-ataques delictivos, ya que esto abre brechas en los sistemas de ciberseguridad y expone fallas tecnológicas o de procedimiento a los delincuentes, competidores y público en general.

"Arreglar" las fallas del sistema puede ser posible, aunque en algunos casos podría llevar mucho tiempo o ser muy costoso, pero superar el impacto de la exposición o recuperar la confianza de clientes y/o socios (especialmente aquellos que han compartido datos o información valiosa o sensible) podría, en algunos casos, ser extremadamente difícil e incluso imposible.

Los elementos que puede ser objeto de amenaza cibernética son:

- **Listas de clientes y cuentas.** Estas contienen información personal de los clientes, incluyendo información de carácter confidencial. La incursión a este tipo de información es muy codiciada por delincuentes con intenciones de obtener beneficios económicos.

- **Localización de medidores y otros equipos.** Las amenazas apuntan principalmente a equipos de distribución de aguas, control de flujos y de medición o alteración de características

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

químicas del agua. Muchos de estos equipos se operan en forma remota, algunos forman parte de sistemas inteligentes de gestión del agua y resultan vulnerables.

- **Planes de servicio/mantenimiento.** Los planes pueden ser para infraestructuras y equipos. Este tipo de información es generalmente extraída por hackers y vendida en el dominio de Internet que no es visible para los motores de búsqueda. Este es conocido como la *dark web* o red obscura.

4.2 Servicios y/o productos en línea

Hoy día, las entidades del sector de aguas tienen información o bases de datos desplegada en páginas web, u ofrecen variados servicios en línea a sus clientes, suscriptores, o el público en general. A su vez, como parte del servicio que brindan, funcionarios de entidades del sector mantienen constante intercambio de comunicación con socios y clientes a través del correo electrónico. Estas actividades requieren el uso de tecnologías de la información y la comunicación (ICT, por sus siglas en inglés), lo que hace que las instituciones del sector de aguas sean vulnerables a amenazas cibernéticas.

Los elementos que puede ser objeto de amenaza cibernética son:

- **Presentación de información en tiempo real.** La información disponible puede darse en forma de boletines, tablas numéricas, gráficas o mapas. La información es generalmente recolectada *in situ* por instrumentos/sensores y transmitida a la entidad en forma inmediata, por diferentes medios. El manipular esta información, o impedir su correcto despliegue o el acceso a los usuarios, puede tener diversos impactos negativos, especialmente si ésta se usa en procesos de toma de decisiones.

- **Resultados de modelaje numérico.** La información recolectada en tiempo real o en otra forma, también puede ser usada para alimentar modelos numéricos que simulan el comportamiento de, por ejemplo, ríos, embalses, glaciares, el tiempo o el clima, a mediano o largo plazo. Estos modelos pueden ser de alcance local o global y la información vertida por los mismos apoya la toma de decisiones a nivel de una entidad o del sector, pero en ocasiones también impacta decisiones o políticas de otro sector o inclusive de otra región. Incursiones cibernéticas no autorizadas que afecten la información/datos que alimentan estos modelos, los equipos o sistemas computacionales que los *corren*, o los resultados de estos, pueden impactar no solo a la institución comprometida, sino también los servicios que ésta brinda en su localidad o país, y en algunos casos, a nivel internacional.

- **Alertas.** De los diversos servicios en línea que ofrecen las entidades del sector del agua, las alertas tempranas son cruciales. De particular importancia son las alertas de crecidas repentinas (*flash floods*). El daño por ataques cibernéticos puede extenderse más allá de la entidad responsable y afectar a varias instituciones del sector, así como a sectores diversos

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

dentro del país, al igual que a otras naciones vecinas con las que se comparte una cuenca particular impactada.

