Deloitte.

Ciberataques en sistemas industriales

Más allá de las pérdidas económicas

Introducción

América Latina está experimentado una transformación digital acelerada que comenzó en los últimos años, impulsada por la adopción masiva de tecnologías de comunicación.

Este avance ha traído consigo innumerables beneficios económicos y sociales; sin embargo, también ha expuesto a los países de la región a una creciente ola de ciberamenazas que ponen en riesgo la seguridad de infraestructuras industriales, incluyendo las infraestructuras críticas nacionales, empresariales y los ciudadanos.

Las infraestructuras industriales son aquellas instalaciones físicas y sistemas tecnológicos destinados a la producción, transformación o distribución de bienes y servicios —como fábricas, plantas energéticas o redes de transporte . Por otro lado, las infraestructuras críticas son aquellas cuya interrupción o destrucción tendría un impacto grave en la seguridad, en la economía o en la salud pública de un país —como redes eléctricas, sistemas de agua potable, telecomunicaciones o servicios de emergencia. Aunque pueden coincidir en algunos casos, la diferencia clave radica en el nivel de dependencia social y en el riesgo asociado a su falla.

En este contexto, la convergencia entre las tecnologías de la información (TI) y las tecnologías operacionales (*OT*, por sus siglas en inglés) —que operan infraestructuras críticas, entre otras—, ha ampliado la superficie de ataque, permitiendo que actores maliciosos accedan a sistemas de control industrial, redes de automatización y dispositivos *IoT* (internet de las cosas).

El papel de los responsables de ciberseguridad, que antes eran vistos como guardias de seguridad únicamente para las TI empresariales, ha ido evolucionando hacia uno que ayude a salvaguardar toda la organización, desde las operaciones comerciales y administrativas, hasta las operaciones industriales, al tiempo que respalda la innovación, la seguridad e integridad tanto de la información como de los empleados, la sostenibilidad de las operaciones y el futuro del negocio.

Riesgo de no proteger los entornos de *OT*

Algunos de los ciberataques más sofisticados de las últimas décadas son:

Junio 2010

Un espía sumamente sofisticado aparece en los sistemas informáticos y fija su objetivo: infraestructuras críticas y entornos industriales en Irán, como centrales nucleares o plantas de energía. El gusano informático *Stuxnet* se instala en los sistemas para robar información. El *malware* es catalogado como el más desarrollado e innovador, así como la primera arma de guerra cibernética (...) Analistas y expertos afirmaron que *Stuxnet* retrasó el programa nuclear iraní provocando grandes daños físicos[1].

Mayo 2017

Sistemas computacionales resultan afectados en toda Europa. Archivos encriptados y usuarios sin acceso al administrador. Miles de empresas quedan paralizadas debido a un *ransomware* en la red llamada *WannaCryptor* o *WannaCry* (...) El *malware* se coló por una vulnerabilidad de un parche de seguridad instaurado en el sistema operativo Microsoft Windows, que infectó a más de 230 mil equipos, entre ellos, servidores en empresas de todos los tamaños y hospitales que perdieron la información histórica de sus pacientes[2].

Mayo 2021

El grupo de *ransomware DarkSide* compromete los sistemas de un operador de un oleoducto clave en Estados Unidos. La compañía detiene sus operaciones y genera una crisis en el suministro de combustible en la Costa Este del país (...) El ataque resaltó la interdependencia entre TI y *OT*. Pese a que el *malware* no afectó directamente los sistemas industriales, la empresa decidió suspender operaciones para evitar una posible propagación en sus sistemas operacionales[3].

Estos son solo algunos ejemplos de una realidad a la que nos enfrentamos: en el mundo se generan cada vez más ciberataques sofisticados y dañinos, con impactos profundos en la seguridad digital y en las finanzas de las víctimas. Son eventos que resaltan la creciente importancia de la ciberseguridad y la necesidad urgente de estar preparados para enfrentar amenazas.

Con el paso de los años, la ciberseguridad en los sistemas de tecnologías operativas o de la operación —*Operational Technology* (*OT*)— ha dejado de ser una opción y se ha convertido en un componente esencial tanto para la continuidad operativa, como para la seguridad de los empleados y la resiliencia del negocio. Cada día, las infraestructuras críticas y los entornos industriales están más conectados y son más dependientes de la tecnología; sin embargo, las amenazas cibernéticas también han evolucionado: son más sofisticadas y perjudiciales.

