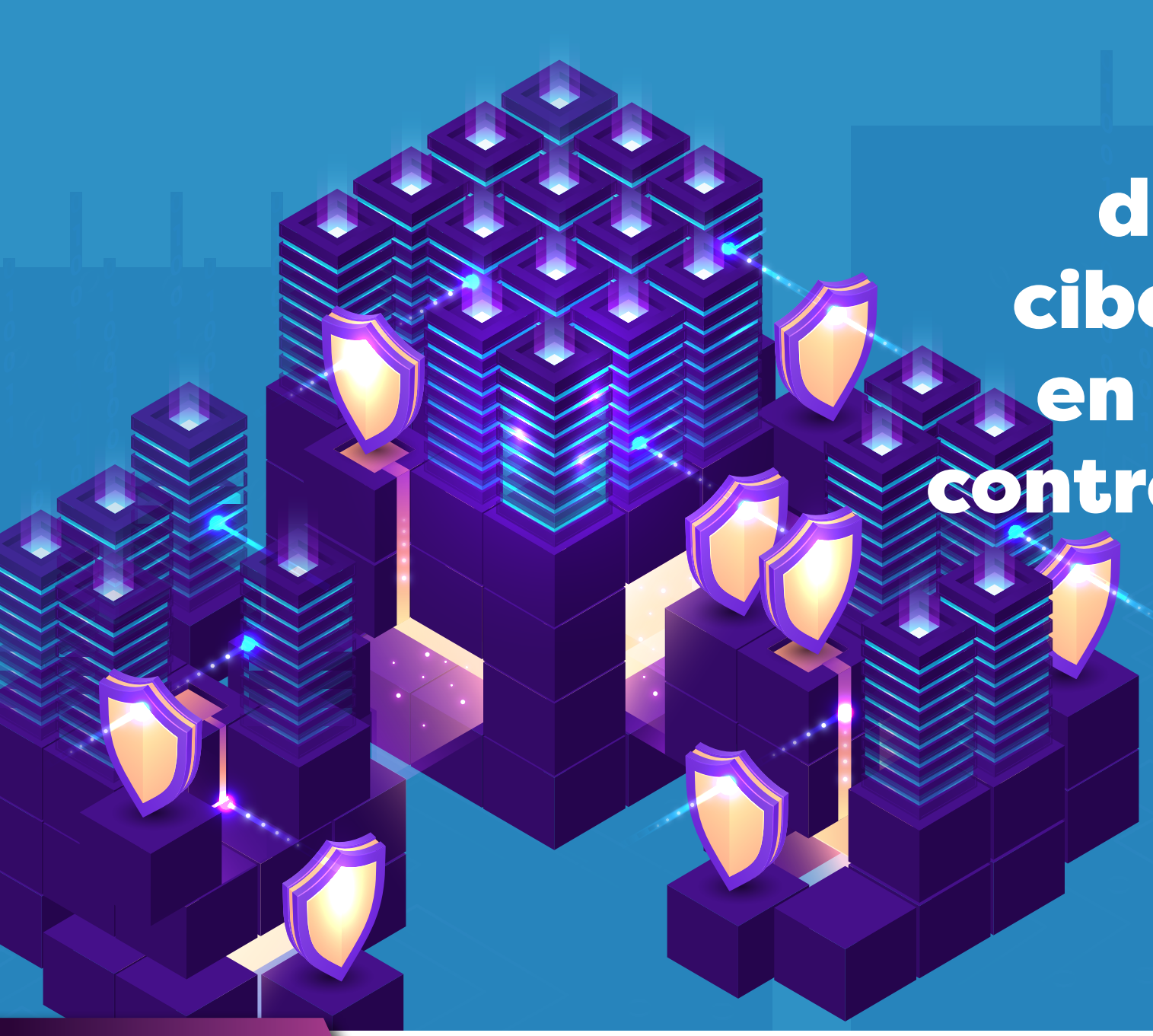


Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)

Mejores Prácticas en Ciberseguridad

B.08

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma inglés bajo el título *Reducción de los riesgos cibernéticos para los sistemas de control industrial (ICS)*. © (2020) Dirección Nacional de Ciberseguridad de Israel.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma inglés. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la división de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/BlobFolder/generalpage/icssolutions/he/ICS_eng.pdf**. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *startups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Clúster de Datos y Gobierno Digital (DDG) de la división Innovación para Servir al Ciudadano (ICS) de BID, disponible en: **https://www.iadb.org/es/quienes-somos/topicos/modernizacion-del-estado/datos-y-gobierno-digital**

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

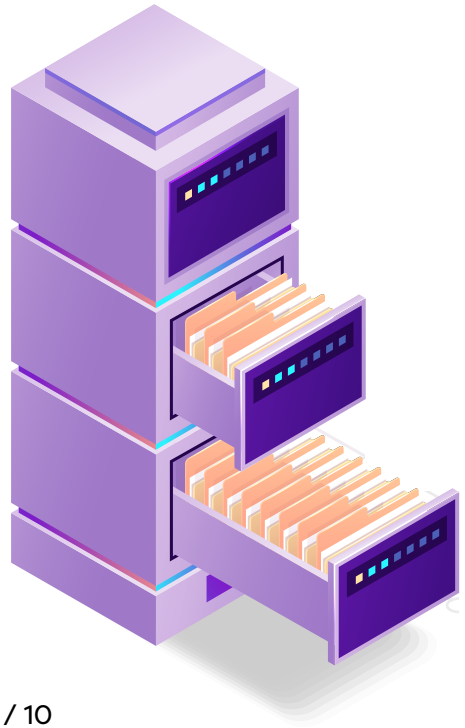
Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

Listado de siglas

Sigla	Definición
BMS	Sistemas de gestión de edificios
CID	Confidencialidad, integridad, disponibilidad
CISO	Director de seguridad de la información
DCS	Sistemas de control distribuido
DDoS	(Ataque) distribuido de denegación de servicio
DLL	Biblioteca de enlace dinámico
DMZ	Zona desmilitarizada
DoS	(Ataque) de denegación de servicio
ERP	Planificación de recursos empresariales
HMI	Interfaz hombre-máquina
ICS	Sistemas de control industrial
IED	Dispositivo electrónico inteligente
IoT	Internet de las cosas
MTU	Unidad terminal maestra
PLC	Controladores lógicos programables
RTU	Unidad terminal remota
SCADA	Sistemas de supervisión, control y adquisición de datos
TCP/IP	Protocolo de control de transmisión/protocolo de Internet
TI	Tecnologías de la información
TO	Tecnología operativa
VLAN	Red de área local virtual
VPN	Red privada virtual

Introducción



Introducción a los entornos ICS

Sistemas de control industrial (ICS, por sus siglas en inglés) es un término general para varios tipos de sistemas de mando y control, que se utilizan en la industria e infraestructuras críticas. Estos sistemas incluyen varios subsistemas y categorías. Algunos están diseñados para controlar un solo componente, como un sensor de altitud o temperatura que sirve para controlar la apertura y el cierre de una válvula o compuerta. Otros están diseñados para controlar múltiples componentes que están distribuidos en el campo. Lo que todos estos sistemas tienen en común es su capacidad de comunicación con los componentes finales, que actúan como sensores o accionadores.

Tipos comunes de ICS

01

Sistemas de supervisión, control y adquisición de datos (SCADA, por sus siglas en inglés).

02

Sistemas de control distribuido (DCS, por sus siglas en inglés).

03

Sistemas de gestión de edificios (BMS, por sus siglas en inglés).[2]

04

Sistemas de automatización y control industrial (IACS, por sus siglas en inglés).