4.3 Procesos operativos

La protección de los procesos operativos contra amenazas cibernéticas es un concepto que solo recientemente está empezando a ser considerado en los planes y protocolos operacionales de las entidades del sector del agua. Sin embargo, para alcanzar la seguridad hídrica es fundamental que el sector pueda operar en forma segura, para garantizar "*cantidades adecuadas de agua de calidad aceptable, que permita sustentar el desarrollo y propiciar tanto la salud humana como la del ecosistema*" (UNESCO, 2012*)*.

En tal sentido, la Cátedra UNESCO de Seguridad Hídrica Sostenible dedica esfuerzos y recursos, analizando casos y compartiendo conocimiento relativo a la consideración de la seguridad del recurso hídrico y del sector del agua en los esquemas de seguridad hídrica (**Figura 2**). A su vez, los Centros de Seguridad Hídrica, bajo los auspicios de la UNESCO en México (CERSHI, https://www.cershi.org/en-us/) y Corea del Sur (i-WSSM, https://unesco-iwssm.org/#), están aportando al avance de la expansión de la inteligencia artificial en el sector del agua, así como al desarrollo de los sistemas de gestión inteligente del agua. Ambos temas reiteran la importancia de la seguridad cibernética para proteger los procesos operativos del sector del agua y consolidar la seguridad hídrica.

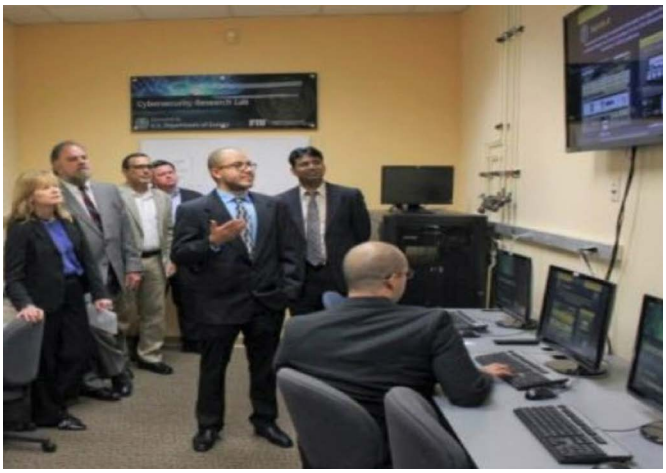

Figura 2. Ejercicio de análisis de amenazas cibernéticas y pruebas de penetración en el Centro de Investigación Aplicada (ARC) de la Universidad Internacional de la Florida. Cortesía: ARC-FIU.
Figure 2. Cyber Threat Analysis and Penetration Testing Exercise at Florida International University Applied Research Center (ARC). Courtesy: ARC-FIU.

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

Los procesos operativos que pueden ser objeto de amenaza cibernética son:

- **Purificación de aguas.** Los procesos de purificación de agua han sido los que han sufrido más atentados cibernéticos. Un ejemplo fue el ataque a una empresa de agua en EE. UU. en el año 2016. Los atacantes accedieron a las válvulas de agua del distrito y a la aplicación de control de flujo que dirige el procesamiento químico del tratamiento de agua. Luego, alteraron la cantidad de sustancias químicas que ingresaban al suministro de agua, lo que afectó la capacidad de producción y tratamiento del agua. Si el ataque no hubiera sido descubierto, la empresa y la comunidad local podrían haber sufrido graves consecuencias (Siggins, 2020). La incursión ilegal a los sistemas de manejo de los procesos de tratamiento de aguas también podría causar catástrofes en los ecosistemas, si aguas contaminadas son vertidas directamente a entornos naturales (ríos, humedales, manglares, etc.).

- **Redes de distribución.** A medida que las comunidades/ciudades hacen la transición a esquemas de gestión inteligente del agua, la vulnerabilidad del sector de agua aumenta frente a amenazas cibernéticas, por cuanto estos esquemas están casi completamente operados por sistemas cibernéticos. Los avances científicos de la inteligencia artificial han sido extraordinarios en los últimos años, pero asimismo ha progresado la sofisticación de los atentados ejecutados.