Las infraestructuras críticas son objetivos prioritarios para los ciberdelincuentes debido a su importancia estratégica y al impacto que su interrupción puede causar en la sociedad. Los ataques pueden tener consecuencias catastróficas, desde cortes de energía masivos hasta interrupciones en el suministro de agua potable y servicios de salud. Un informe de la Comisión Económica para América Latina y el Caribe (CEPAL) destacó que, entre 2020 y 2022, se registró un aumento significativo en los ciberataques dirigidos a infraestructuras críticas en diez países de la región[4].

Dichos ataques son los que, además de buscar interrumpir servicios esenciales, pretenden obtener información sensible y ejercer presión económica o, incluso, política. Esta última característica, de acuerdo con la Organización de las Naciones Unidas (ONU), afecta por igual a entidades de los sectores público y privado, ya que van de lo financiero a lo simbólico[5]. El organismo puntualiza que los ciberataques de carácter político pueden estar orientados a tener una mayor visibilidad —y con un alcance que puede ser mundial— por *hackers* que buscan fama. Asimismo, los objetivos gubernamentales pueden ser más atractivos para los *"hacktivistas"* que se conducen por razones políticas o ideológicas; es decir, aunque los métodos de los ataques son similares o idénticos, las motivaciones pueden ser diferentes.

A menudo, los sistemas *OT* controlan maquinaria pesada y procesos industriales que, si son manipulados maliciosamente, pueden causar accidentes graves y poner en peligro vidas humanas (como sucedió

en 2010 con el *malware Stuxnet*, al infectar sistemas de control y alterar la velocidad de las centrifugadoras, retrasando el programa nuclear iraní y generando un peligro latente de explosiones o de fuga de material radiactivo). Por lo tanto, proteger estos sistemas, además de ser una cuestión de seguridad laboral, es una responsabilidad corporativa.

Entre los impactos más significativos por ataques de ciberseguridad en *OT*, detallamos los siguientes:

Riesgo de producción paralizada.

Uno de los impactos más inmediatos y perjudiciales de un ciberataque en sistemas *OT* es la interrupción de la producción. Este tipo de sistemas controla procesos industriales esenciales y, cuando son comprometidos, pueden detener operaciones completas. Esto no solo resulta en pérdidas económicas directas, debido a la interrupción de la producción, sino que también puede afectar la cadena de suministro, retrasar entregas y generar costos adicionales en términos de tiempo y recursos necesarios para restablecer las operaciones. En industrias donde el tiempo de inactividad se mide en dólares, las pérdidas pueden ser desmesuradas.

Daños a la reputación

La reputación de una empresa es uno de los activos más valiosos y, a su vez, más vulnerables. Un ciberataque exitoso, especialmente uno que comprometa la seguridad de los sistemas *OT* y cause interrupciones significativas, puede erosionar rápidamente la confianza de clientes, socios y del público en general. La cobertura mediática negativa y la percepción de que una empresa no puede proteger adecuadamente sus activos pueden llevar a la pérdida de clientes y contratos, así como a una disminución del valor de la marca. La recuperación de la reputación dañada puede llevar años y requerir inversiones sustanciales en relaciones públicas y *marketing*.

Amenazas a la seguridad física.

Los sistemas *OT* están directamente vinculados a la seguridad física de los empleados y de la ciudadanía. Un ataque cibernético que manipule o dañe estos sistemas puede tener consecuencias como explosiones, derrames de sustancias químicas tóxicas, fallos en equipos de seguridad y otros incidentes que pongan en riesgo la vida y la integridad física de las personas, así como del medio ambiente en el que opera.

Un ejemplo documentado en esta década es la amenaza ocurrida en febrero de 2021 en Florida, Estados Unidos[6]. Con el *software* de acceso remoto *TeamViewer*, un hombre ingresó a los sistemas de control de la planta de tratamiento de agua en la ciudad de Oldsmar, donde intentó aumentar la cantidad de hidróxido de sodio (también conocido como sosa cáustica o lejía) en el suministro de agua, a niveles peligrosamente altos[7]. El presunto atacante no logró su objetivo porque un operador de la planta notó el aumento inusual en la dosificación de hidróxido de sodio y rápidamente revirtió el cambio, evitando así cualquier daño a la población.