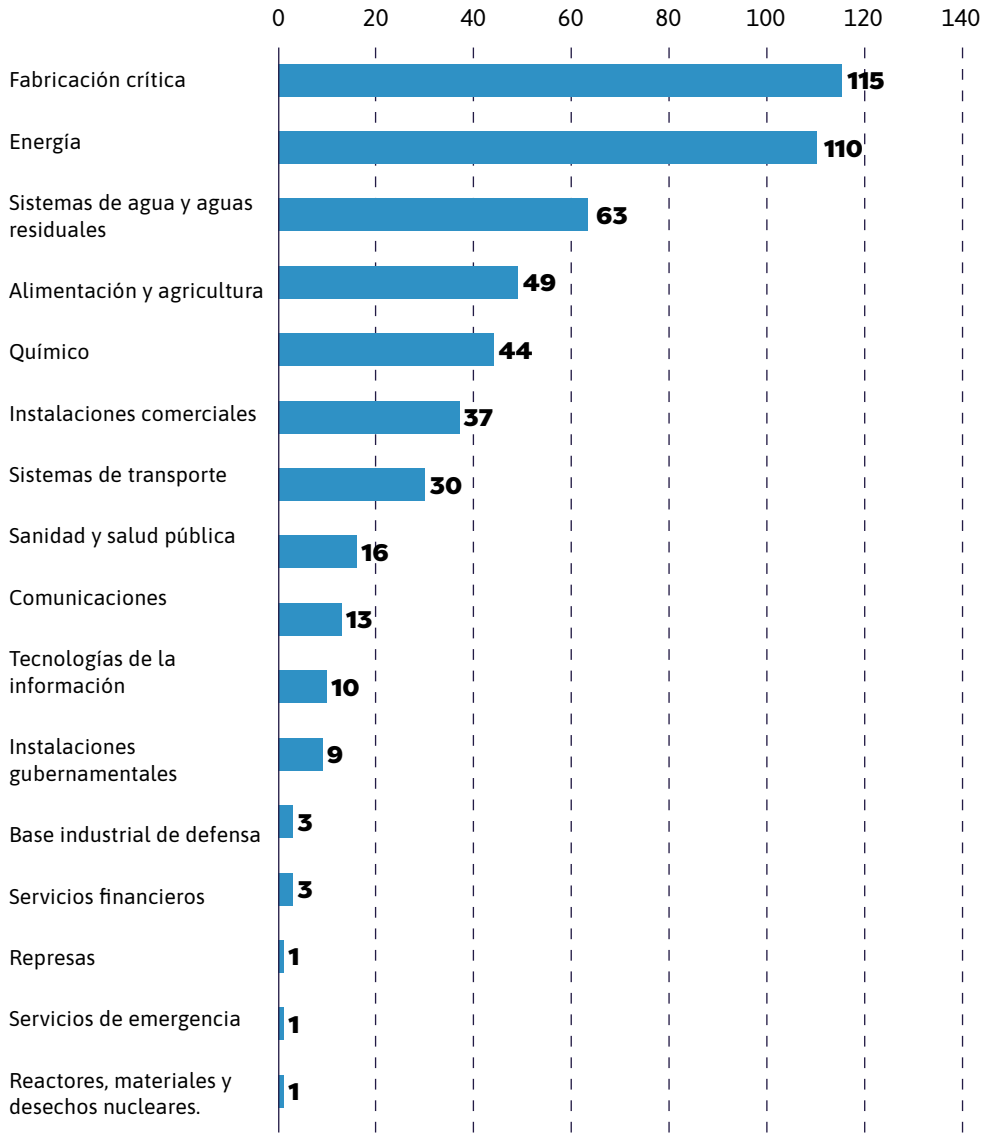
En los últimos años ha aumentado la concienciación sobre los eventos cibernéticos, los cuales se han centrado en los ataques a sistemas de la red espacial ICS.

A diferencia de los eventos contra las redes y equipos informáticos tradicionales, es muy probable que los destinados al entorno ICS afecten directamente la calidad de vida y seguridad física de los ciudadanos. Más allá de los posibles **daños a la línea de producción**, los daños a estos sistemas pueden provocar inundaciones en las ciudades, fugas de gases, venenos, toxinas o aguas residuales al medio ambiente, la explosión de contenedores y la inhabilitación de servicios esenciales como electricidad, gas o agua, entre otros.

La tendencia de los ciberataques contra los ICS ha ido en aumento en los últimos años. El motivo principal se debe al atractivo del ataque y a la dificultad de implementar en el entorno de tecnología operativa (TO) controles de protección y seguridad como en la red informática.

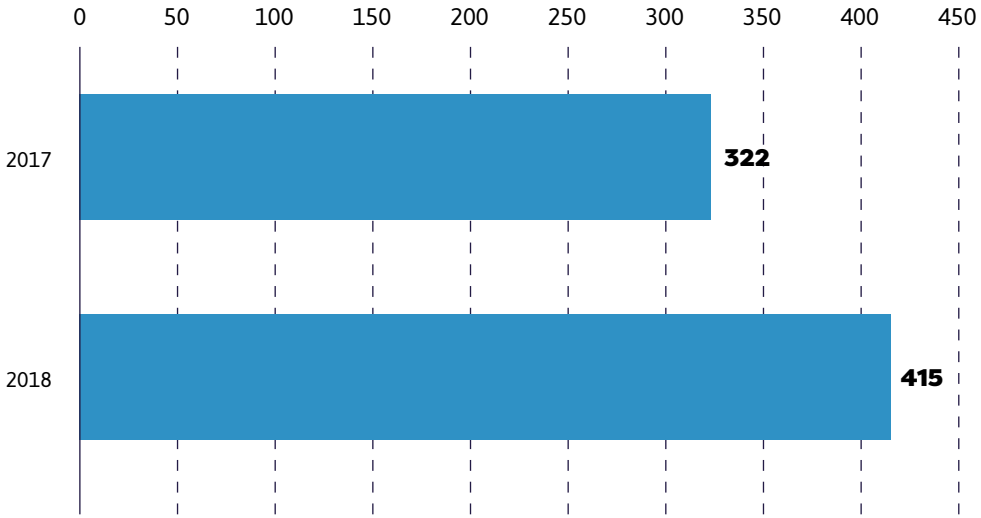
2. Para ampliar este tema, consulte el documento ***Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)*** de próxima publicación dentro de esta serie de guías de buenas prácticas en ciberseguridad.

Gráfico 1. Mapa de vulnerabilidades en ICS por sectores



Fuente: Kaspersky (2019).

Gráfico 2. Número de vulnerabilidades en ICS descubiertas en 2018 en comparación con 2017



Fuente: Kaspersky (2019).

Entre los eventos más destacados que se han publicado en los últimos años se encuentran los siguientes:[3]

- **Ataque a Triconex.** En diciembre de 2017 se produjo un ataque basado en un troyano de la familia Triton, dirigido contra un sistema de seguridad industrial. El atacante obtuvo acceso a la estación de trabajo de ingeniería y al sistema instrumentado de seguridad (SIS) y desde allí utilizó la mencionada plataforma de ataque para intentar cambiar el funcionamiento y programación de los controladores del sistema de seguridad. El objetivo del atacante era causar daños para desactivar y neutralizar el sistema de seguridad implementado en el proceso de fabricación.[4]

3. Puede leerse más al respecto en: **https://web.archive.org/web/20200313105355/https://ics.sans.org/media/SANSICS_DUC4_Analysis_of_Attacks_on_US_Infrastructure_V1.1.pdf**.

4. Para leer más visítese: **https://www.gov.il/BlobFolder/reports/sis/he/SIS-CERT-IL-W-400.pdf** (en hebreo).

- **Hackeo de la represa Bowman en Estados Unidos.** El 24 de marzo de 2016 se informó que unos hackers obtuvieron acceso a una pequeña represa del estado de Nueva York en los Estados Unidos. Esta toma de control maliciosa podría haber provocado una inundación en la ciudad, daños en los sistemas críticos y un importante perjuicio económico para la ciudad.