- **Operación de compuertas.** La manipulación de compuertas en vertederos que regulan embalses podría originar una situación de gran peligro para las comunidades de aguas abajo. De lograr los ciber-criminales controlar la(s) compuerta(s), podría hacer que el agua se desborde sobre la presa y erosione la estructura, situación que pudiera ocasionar la destrucción parcial o total de la presa y causar pérdida de vidas y/o daños irreparables a los ecosistemas cercanos.

4.4 Maquinaria e infraestructura

La maquinaria y la infraestructura que posee el sector del agua a nivel global están valorados en miles de millones de dólares. El daño que resulte a maquinaria o infraestructura por ciber-ataques puede implicar pérdidas millonarias y afectar servicios por extensos periodos, pero también puede comprometer al recurso agua, contaminándolo o desperdiciándolo en forma incontrolada, más allá del impacto que pueda causar a seres humanos y a los ecosistemas naturales.

Los elementos que puede ser objeto de amenaza cibernética son:

- **Maquinaria/equipos.** En la actualidad, la mayor parte de la maquinaria y equipos que se usan en el sector del agua son operados a través de sistemas computacionales, de diferente grado de complejidad. El ataque relativamente reciente a empresas del sector del agua en Israel fue diseñado para comprometer los sistemas de control de estaciones de bombeo, los

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

sistemas de alcantarillado, las plantas de aguas residuales y las bombas de ciertos sistemas agrícolas. El incidente tenía como objetivos finales aumentar el cloro y otros productos químicos en el agua a niveles dañinos, e interrumpir el suministro de agua durante una ola de calor (Weinberg, 2021).

- **Presas.** Las presas son infraestructuras intrínsecas del sector de aguas. Como ejemplo de ciber-ataques tenemos el caso del Bowman Dam (estado de Nueva York). El ataque ocurrió en diciembre de 2015, cuando el sistema estaba conectado a un módem celular que se encontraba en mantenimiento (Assante y Lee, 2016). Los "hackers" usaron la conexión de módem desprotegida y la falta de controles de seguridad para penetrar los sistemas de la presa.

- **Sistemas de riego.** Los sistemas de riego, quizás por su ubicación física, aún se manejan en forma casi manual. Sin embargo, con el avance de la *agricultura eficiente* y la inversión en sistemas inteligentes de control de riego, la posibilidad de que este subsector sea afectado por amenazas cibernéticas aumenta exponencialmente.

- **Vías de navegación.** Numerosas vías de navegación, como el canal de Panamá (**Figura 3**) o el sistema de los Grandes Lagos, forman partes de sistemas multipropósito complejos, vinculados total o parcialmente con el sector del agua. La seguridad de los sistemas cibernéticos y de manejo de la vía son de vital importancia, pues de ser exitosos determinados ataques cibernéticos, los efectos que éstos produzcan serían nefastos no solo para la empresa o el país, sino también para la navegación y el comercio marítimo mundial. Los impactos de cualquier tipo de ataque pueden afectar la operación del canal principal, así como los sistemas naturales que se encuentran en la cuenca de la vía y sus alrededores.

Figura 3. Vista de la de nueva sección ampliada del Canal de Panamá.
Figure 3. View of the new enlarged section of the Panama Canal.

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

5. Propuesta para la acción y consideraciones finales

Pese al aumento de casos registrados de delincuencia cibernética en el sector del agua, la ciberseguridad en América Latina y el Caribe se encuentra en una fase incipiente. La disparidad en cuanto a recursos y capacidades para abordar el tema de la ciberseguridad entre las entidades del sector es enorme. Además, la inclusión de elementos de seguridad *per se* en el abordaje de la seguridad hídrica es igualmente incipiente en la región.