Sanciones regulatorias

El incumplimiento de las regulaciones de ciberseguridad puede resultar en sanciones regulatorias. Hay normativas que establecen requisitos estrictos para la protección de infraestructuras críticas, y las organizaciones que no las cumplan pueden enfrentar multas. Además, el incumplimiento conduce a una mayor supervisión regulatoria y a la imposición de medidas correctivas obligatorias, lo que puede aumentar los costos operativos y afectar la eficiencia de la empresa.

La importancia de las regulaciones

En el mundo, las regulaciones y los estándares de ciberseguridad se han vuelto más estrictos y específicos. Por ejemplo, la Directiva *NIS2* de la Unión Europea exige a los operadores de servicios esenciales y proveedores de servicios digitales adoptar medidas de seguridad más rigurosas y reportar incidentes significativos[8]. La serie de normas *IEC* 62443 —emitida por la Comisión Electrotécnica Internacional (*IEC*, por sus siglas en inglés)— proporciona un marco para la seguridad de los sistemas de automatización y control industrial, abordando aspectos como la evaluación de riesgos, la gestión de vulnerabilidades y la respuesta a incidentes. Por su parte, estándares como el *NERC CIP* (*North American Electric Reliability Corporation Critical Infrastructure Protection*) son obligatorios para las empresas del sector eléctrico en Norteamérica y establecen requisitos detallados para proteger los sistemas de control y redes de comunicación.

En Latinoamérica, por su parte, no todos los países cuentan con leyes en materia de ciberseguridad y normas que protejan las infraestructuras críticas. Si bien la mayoría ha llevado a cabo esfuerzos para establecer estrategias y políticas nacionales[9], países como Colombia, Chile y Perú cuentan con las siguientes leyes:

Colombia. La *Ley 1273* de 2009 protege la información y los datos. Esta ley es aplicable a *OT* en la medida que los sistemas están interconectados, dada la convergencia de IT/*OT*. Además, preserva los sistemas de tecnologías de la información y las comunicaciones:

> Con ella, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones[10].

Chile. La *Ley 21663* protege la ciberseguridad y la infraestructura crítica de la información. Su aplicación en OT tiene como objetivo proteger los sectores críticos de la economía:

> El Estado velará por que todas las personas puedan participar de un ciberespacio seguro, por lo que otorgará especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques[11].

Perú. El Reglamento para la gestión de seguridad de la información y ciberseguridad, aprobado en 2021, requiere a las empresas contar con un entorno seguro y confiable:

> Reglamento para la gestión de seguridad de la información y ciberseguridad, el cual tiene por objetivo requerir a las empresas un entorno seguro y confiable para la provisión de productos y servicios a sus usuarios; y, que les permita estar preparadas frente al incremento de los riesgos asociados a la seguridad de la información producto del creciente avance en las tecnologías, la mayor interconectividad entre las empresas y el auge de la transformación digital[12].

En México, si bien se cuenta con un marco legal que aborda distintos aspectos relacionados con la seguridad informática y la protección de datos, carece de una ley específica de ciberseguridad. Desde el Congreso han surgido iniciativas encaminadas a fortalecer dicha materia; no obstante, ninguna propuesta legislativa ha llegado a concretarse[13].

México, como la segunda economía más grande de América Latina, ha avanzado significativamente tanto en inversión de automatización industrial, como en digitalización de procesos productivos. Sin embargo, existe una creciente amenaza a la que están expuestas las empresas, especialmente aquellas que no han implementado medidas de seguridad adecuadas en sus sistemas *OT*. Durante el tercer trimestre de 2024, las organizaciones en el país experimentaron un promedio de 3,124 ataques cibernéticos semanales, lo que representa un aumento de 78%, en comparación con el mismo periodo del año anterior[14].