- **BlackEnergy: centrales eléctricas inhabilitadas en Europa.** El 23 de diciembre de 2015 se produjeron cortes de energía en compañías eléctricas europeas, lo que dejó regiones enteras sin electricidad. Se descubrió que un atacante implantó un *software* malicioso (*malware*) mediante un ataque de suplantación de identidad dirigida (*spear phishing*). La capacidad de suplantación de identidad (*spoofing*) y vulneración de las medidas *air gap* existentes entre los sistemas de tecnologías de la información (TI) y los sistemas TO llevó a la ejecución de BlackEnergy en la organización. En este caso, el atacante se aprovechó de la capacidad de saltar de los sistemas TI a los sistemas TO.[5]

Propósito de esta publicación

Esta publicación se propone ofrecer al público profesional los conocimientos básicos necesarios para una mejor protección de los entornos ICS. Para ello, además de conocimientos se aportan métodos y flujos de trabajo para aumentar la resiliencia en las líneas de producción. Al mismo tiempo, se incluyen ejemplos representativos y riesgos, métodos de defensa, recomendaciones y controles para mitigar los riesgos en el entorno TO. La publicación constituye una extensión profesional en el ámbito de los ICS a la ***Metodología de ciberdefensa para organizaciones 1.0***[6] publicada por la Dirección Nacional de Ciberseguridad (INCD, 2017).

Destinatarios

Esta publicación es relevante para quienes se dedican a la protección y defensa de los sistemas de control industrial, incluyendo el Director de Seguridad de la Información (CISO, por sus siglas en inglés), el personal de ciberdefensa en la organización y el personal de operaciones y control. Asimismo, está destinada a otros miembros de la organización, como los gestores de riesgos y el personal de adquisición, que también son responsables de los equipos informáticos para el entorno TO. El público objetivo de este documento incluye a los siguientes:

- **Ingenieros/técnicos de ICS:** los encargados de los procesos de instalación y mantenimiento de los ICS.

- **Operadores de ICS:** aquellos que están involucrados en las operaciones continuas y en curso de los sistemas.

- Personal de seguridad de la red en los ICS.

- **Administradores de seguridad de ICS:** como parte de sus responsabilidades (en la mayoría de los casos, nombrados por el CISO o un órgano de gestión).

- Empresas de integración o de consultoría y proveedores de servicios ICS.

- Profesionales de TI.

5. Más información al respecto disponible en: **https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01**.
6. El documento ***Metodología de ciberdefensa para organizaciones 1.0*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad**.

/01. Contexto tecnológico de los entornos ICS (topología y componentes principales)

Subsistemas, protocolos y componentes clave en el entorno ICS

Sistema SCADA

Es un sistema basado en la comunicación que permite el control de procesos a través del envío de comandos dedicados a equipos controladores. El sistema incluye una capa informatizada para supervisar y controlar los dispositivos y accesorios posicionados a lo largo de instalaciones y líneas de producción.

Entre los **procesos industriales** se encuentran los de producción, refinado, generación de energía y ensamblaje de productos. Por su parte, los **procesos en infraestructuras públicas o privadas** incluyen, entre otros, los sistemas de alumbrado exterior (urbano e interurbano), de abastecimiento de agua, de recolección y depuración de aguas residuales, la supervisión de oleoductos y gasoductos, las redes eléctricas, los sistemas de alarma y los grandes sistemas de comunicación. A su vez, los **procesos en instalaciones públicas o privadas** comprenden los sistemas de gestión de edificios, aeropuertos, puertos, barcos y estaciones espaciales. En este mismo contexto, los sistemas SCADA son los que supervisan y controlan los sistemas de climatización que funcionan en las instalaciones.

Protocolos de redes industriales

Son protocolos de comunicación en tiempo real desarrollados para enlazar sistemas, interfaces y dispositivos que juntos constituyen un ICS. La mayoría de ellos se diseñaron inicialmente para la comunicación en serie a través de conexiones seriales, pero luego se adaptaron para funcionar en redes Ethernet que utilizan un protocolo de comunicación como el protocolo de control de transmisión/protocolo de Internet (TCP/IP, por sus siglas en inglés).

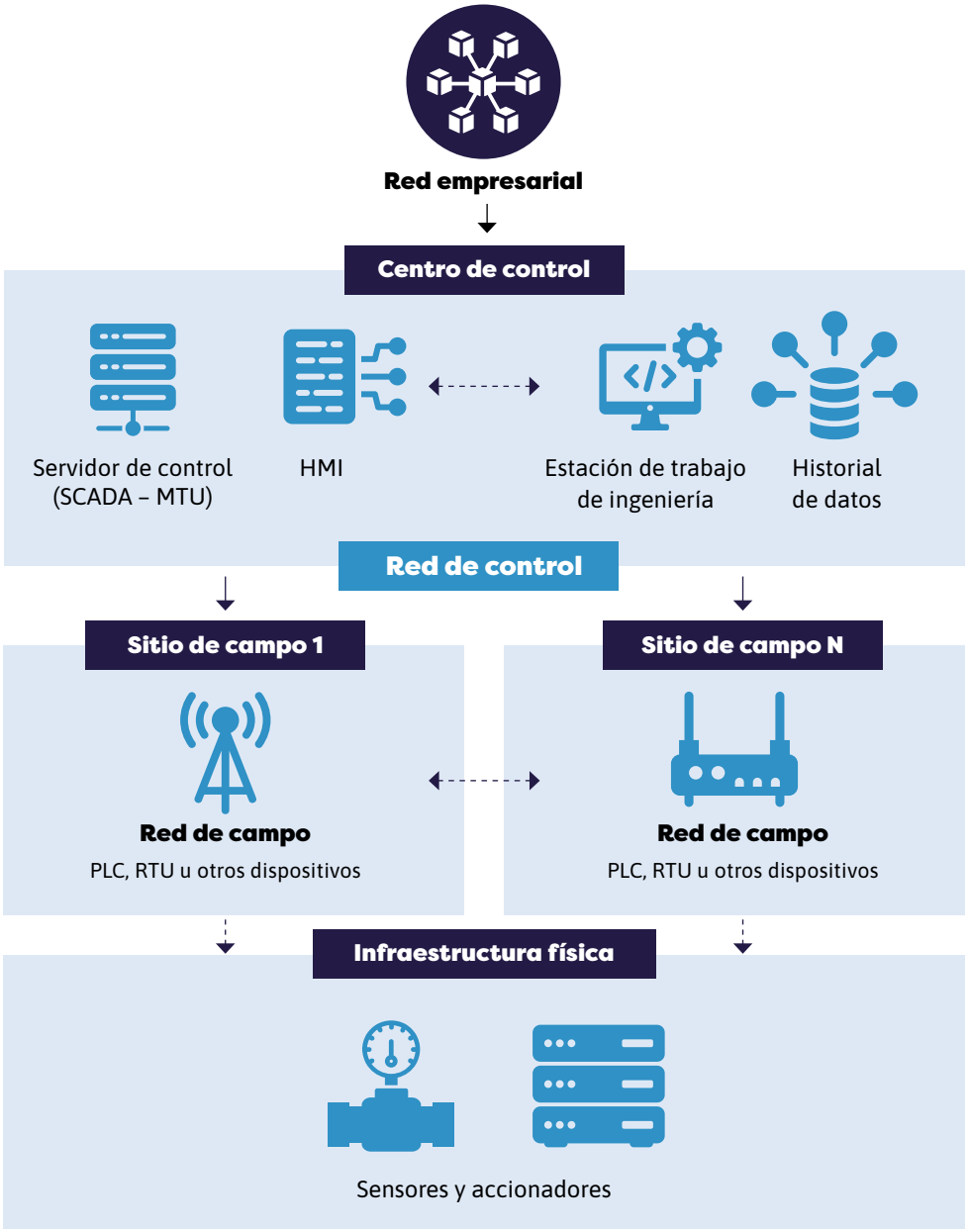
Los puntos débiles de las redes industriales son conocidos, en su mayoría, y se deben a la falta de concienciación y de conocimientos, a problemas en la configuración del sistema, a debilidades del *software*, a la falta de protección contra los *malware*, a problemas de encriptación, etcétera.