Por tanto, es necesario implementar acciones en apoyo al avance de la seguridad cibernética en el sector, entre las que figuran las siguientes:

- **Aumentar esfuerzos para alertar al sector del agua.** Algunas organizaciones (internacionales y nacionales, gubernamentales y ONGs), empresas del sector (públicas o privadas), compañías y consultoras relacionadas con la informática, así como instituciones académicas (entre ellas la Cátedra UNESCO en FIU) han dedicado esfuerzos considerables para sensibilizar al sector en relación con la importancia de la seguridad cibernética. Sin embargo, estas campañas son insuficientes para llenar el gran vacío que existe en torno a esta temática, por lo que se requieren mayores esfuerzos.

- **Desarrollar y/o adecuar políticas y regulaciones.** Si bien la mayoría de los estados de América Latina y el Caribe tienen políticas y leyes en torno a la cibernética, es preciso en muchos casos adaptar las mismas a los avances tecnológicos. Esta tarea, aun siendo difícil por la dinámica particular de los procesos legislativos, es crucial para poder tener la base legal necesaria para atender las amenazas de hoy. A su vez, las empresas del sector requieren desarrollar y/o actualizar sus políticas y protocolos en ciberseguridad.

- **Propiciar y fortalecer la colaboración entre instituciones y expertos.** En este sentido, organismos intergubernamentales de la región, como la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), están emprendiendo acciones conjuntas para apoyar los esfuerzos de los estados para contrarrestar las amenazas cibernéticas. Pese a esto, se precisa ampliar y fortalecer el intercambio de experiencias entre profesionales del agua y expertos en ciberseguridad.

- **Promover y apoyar la innovación**. Aun cuando existen actividades conjuntas (Norte-Sur y Sur-Sur) de investigación y desarrollo tecnológico, es crucial ampliar y formalizar iniciativas de esta naturaleza en áreas de incidencia en la seguridad cibernética, tales como en inteligencia artificial, internet de las cosas, software y hardware, entre otros.

- **Contribuir al incremento de la oferta académica formal y de oportunidades de capacitación en ciberseguridad.** La UNESCO, a través de su red de Centros y Cátedras, en colaboración con instituciones de educación superior, están diseñando y ofreciendo nuevos programas de grado y postgrado, así como programas para profesionales. Aun así, se requiere expandir las acciones más allá del ámbito de la educación formal.

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

Considerando la información aquí aportada, se observa que las amenazas cibernéticas están escalando rápidamente. En consecuencia, se subraya que la resiliencia cibernética, o ciber-resiliencia, en la realidad actual pasa a ser una necesidad importante, en vez de una mera opción funcional. Igualmente, los planteamientos y ejemplos presentados demuestran que la incidencia de ciber-ataques en el sector del agua compromete la seguridad de sus bases de información y datos, procesos operacionales y estructuras.

Al recapacitar acerca de las múltiples formas en que los ciber-ataques pueden impactar el sector del agua, así como al reflexionar en torno a cómo se ve afectada la cantidad y calidad del recurso, se concluye que la ciberseguridad es importante para garantizar la seguridad hídrica sostenible. En consecuencia, se recomienda que las estrategias y planes de seguridad hídrica contemplen las amenazas al agua, es decir la seguridad *per se* de los recursos hídricos, y por consiguiente se aborden aspectos de ciberseguridad. En conclusión, se deben multiplicar los esfuerzos para consolidar la ciberseguridad en el sector del agua, a fin de fortalecer la seguridad hídrica sostenible.