Convergencia de TI y *OT*, un nuevo desafío en ciberseguridad

A medida que las redes *OT* se integran más con las tecnologías de la información y se conectan a internet, aumentan las superficies de ataque, exponiendo estos sistemas a riesgos cibernéticos. La convergencia de TI y *OT* es una tendencia significativa que está moldeando el campo de la ciberseguridad, pues, históricamente, ambos entornos actuaban de manera aislada. Ahora, su integración está aumentando debido a los beneficios operativos y económicos que ofrece, como la optimización de procesos y la mejora en la toma de decisiones. No obstante, esta convergencia también introduce nuevas vulnerabilidades, ya que los sistemas *OT* están ahora expuestos a amenazas que antes eran exclusivas del ámbito TI.

Las diferencias clave entre TI y *OT* son fundamentales para comprender cómo deben ser abordadas y gestionadas en términos de ciberseguridad. Mientras que ambos dominios comparten el objetivo de proteger los sistemas y los datos, las prioridades y los enfoques varían de forma significativa a causa de sus diferentes funciones y contextos operativos. A continuación, se detallan las principales diferencias destacando la importancia de la disponibilidad y la seguridad de los sistemas físicos en *OT*:

Tecnología de la Información (TI)	Tecnología Operativa (*OT*)
Prioridades de seguridad	
La confidencialidad, integridad y disponibilidad de los datos son las principales prioridades de seguridad. La confidencialidad se centra en proteger los datos sensibles de accesos no autorizados, la integridad asegura que los datos no sean alterados o destruidos de manera indebida, y la disponibilidad garantiza que los sistemas y datos estén accesibles cuando se necesiten.	La disponibilidad y seguridad de los sistemas físicos son la prioridad absoluta. A diferencia de TI, la disponibilidad contempla intrínsecamente a la integridad y se refiere a la capacidad de los sistemas para operar continuamente sin interrupciones y de manera confiable. La seguridad física se enfoca en proteger los equipos, instalaciones y personas de daños o peligros causados por fallos en los sistemas de control industrial. La confidencialidad de los datos, aunque importante, no es tan prioritaria como en TI.
Naturaleza de los sistemas	
Los sistemas TI incluyen servidores, aplicaciones, bases de datos, redes y dispositivos de usuario final. Estos sistemas son diseñados para gestionar información y soportar operaciones empresariales, como finanzas, recursos humanos y ventas. Los ciclos de actualización y parches en TI son frecuentes y necesarios para mantener la seguridad y la funcionalidad.	Los sistemas *OT* comprenden controladores lógicos programables (*PLC*, por sus siglas en inglés), sistemas de control distribuido (*DCS*, por sus siglas en inglés), sistemas *SCADA*, sensores y actuadores que gestionan y controlan procesos físicos en entornos industriales. Estos sistemas están diseñados para operar en tiempo real y tienen ciclos de vida más largos que los sistemas TI. Las actualizaciones y parches son menos frecuentes, debido a la necesidad de asegurar la continuidad operativa y de evitar interrupciones en los procesos industriales.
Entorno operativo	
Suele ser más flexible y adaptable a cambios. Los sistemas TI operan en redes corporativas que pueden ser segmentadas y protegidas mediante *firewalls*, antivirus y otras soluciones de ciberseguridad. La gestión de estos entornos se centra en la protección de la información y la continuidad de las operaciones empresariales.	Es más rígido y sensible a cambios. Los sistemas *OT* operan en entornos industriales donde los procesos físicos deben ser monitoreados y controlados en tiempo real. La prioridad es mantener la disponibilidad y seguridad de estos sistemas para prevenir interrupciones en la producción y garantizar la seguridad física. Las soluciones de ciberseguridad para *OT* deben ser específicas y cuidadosas para no interferir con los procesos operativos.
Impacto de las interrupciones	
Las interrupciones en los sistemas TI pueden resultar en pérdida de datos, reducción de productividad y daños a la reputación. Sin embargo, las consecuencias suelen ser limitadas al ámbito empresarial y pueden ser gestionadas mediante planes de recuperación de desastres y copias de seguridad.	Las interrupciones en los sistemas *OT* pueden tener consecuencias mucho más graves, incluyendo pérdidas económicas significativas, daños a la infraestructura crítica, riesgos para la seguridad física de los empleados y el público, e, incluso, daños ambientales. La recuperación de estas interrupciones es compleja y requiere coordinación entre múltiples equipos y sistemas.