SCADA suele incluir los siguientes componentes:

- **Interfaz hombre-máquina (HMI, por sus siglas en inglés):** interfaz que muestra los datos y la información del proceso al operador, lo que le permite supervisar y controlar el proceso.
- **Unidad terminal maestra (MTU, por sus siglas en inglés):** sistema de control centralizado diseñado para supervisar, controlar y operar los componentes finales.
- **Controladores lógicos programables (PLC, por sus siglas en inglés):** controladores lógicos diseñados para recibir entradas, ejecutar lógica precargada (y lógica basada en la transferencia de comandos a los equipos finales).
- **Unidad terminal remota (RTU, por sus siglas en inglés):** unidades de monitoreo remoto, que intervienen en el proceso, están conectadas a sensores y ubicadas en el sitio del proceso.
- **Historial:** sistema que almacena los valores puntales del campo a lo largo del tiempo y muestra las tendencias de cambio de los parámetros medidos en el proceso. El sistema suele ser utilizado por los ingenieros de control para mejorar y afinar el proceso.

- **Sensores:** dispositivos que miden las condiciones físicas y pueden activar accionadores y transmitir a los sistemas de control.
- **Accionadores:** activados por los sensores, desencadenan el cambio requerido (como la apertura de una válvula).
- **Infraestructura de comunicación:** conecta el sistema de control con las unidades (comunicaciones por cable, radio, celular, wifi, satélite).
- **Dispositivo electrónico inteligente (IED, por sus siglas en inglés):** dispositivos que forman parte de los sistemas de control, como sensores, motores, transformadores, bombas, etc., y están equipados con un pequeño procesador de información. Suelen comunicarse a través del protocolo Fieldbus, funcionan como elementos esclavos y son controlados por unidades finales remotas.
- **Internet de las cosas (IoT, por sus siglas en inglés):** componentes dedicados, basados en la comunicación y la capacidad de intercambiar datos e información a través de Internet.
- **Internet industrial de las cosas (IIoT, por sus siglas en inglés):** componentes diseñados para la industria manufacturera basados en las comunicaciones.

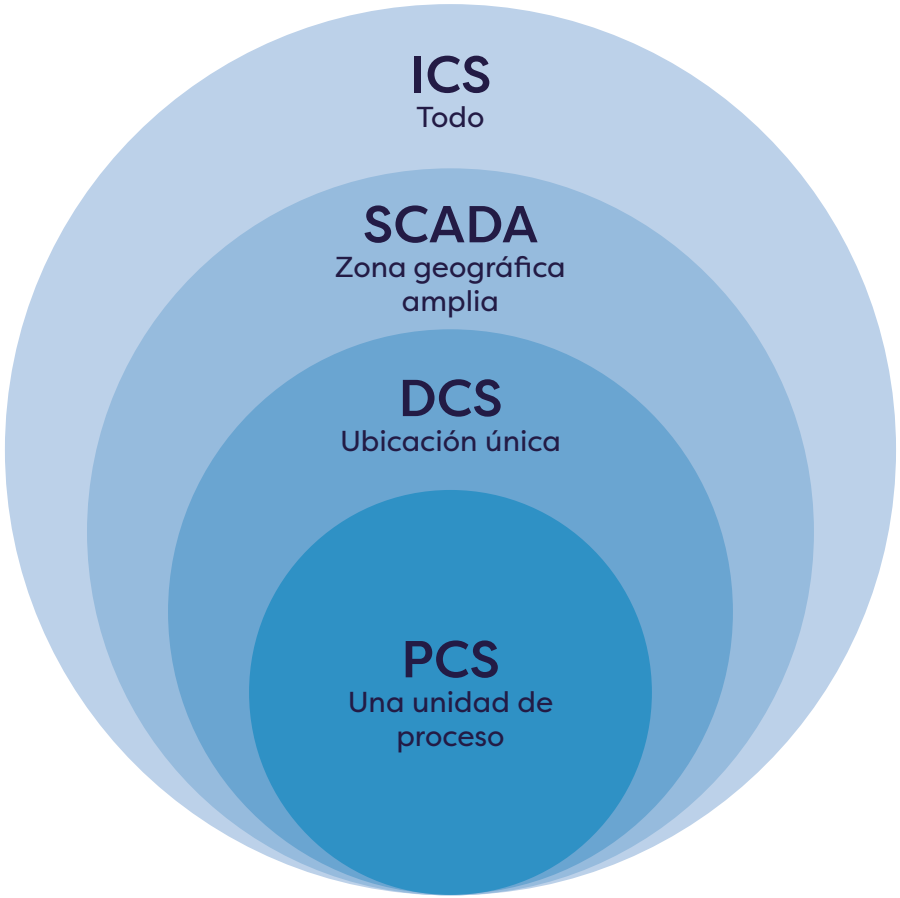
Gráfico 3. Descripción de los componentes del entorno ICS



Sistema de control distribuido

El DCS se diferencia de los sistemas no distribuidos que utilizan un único controlador centralizado. Este sistema suele emplear procesadores optimizados para los procesos (jerárquicos) y conectados por redes de comunicación para la supervisión y el control.

Gráfico 4. Principales subsistemas del mundo ICS



Nota: PCS: sistemas de control de procesos (siglas en inglés).

Topología clásica en el entorno ICS

El entorno ICS es complejo dado que incorpora un entorno de gestión, a veces vinculado al sistema de planificación de recursos empresariales (ERP, por sus siglas en inglés) y a otros sistemas de este tipo, un entorno TO, posiciones informáticas, sensores y controladores (véase el entorno clásico en el gráfico 3). Hay dos modelos que pueden ayudar en las fases de planificación e implementación de la arquitectura en el entorno ICS:

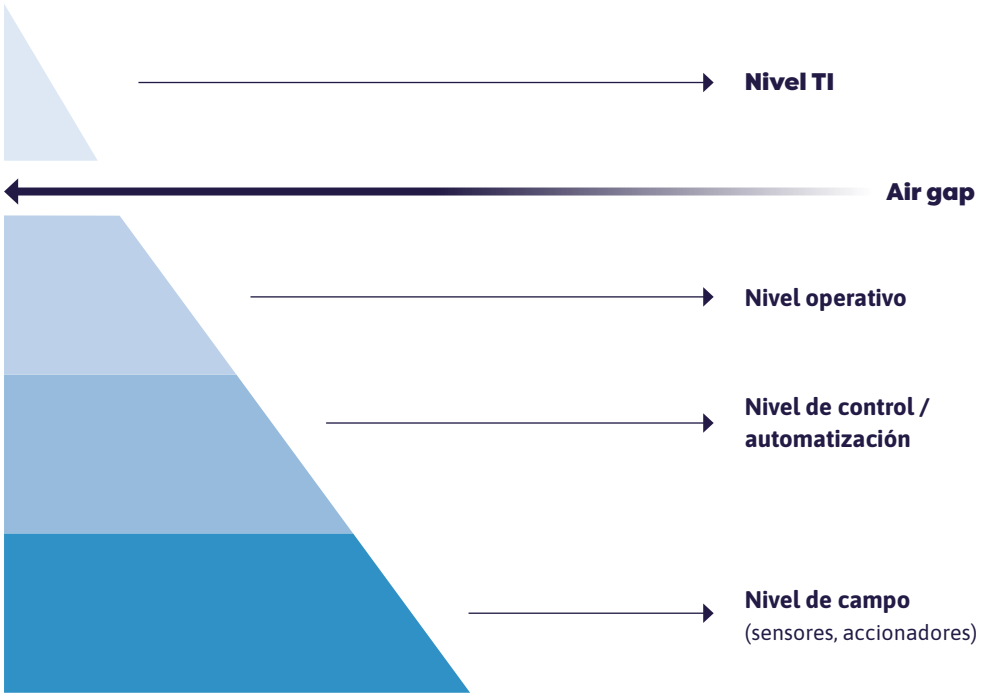
- el modelo triangular (basado en ISA 95);
- el modelo Purdue.