6. Referencias

APWG. (2021). *Phishing Activity Trends Report 4th Quarter 2020*. https://apwg.org/trendsreports/

Assante, M. & Lee, R. M. (2016). *Deconstructing the Reports of Iranian Activity against the Power Grid and New York Dam*. https://www.sans.org/webcasts/deconstructing-reports-iranian-activity-power-grid-york-dam-101327/

Bulao, J. (2021). *How Many Cyber Attacks Happen Per Day in 2021?*. https://techjury.net/blog/how-many-cyber-attacks-per-day/

Center for Strategic and International Studies (2021). *Inside Cyber Diplomacy*. https://www.csis.org/podcasts/inside-cyber-diplomacy

Donoso, M. C. (2021a). *Hacia una definición de la gestión inteligente del agua*. [White paper - UNESCO Chair on Sustainable Water Security at the Institute of the Environment]. Florida International University

Donoso, M. C. (2021b). *Cybersecurity for Water Security*. [White paper - UNESCO Chair on Sustainable Water Security at the Institute of the Environment]. Florida International University

Donoso, M. C. (2021c). *La ciberseguridad en la gestión inteligente del agua*. [Conferencia Magistral en el Curso en línea "Inteligencia artificial y transformación digital para la Seguridad Hídrica. UNESCO PHI-LAC, CODIA- España, y CERSHI- México]. https://events.unesco.org/event?id=3512548774&lang=3082

Finances Online. (2021). *Cybersecurity Statistics*. https://financesonline.com

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

Florida International University (2021). *UNESCO Chair on Sustainable Water Security*. https://environment.fiu.edu/where-we-work/freshwater/unesco-chair/

Lombana Cordoba, C., Saltiel, G., Sadik, N., & Pérez Peñalosa, F. (2021). The Utility of the Future [Diagnostic Assessment and Action Planning Methodology Working Paper]. Banco Mundial.https://documents1.worldbank.org/curated/en/796201616482838636/pdf/Utility-of-the-Future-Taking-Water-and-Sanitation-Utilities-Beyond-the-Next-Level.pdf

Mordor Intelligence. (2020a). *Cybersecurity market – growth, trends, COVID-19 impact, and forecasts (2021 – 2026)*. https://www.mordorintelligence.com/industry-reports/cyber-security-market

Mordor Intelligence. (2020b). *Latin America Cyber Security Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)*. https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

Morgan, S. (2021). *Report: Cyberwarfare in the C-Suite*. https://1c7fab3im83f5gqiow2q-qs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Siggins, M. (2020). *Major SCADA attacks and what you can learn from them*. https://www.dps-tele.com/blog/major-scada-hacks.php

Sophos. (2021). *SOPHOS 2021 Threat Report: Navigating cybersecurity in an uncertain world*. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

Trend Micro (2020). *Developing Story: COVID-19 Used in Malicious Campaigns*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains#:~:text=COVID%2D19%20is%20being%20used,as%20a%20lure%20likewise%20increase.

UNESCO. (2012). *Octava fase, Seguridad hídrica: respuestas a los desafíos locales, regionales y mundiales: plan estratégico, PHI-VIII (2014-2021)*. https://unesdoc.unesco.org/ark:/48223/pf0000218061_spa

UNESCO. (2021). Science for a Water Secure World in a Changing Environment. The ninth phase of the Intergovernmental Hydrological Programme 2022-2029. https://en.unesco.org/sites/default/files/2020-10_08_ihp-ix_2nd_order_draft_by-2.pdf

United Nations (2015). *Transforming our world: the 2030 Agenda for Sustainable Development*. [Resolution adopted by the General Assembly on 25 September 2015]. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E

Revista de
CIENCIAS AMBIENTALES
Tropical Journal of Environmental Sciences

Revista de Ciencias Ambientales (Trop J Environ Sci)
e-ISSN: 2215-3896
(Enero-Junio, 2022) . Vol 56(1): 284-297
DOI: https://doi.org/10.15359/rca.56-1.15
Open Access: www.revistas.una.ac.cr/ambientales
e-mail: revista.ambientales@una.ac.cr
Donoso M..

Weinberg, A., (2021). *Analysis of the top 11 cyberattacks on critical infrastructure.* https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure

World Economic Forum (2020). *The Global Risks Report 2020*. https://www.weforum.org/reports/the-global-risks-report-2020