Fortaleciendo la seguridad en *OT*

La persistencia de equipos heredados sin actualizaciones representa diversos riesgos significativos para las infraestructuras industriales. Muchos sistemas o dispositivos antiguos no reciben parches de seguridad y esto los convierte en blancos vulnerables para los atacantes. La falta de actualizaciones incrementa la exposición a vulnerabilidades explotables, permitiendo que los ciberdelincuentes accedan a redes y a sistemas críticos.

Asimismo, la creciente conectividad remota representa otra amenaza para la ciberseguridad en *OT*. Con el auge del teletrabajo y la gestión remota de infraestructuras, las conexiones no seguras y las credenciales de acceso comprometidas pueden abrir la puerta a usuarios no autorizados. La falta de controles estrictos en estos accesos puede derivar en la manipulación de sistemas críticos y en la interrupción de operaciones esenciales. Por su parte, el *ransomware* continúa siendo una de las amenazas más serias en los entornos industriales, ya que este tipo de ataque puede paralizar por completo las operaciones, impactar la producción y generar grandes pérdidas económicas.

La ciberseguridad en entornos *OT* requiere una estrategia integral que combine evaluación de riesgos, defensa en profundidad y una cultura organizacional sólida para garantizar la protección de infraestructuras críticas.

El primer paso en este proceso es la evaluación de riesgos *OT*. Es fundamental identificar los activos críticos dentro del entorno industrial, estimar sus vulnerabilidades y priorizar los controles de seguridad adecuados con base en la consecuencia de la explotación de estas vulnerabilidades sobre los procesos industriales críticos. Dicha estimación permite comprender mejor los posibles puntos de ataque y la implementación de medidas preventivas específicas costo-efectivas, reduciendo así la exposición a amenazas cibernéticas.

Para fortalecer la seguridad, es recomendable adoptar un modelo de defensa en profundidad. Este enfoque se basa en la implementación de múltiples capas de seguridad que dificultan el acceso no autorizado y limitan la propagación de amenazas. Entre las medidas clave, se encuentran la segmentación de red para restringir el movimiento lateral de atacantes, el monitoreo constante de amenazas mediante herramientas avanzadas de detección, el control riguroso de accesos para garantizar que solo personal autorizado interactúe con sistemas críticos, y la gestión eficiente de parches de seguridad para mitigar vulnerabilidades conocidas.

Sin embargo, ninguna estrategia de ciberseguridad es completamente efectiva, sin una cultura organizacional orientada a la seguridad. La capacitación continua del personal, los programas de sensibilización sobre ciberamenazas y la realización de simulacros de respuesta ante incidentes son esenciales para preparar a los equipos frente a ataques reales. Un personal capacitado y consciente de los riesgos cibernéticos puede identificar y responder rápidamente a amenazas, minimizando con ello el impacto de posibles ataques.

Integrar estos tres pilares (evaluación de riesgos, defensa en profundidad y cultura organizacional) es clave para fortalecer la seguridad en entornos *OT*. La combinación de tecnologías avanzadas con una estrategia proactiva de prevención y respuesta va a garantizar la resiliencia de los sistemas industriales frente a un panorama de amenazas en constante evolución.

El compromiso de la alta dirección es esencial para garantizar una estrategia efectiva de ciberseguridad *OT*. La protección de infraestructuras industriales no puede ser delegada únicamente a los equipos técnicos; debe estar en la agenda del director de ciberseguridad (*CISO*, por sus siglas en inglés), así como de los líderes empresariales. En 2024, Deloitte llevó a cabo una encuesta

a casi 1,200 responsables de la toma de decisiones cibernéticas a nivel directivo, incluidos ejecutivos de alto nivel y sus subordinados directos[15]. Los resultados —recopilados de 43 países y seis industrias— destacan el papel y la responsabilidad que tiene el *CISO* en la mayoría de las actividades de ciberseguridad. Dentro de las principales áreas en las que los *CISO* se involucran en discusiones sobre las capacidades tecnológicas críticas para el negocio, la ciberseguridad *OT* ha aumentado el interés en la misma proporción que temas como respaldos en la Nube e inteligencia artificial (IA) generativa.