Estos modelos permiten establecer la referencia estructural por jerarquía y capas del sistema de control. En el modelo triangular, la descripción sistémica presentada a través de los cinco niveles en un triángulo (que incluye *air gap)* es más simplista y adecuada para sistemas sencillos. Por su parte, el modelo Purdue tiene una distribución de seis niveles y es adecuado para organizaciones más grandes o entornos más complejos.

Por regla general, ambos modelos separan el sector de TI, que gestiona el sistema de negocio de la organización, de la TO y del dominio en el que también se gestionan los componentes físicos, que reciben instrucciones a través de comandos de cambios de potencia eléctrica.

Modelo triangular (para entornos sencillos y organizaciones pequeñas)

Gráfico 5. Modelo triangular



Separación del triángulo tras las aportaciones de diferenciación de TI:[7]

- **Entorno empresarial y participación de TI en la organización:** esta red está a veces directamente conectada a Internet.
- **Entorno de gestión en la red de producción** (*air gap*).
- **Servidores de mando y control y los propios controladores:** constituyen el núcleo del sistema, es decir, una zona donde se ejecutan los procesos para todos los dispositivos locales y remotos.
- **Dos capas inferiores del modelo:** allí se encuentran los controladores industriales PLC, equipos de entrada/salida remota (RIO, por sus siglas en inglés), IED, en consonancia con la estructura del sistema. Estos componentes están conectados a sensores y accionadores a través de relés que controlan el proceso de fabricación.

7. La separación *air gap* se practica principalmente en infraestructuras críticas. Hay organizaciones en las que la separación entre entornos se basa en la red de área local virtual (VLAN, por sus siglas en inglés), cortafuegos dedicado, etcétera.

Modelo Purdue

Gráfico 6. Distribución del modelo Purdue por regiones

Fuente: EnCompass (2018).

Este modelo presenta una descripción ampliada del modelo triangular y contiene seis niveles (0-5). Dicho modelo de estructura es adecuado para organizaciones medianas y grandes, que tienen una interfaz con la red de TI.

- **Niveles 5 y 4:** esta área está dedicada a un entorno de gestión de procesos empresariales y, como tal, se basa en los sistemas y servicios de TI de la empresa. El área incluye la conexión a Internet de la empresa, los sistemas ERP, etcétera.[8]

- **Nivel 3:** esta área incluye un entorno de gestión de la red de producción, materiales, mano de obra, inventario, disponibilidad de máquinas (como los sistemas de ejecución de fabricación [MES, por sus siglas en inglés], etc.). La conexión entre las capas 3 y 2 se realizará mediante dispositivos de cortafuegos o aquellos en los que la comunicación es unidireccional y se separa mediante un dispositivo para crear un tráfico unidireccional (diodo).

- **Nivel 2:** en este entorno se encuentra el sistema de control en la HMI y su función es permitir la supervisión y el control de los procesos de inicio de sesión (SIP, por sus siglas en inglés), así como permitir la intervención del operador según sea necesario y de acuerdo con sus permisos para programar o cambiar los comandos del controlador. Los sistemas complejos tienen varios puestos de operador (HMI), lo que permite a los operadores centrarse en diferentes áreas del sistema o intervenir de acuerdo con las necesidades del proceso.

- **Nivel 1:** en este entorno, los procesos se gestionan mediante ordenadores de control (servidor de automatización) para todos los dispositivos que ejecutan RTU, controladores PLC, etcétera.

- **Nivel 0:** representa la capa más baja del modelo Purdue y está conectada a los sensores y accionadores que operan la máquina.

8. Para ampliar este tema, consulte el documento ***Seguridad de sistemas de planificación de recursos empresariales (ERP)*** de próxima publicación dentro de esta serie de guías de buenas prácticas en ciberseguridad.

Cuadro 1. Mapa de posibles ataques según el modelo Purdue

						
Posible curso de acción para el ataque	**Capas 4 y 5**	USB infectados	*Scripting* entre sitios (XSS, por sus siglas en inglés)	Documentos infectados	Ingeniería social	*Phishing* de credenciales
Métodos de ataque	**Capa 3**	· Error de búfer · Inyección de biblioteca de enlace dinámico (DLL, por sus siglas en inglés)	Troyano de acceso remoto (RAT, por sus siglas en inglés) que toma el control	*Keylogger* que roba las de credenciales de la red privada virtual (VPN, por sus siglas en inglés)	· Inserción de un troyano · Apertura de una puerta trasera	· Inyección de DLL · Establecimiento de una puerta trasera
	Capa 2	· Escalada de privilegios · Ataque a la memoria	Hallazgo de debilidades en *air gap*	· Depósito de troyanos · Daño al registro · Toma de control de servidores	· Ataque a la memoria · Descubrimiento e inversión de relés	Daño a las estaciones de trabajo de ingeniería
	Capa 1	· Cambios en la configuración del PLC · Daño a los equipos	· Modificación del *firmware* · Apertura de interruptores · Daño a los sistemas	Relés invertidos que ocasionan daños y cortes de energía	Ejecución de comandos falsos en el PLC	· Cifrado de los archivos para secuestro de datos (*ransomware*) · Desactivación de sistemas
	Capa 0	Cambios en la configuración de los sensores	Cambio en la actividad de los accionadores	Daños físicos	Cambios de funciones y valores	Impactos en las condiciones ambientales

Programación y comunicación entre controladores y HMI

Este apartado describe el proceso de fondo en la programación de controladores con el objetivo de comprender las oportunidades desde el punto de vista del atacante y los riesgos en el proceso de carga del controlador (y la capacidad de programación).

A lo largo de los años, los controladores PLC han sido desarrollados por diferentes fabricantes, los cuales han creado una interfaz de usuario única y funciones propias. Como consecuencia de esto, la conformación de los procesos de programación y comunicación entre controladores y HMI se ha visto influenciada por las exigencias y tecnologías particulares de un mercado de soluciones ICS ampliamente diversificado como lo son:

- **Entornos y necesidades cambiantes:** conllevan un aumento de las dificultades operativas y de seguridad en la comunicación entre los controladores programados por varios fabricantes.

- **Entorno de controles mixtos:** a pesar de la necesidad y recomendaciones del fabricante de utilizar controladores únicos (del mismo fabricante y de la misma familia de productos), también hay entornos mixtos que incorporan varios controladores, producidos por diferentes proveedores.

- **Estándar y métodos de programación:** como se describe en la norma IEC 61311-3, en la versión estándar (publicada en 2013) se definieron cinco lenguajes de programación. Cada familia de controladores producidos por un proveedor particular tiene una interfaz gráfica única que "compila" el archivo de configuración de forma única para el mismo tipo de controlador (de los mismos proveedores).