Asimismo, la encuesta refleja cómo la ciberseguridad influye en las decisiones sobre presupuestos en capacidades tecnológicas. Es, en este segmento, donde la ciberseguridad *OT* forma parte de áreas prioritarias después de la Nube, la IA generativa, el análisis de datos y la computación cognitiva. Tanto la IA, como la IA generativa, forman parte fundamental de la conversación entre los directores de ciberseguridad encuestados y esto puede obedecer a que su uso es una tendencia que va en aumento y que tiene como objetivo, principalmente, detectar anomalías en tiempo real. Se estima que el mercado de ciberseguridad industrial en Latinoamérica alcance 3,800 millones de dólares en 2025, con un fuerte enfoque en soluciones basadas en IA.

La IA tiene un desempeño clave en la ciberseguridad *OT* al responder también ante amenazas en infraestructuras críticas. En cuanto a la detección en tiempo real, los sistemas *OT* operan con protocolos específicos y dependen de dispositivos *IoT*, sistemas de supervisión y adquisición de datos (*SCADA*, por sus siglas en inglés) y controladores lógicos programables (*PLC*, por sus siglas en inglés). La IA es capaz de analizar patrones de comportamiento en la red y detectar anomalías o actividades sospechosas, como cambios inesperados en la configuración de dispositivos o tráfico inusual de datos. Un ejemplo de esto es que los modelos de aprendizaje automático pueden detectar ataques de *ransomware* industrial, como los que han afectado plantas de energía y suministro de agua.

En el análisis predictivo y la prevención de ataques, los algoritmos de *machine learning* pueden anticipar embates basándose en patrones históricos y comportamiento de amenazas previas. La IA permite identificar vulnerabilidades en sistemas *OT* antes de que sean explotadas por atacantes, recomendando acciones correctivas. Por ejemplo, en sistemas eléctricos inteligentes, la IA puede predecir intentos de intrusión en subestaciones y activar protocolos de seguridad.

La respuesta automatizada y la mitigación de incidentes es otro aspecto esencial. La IA puede automatizar respuestas ante ciberataques, reduciendo el tiempo de reacción y limitando daños en la infraestructura crítica. Los sistemas pueden configurarse para bloquear tráfico sospechoso, aislar dispositivos comprometidos y generar alertas a los equipos de seguridad.

Asimismo, es fundamental fortalecer la seguridad en entornos *OT* - TI debido a la integración entre ambas tecnologías que ha incrementado el riesgo de ciberataques. La IA ayuda a monitorear la convergencia entre estos entornos, detectando intentos de acceso no autorizado y asegurando la segmentación de redes. Un ejemplo de ello sería el intento de un usuario de TI que pretende acceder a sistemas *OT* sin autorización, actividad que puede ser identificada por algoritmos de IA.

La simulación y pruebas de ciberseguridad —también conocida como *red teaming* automatizado— es otra aplicación importante. La IA puede simular ataques para evaluar la resiliencia de los sistemas *OT* frente a diferentes amenazas. Se pueden usar técnicas como adversarial *machine learning* para probar la efectividad de los sistemas de defensa y mejorar su respuesta ante ataques reales.

Sin embargo, existen desafíos y consideraciones que deben ser tomados en cuenta. La IA tiene que ser entrenada con datos específicos de *OT* para evitar errores en la detección de amenazas, lo que implica enfrentar falsos positivos y negativos. Además, la dependencia del aprendizaje supervisado requiere una base de datos de ataques *OT* para mejorar la precisión de los modelos. Otro de los retos es la integración con infraestructuras heredadas, pues muchos sistemas *OT* son antiguos y no fueron diseñados para trabajar con soluciones de IA.

Conclusión

La ciberseguridad *OT* es un componente estratégico que no puede abordarse de manera aislada, sino que requiere la colaboración estrecha entre áreas clave como TI, operaciones, ingeniería y cumplimiento. Integrar la seguridad en la planificación empresarial, además de fortalecer la resiliencia operativa, alinea también las medidas de protección con los objetivos generales del negocio.