- En un entorno mixto, los ingenieros de control deben familiarizarse con algún *software* gráfico. En los sistemas modernos, la programación de los controladores se realiza en uno de los cinco lenguajes definidos en la norma antes mencionada, lo que permite transferir e integrar con relativa facilidad las aplicaciones cuando se trabaja con controladores de varios fabricantes.

- **Programación de controladores:** en el pasado, se acostumbraba a programar los controladores utilizando un único método llamado Ladder Logic, y los ordenadores de control (HMI) utilizando el *software* del proveedor de la HMI. Este proceso se realiza en una estación de ingeniería.

Lenguajes de programación más comunes

01

Lenguaje Ladder: un método clásico, que permite al programador traducir el proceso de pensamiento lógico en un dibujo y diagrama. El proceso de programación se realiza a través de la traducción. Un proceso de trabajo es deseable para secuenciar operaciones representadas por ilustraciones del sector eléctrico que simulan un interruptor, una entrada digital, un contador de tiempo y más.

02

Bloques de función: la función permite utilizar un componente de *software* en varios lugares diferentes, manteniendo la uniformidad de las operaciones y optimizando el proceso de escritura del *software*.

Nota: Es importante tener en cuenta que los controladores desarrollados con estos lenguajes son más inmunes a la hora de realizar cambios en el proceso de *software* que puedan perjudicar el proceso.

03

Más lenguajes: lista de instrucciones (IL, por sus siglas en inglés), texto estructurado (ST, por sus siglas en inglés), diagrama funcional secuencial (SFC, por sus siglas en inglés).

Tendencias y retos comunes en los entornos ICS

Entorno de producción

- Estandarización: uso de sistemas operativos estándar que incluyen vulnerabilidades explotables por vía cibernética.

- Necesidad de conectividad: la vinculación de redes o la conexión con TI e Internet aumenta la visibilidad y la superficie de ataque.

- Conectividad no segura: módems, enfoques de mantenimiento remoto, comunicación inalámbrica (como wifi).

- Seguridad de la información y arquitectura: disponibilidad de información sobre la arquitectura, las prácticas de instalación y mantenimiento, la estructura de la configuración de interconexión con los controladores, los controladores sobre los controladores y las víctimas famosas y conocidas de ciberataques por Internet.

- Uso de dispositivos y capacidades de IoT.

Capa de aplicaciones

- Aplicaciones obsoletas, escritas de forma no segura.

Capa de configuración

- Los sistemas se han desarrollado para funcionar durante años sin reinicios, por lo que es muy difícil de implementar actualizaciones.
- Muchas veces, las contraseñas están grabadas en el código de contraseñas por defecto de fábrica y son difíciles de cambiar.
- Suele haber dificultades para encriptar los campos (sensibles).
- No siempre se pueden instalar sistemas antivirus en los equipos (por razones operativas y contractuales), o sistemas que impidan la ejecución de códigos desconocidos.
- Dificultad para gestionar e identificar a los usuarios, ya que se trata de un entorno TO.

Capa de red

- El desarrollo de la tecnología ha llevado a la tendencia de vincular las redes operativas aisladas a un entorno administrativo, creando muchas vulnerabilidades que las exponen a una amplia gama de amenazas.
- El hecho de centrarse en el rendimiento en tiempo real dificulta la introducción de componentes de seguridad de la información en la red (latencia).
- Dificultad para realizar el escaneo de la red (gestión de activos) debido al miedo y al riesgo de retrasar los procesos de producción (como el barrido de ping [*ping sweep*] que solía causar fallos en el pasado).
- Dificultades operativas y legales para realizar pruebas de intrusión clásicas y activas en la red y en los equipos por miedo a que se caiga el sistema.
- Dificultad en el cifrado y la segmentación de la red.

/02.
Presentación de los riesgos de ciberseguridad en el ámbito de los ICS

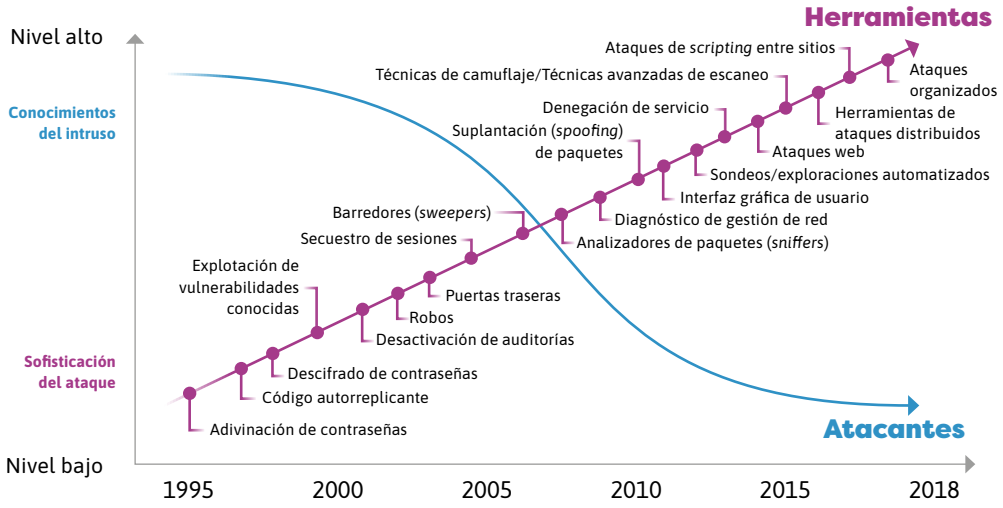
Introducción a los riesgos de ciberseguridad en los entornos ICS

Al igual que los sistemas operativos y las líneas de producción, los ICS son sistemas que se han diseñado y utilizado durante años. A veces se trata de redes sin controles ni mecanismos de seguridad (físicos o lógicos) y sin entradas contra los ciberataques. En los últimos años, los ataques a los ICS se han vuelto aún más fáciles. Esta tendencia se debe, entre otras cosas, a la capacidad de detectar vulnerabilidades, identificar lagunas, obtener y utilizar herramientas de *hacking*, lo que ha provocado un aumento de la tendencia de los ataques.[9] El uso de las herramientas y capacidades existentes, como el uso del sitio web SHODAN, permite el mapeo de los entornos ICS conectados a Internet.

9. Más información disponible en: **https://cdn.prod.website-files.com/645a4534705010e2cb244f50/649132a41339581aa24a9426_Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf**.

Un análisis del historial de eventos de ICS publicados muestra que las amenazas a estos entornos no son significativamente diferentes de las amenazas a los entornos TI. En ambos casos, las amenazas pueden clasificarse como aquellas que buscan comprometer la confidencialidad (C), integridad/fiabilidad (I) y disponibilidad de los datos (D) (la tríada CID). Estas amenazas incluyen los intentos de dañar la continuidad del negocio a través de un ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés), la escucha de las comunicaciones, la interrupción y/o el cambio de la función de un componente, el robo de datos, los ataques de *ransomware*, etc. A veces, el ataque a la red de producción comienza con un ataque previo a las redes de TI (como el evento de ataque a la infraestructura energética BlackEnergy, ya mencionado).[10] El gran riesgo en los ataques a ICS es que el proceso de equilibrado y los daños materiales, como, por ejemplo, a calderas, turbinas, etc., puede causar problemas importantes en la prestación de un servicio esencial o perjudicar la vida humana.

Gráfico 7. Desarrollo de herramientas de ataque para entornos ICS en los últimos años



Fuente: Di Pinto, Dragoni y Carcano (2018).

10. Puede leer más al respecto en: **https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors**.

Los métodos de ataque más populares para las redes ICS se basan, entre otras implementaciones, en las siguientes:[11]

01

Utilización de mecanismos de autenticación débiles.

02

Escaneo de la red/sondeo (escaneo de puertos): como parte del proceso de ataque para localizar puertos abiertos en la organización y durante la etapa de recopilación.

03

Medios extraíbles: como parte de un salto entre diferentes entornos.

04

Activación de herramientas y *software* de fuerza bruta para el descifrado de contraseñas como parte de un proceso de hackeo.

05

Abuso de la autoridad de acceso (permisos legítimos): por el usuario o el *malware* programado para utilizar los permisos.

06

Phishing: ataques de suplantación de identidad (principalmente populares para las redes ICS conectadas a Internet, como el evento BlackEnergy y un ataque a infraestructuras críticas).

07

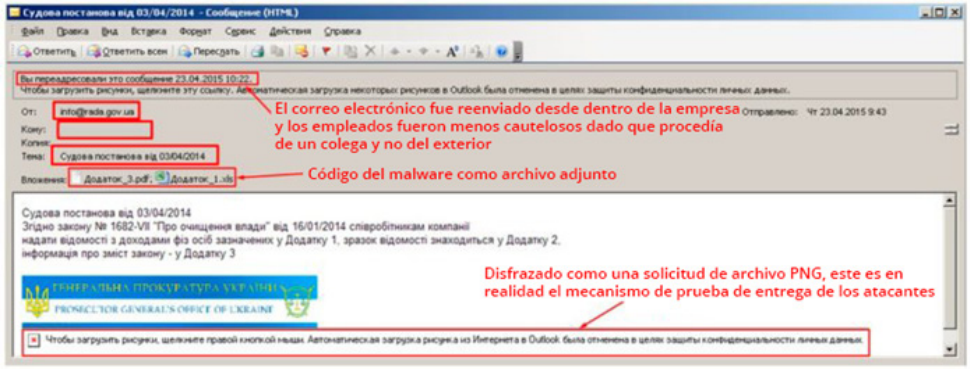
Inyección de lenguaje de consulta estructurada (SQL, por sus siglas en inglés).

11. Para más información, véase: **https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf**.

Ejemplos de escenarios

- Usar las contraseñas predeterminadas del fabricante para obtener acceso al sistema.
- Cambiar el comando de un controlador.
- Atacar sistemas basados en sistemas de posicionamiento global (GPS, por sus siglas en inglés) o comunicaciones por satélite.
- Escuchar secretamente la comunicación.
- Insertar un código hostil a través de una actualización.
- Introducir un código hostil utilizando una conexión de dispositivo externo.

Imagen 1. Ataque iniciado en la superficie del entorno TI con el fin de ejecutarse en el entorno TO



Fuente: Yasinskiy (2016).

En el *ranking* de las 10 principales amenazas en entornos ICS para 2019, publicado por la Oficina Federal de Seguridad de la Información alemana (BSI, por sus siglas en alemán), se observa el panorama que se muestra en el cuadro 2.

Cuadro 2. Cambios en las tendencias de los ataques a entornos ICS en 2019 frente a 2016

Las 10 principales amenazas	Tendencia desde 2016
Infiltración de *malware* a través de medios extraíbles y *hardware* externo	↗
Infiltración de *malware* a través de Internet e intranet	↗
Error humano y sabotaje	↑
Vulneración de los componentes de la extranet y la nube	↑
Ingeniería social y *phishing*	↘
Ataques de denegación de servicio (DoS, por sus siglas en inglés) y ataques DDoS	↑
Componentes de control conectados a Internet	→
Intrusión mediante acceso remoto	→
Fallos técnicos y fuerza mayor	↘
Vulneración de *smartphones* en el entorno de producción	→

Fuente: BSI (2019).

En muchos casos, las redes operativas están aisladas y separadas de Internet. Estas disposiciones de seguridad dificultan la organización y penetración del proceso. Sin embargo, atacar las redes ICS como una red diferenciada suele ser posible en cuatro ejes principales (y según sus requisitos e insumos de protección en las etapas de diseño de abajo):

- **Amenaza interna** (un incidente operativo causado por el empleado de forma inadvertida o fraudulenta) y en los casos en los que el atacante tuviera accesibilidad física (incluida la explotación de técnicos).[12]

- **Mapeo y explotación de oportunidades en el eje de la cadena de suministro**, como la explotación mediante la suplantación (*spoofing*) o movilización de una parte que da soporte al sitio o la instalación de *malware* en el equipo del proveedor.[13]

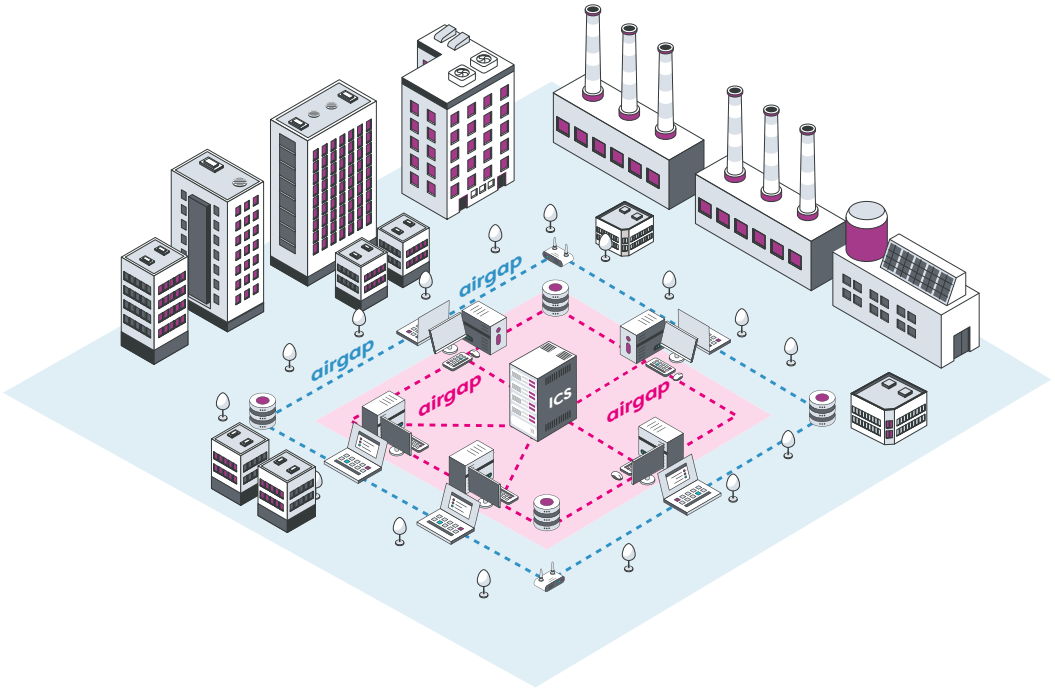
- **Explotación de los canales de entrada y salida** y ejecución de ataques a través de ellos, como el saneamiento de datos y el desarmado y reconstrucción de contenido (CDR, por sus siglas en inglés), actualizaciones, etcétera.

- **Ataques basados en el ataque de canal lateral:** explotación de las limitaciones del entorno físico y tecnológico que existen en el entorno informático para procesos de adivinación de datos, recolección o interferencia, como el uso de la inductancia electromagnética.

En los últimos años, ha aumentado la potencia de la informática y la necesidad de una conectividad diversa con otros sistemas, como el análisis y la previsión empresarial, el análisis del rendimiento operativo, la medición del rendimiento, la previsión de fallos, la resolución de averías, etc. Estas capacidades están diseñadas para aprovechar las actividades de la organización y satisfacer las necesidades empresariales y funcionales presentes y futuras. Esta conectividad se apoya además en la integración de las tecnologías del IoT, que también permiten los canales de ataque.