Es imperativo implementar prácticas robustas —como el monitoreo continuo, la segmentación de redes, la gestión de parches y la capacitación constante— y adoptar un enfoque proactivo basado en la detección y respuesta temprana para mitigar riesgos antes de que se materialicen en incidentes graves.

Asimismo, la inversión en ciberseguridad *OT* debe considerarse un elemento esencial para la mitigación de riesgos financieros y operativos, justificándose mediante el retorno de inversión que se traduce en la reducción de incidentes, la mejora en la disponibilidad de sistemas y una respuesta optimizada ante posibles ataques. Sin una estrategia clara y una inversión bien dirigida, las organizaciones van a experimentar sucesos vulnerables, por lo que solo a través de la integración de la ciberseguridad en todos los niveles, se podrá garantizar una protección efectiva y resiliente frente a los desafíos.

Contactos:

Paula Álvarez
Socia de Tecnología, Transformación y Ciberseguridad
Deloitte México
palvarez@deloittemx.com

Ernesto Landa
Gerente *Senior* de Ciberseguridad *OT*
Deloitte Spanish Latin America
elanda@deloitte.com

Referencias

1. Malwarebytes, (2025). "¿Qué es Stuxnet?" https://www.malwarebytes.com/es/stuxnet
2. Kaspersky, (2025). "¿Qué es el ransomware WannaCry? AO Kaspersky Lab". https://www.kaspersky.es/resource-center/threats/ransomware-wannacry
3. U.S. Department of Energy, (2021). "Colonial Pipeline Cyber Incident". Office of Cybersecurity, Energy Security, and Emergency Response. CESER. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
4. Díaz, R. y Núñez, G. (2023). "Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe". CEPAL. Naciones Unidas. https://www.cepal.org/es/publicaciones/49086-ciberataques-la-logistica-la-infraestructura-critica-america-latina-caribe
5. Flores, J. Et al. (2021). "La ciberseguridad en las organizaciones del sistema de las Naciones Unidas". ONU. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf
6. Vera, A. Et al. (2021). "Alguien trató de envenenar con lejía a la población de una ciudad de Florida hackeando el sistema de tratamiento de agua, dice el sheriff". Cable News Network. CNN. https://cnnespanol.cnn.com/2021/02/08/florida-envenenar-lejia-oldsmar
7. El hidróxido de sodio se utiliza en pequeñas cantidades para controlar la acidez del agua, pero en altas concentraciones puede ser extremadamente peligroso para la salud humana, causando quemaduras y otras lesiones graves.
8. Comisión Europea, (2025). "Directiva SRI 2: nuevas normas sobre ciberseguridad de las redes y sistemas de información". https://digital-strategy.ec.europa.eu/es/policies/nis2-directive
9. Arenas, J. (2024). "Estas son las estrategias nacionales de ciberseguridad de los países latinoamericanos". CIBERILATAM. https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html
10. Función Pública, (2020). *Políticas de Operación Proceso de Tecnologías de la Información. Seguridad de la Información*. https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf
11. Biblioteca del Congreso Nacional de Chile, (2024). *Ley 21663. Ley Marco de Ciberseguridad.* BCN. https://bcn.cl/3isi2
12. Superintendencia de Banca, Seguros y AFP, (2021). "Seguridad de la información y ciberseguridad: nuevo reglamento para promover un entorno seguro y confiable en beneficio de los usuarios de los sistemas supervisados". https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1147
13. Llamas, J. (2024). *Ciberseguridad en México: nueve años de debate legislativo y propuestas de ley (2015-2024)*. Foro Jurídico. https://forojuridico.mx/ciberseguridad-en-mexico-nueve-anos-de-debate-legislativo-y-propuestas-de-ley-2015-2024/
14. Riquelme, R. (2024). "Ciberseguridad en México: ataques aumentan 78% en un trimestre". El Economista. https://www.eleconomista.com.mx/tecnologia/ciberseguridad-mexico-ataques-aumentan-78-trimestre-20241026-731628.html
15. Deloitte, (2024). *The global future of cyber survey, 4th edition. The promise of cyber.* https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/deloitte-global-future-of-cyber-survey-4th-edition-the-promise-of-cyber.pdf

Deloitte.