Debido a las ventajas del desarrollo de las tecnologías anteriores, el concepto de **red operativa diferenciada** se está diluyendo. En la actualidad, los motores de búsqueda como SHODAN permiten acceder a las interfaces de gestión de los entornos operativos.

Gráfico 8. Red aislada de la red externa



12. Para ampliar este tema, consulte el documento ***Recomendaciones de defensa: La amenaza interna*** disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.
13. Para ampliar este tema, consulte el documento ***Cadena de suministro*** disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/cadena-de-suministro-cuando-todos-los-eslabones-son-fuertes-su-organizacion-esta-protegida-mejores**.

Desafíos de la defensa en entornos TO frente a los TI

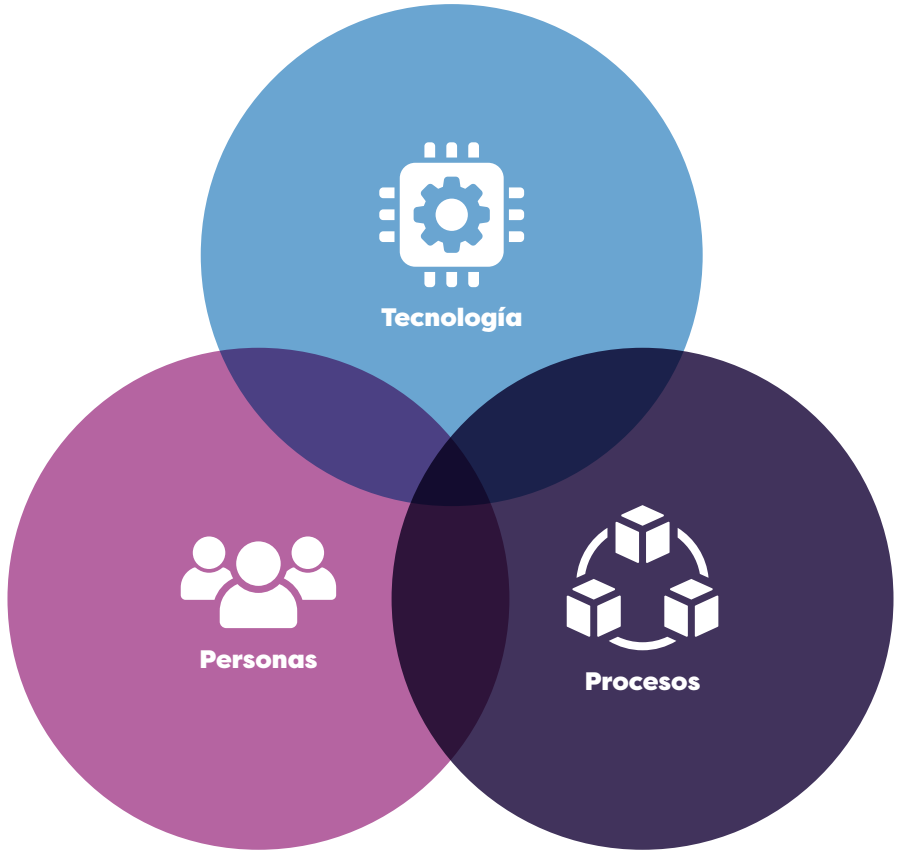
Diferencias en la protección de los sistemas TI frente a los TO y los ICS

Mientras que los trabajadores de la ciberdefensa están familiarizados y tienen experiencia en los procesos y tecnologías para proteger el entorno informático tradicional (esto es, el entorno TI), el conocimiento y capacidad para realizar el mismo tipo y nivel de protección en el entorno TO son limitados. Esta limitación se debe, en parte, a los retos que se mencionan a continuación.

Personas

- **Conocimiento:** los profesionales de la seguridad de la información y la ciberseguridad están más familiarizados con la protección de los entornos TI (protocolos, productos, herramientas, etc.). Por ese motivo, a veces, no comprenden el cambio necesario para adaptar sus conocimientos a la hora de evaluar los riesgos, elegir las soluciones de protección, supervisar y preparar un plan de recuperación de los entornos TO.
- **Colaboración:** la mayoría de las veces, la confianza en la operación y mantenimiento de los sistemas en el entorno de producción es un factor que no está sujeto jerárquicamente al responsable de la seguridad de la información ni al responsable de los sistemas de información y redes de comunicaciones de la organización. La capacidad de realizar revisiones/cambios y endurecer los requerimientos exige una profunda colaboración entre las dos unidades de la organización. Si bien los profesionales de ciberdefensa suelen tener los conocimientos necesarios para hablar con los profesionales de TI, los saberes para dialogar con los profesionales de operaciones/control son diferentes (conocimientos específicos del sector, como una variedad de conceptos y equipos relevantes para un entorno de producción, como es el caso de los controladores de automatización programables [PAC, por sus siglas en inglés], inexistentes en las redes de TI, comprensión de los procesos químicos o de ingeniería, etc.).
- **Dependencia de partes externas:**[14] si bien el entorno informático puede ser utilizado por los empleados de la empresa y proveedores locales con los que la organización está bien familiarizada (incluidos el trabajo de fondo/la comprobación de fiabilidad), al trabajar con estos fabricantes, el soporte y el mantenimiento suelen proporcionarlos partes profesionales dependientes o están en garantía, por lo que la capacidad del cliente para influir en ellos es baja (como un proveedor de sistemas o un experto en *software* del extranjero).

Gráfico 9. Sinergia, colaboración y sincronización entre tecnología, procesos y personas



14. Más información disponible en: **https://www.gov.il/en/pages/cyber_industry_toxins_permit** (en inglés).

Procesos

- **Alta capacidad y coste de la línea de producción y de las operaciones comerciales:** toda necesidad de actualización, puesta al día o tiempo de inactividad se traduce inmediatamente en una gran cantidad de dinero y riesgo para el proceso de control. En el marco de la reducción de riesgos se puede considerar un área dedicada a la ejecución de archivos y simulaciones como proceso preliminar antes de la puesta en línea de la red.

- **Costo de parada/tiempo de inactividad:** dificultad para equilibrar el riesgo y para localizar controles adecuados que impidan detener el proceso frente a la localización de controles compensatorios que permitan reducir el riesgo sin detener ni vulnerar la línea de producción.

Tecnología

- **Oferta limitada de soluciones de protección dedicadas:** aunque soluciones como el análisis de código, la detección de vulnerabilidades y otras están disponibles e integradas en muchos sistemas de todo el mundo, no siempre son compatibles con los entornos ICS dedicados. Además, estas herramientas no siempre están aprobadas para su uso por el fabricante o por los operadores de los equipos, debido a la preocupación por los daños operativos, la cobertura de responsabilidad, etcétera.

- **Ciclo de vida de los equipos:** mientras que los equipos de TI se reemplazan con relativa frecuencia en las organizaciones y de forma proporcional (en relación con el ciclo financiero de la organización), la sustitución de un controlador o componente de SCADA implica esfuerzos, recursos y costos financieros importantes para la organización. Esto lleva a una realidad en la que los equipos tienen entre 10 y 20 años o más, lo que obliga a protegerlos con las herramientas existentes, que son limitadas y a menudo nunca se ajustan a este contenido.

- **Utilización de tecnologías antiguas e inmutables:** por ejemplo, una red a la que no se le han proporcionado aportes de seguridad en el proceso de caracterización y construcción, el uso de controladores antiguos, protocolos y comunicación tradicional basada en tecnologías clásicas obsoletas y sin soporte. De ahí que haya dificultades para ejecutar antivirus o actualizaciones de seguridad, etcétera.

Adaptación del modelo CID como modelo DIC al entorno TO

En el mundo de la protección de datos, el objetivo es la información. Los daños a la información pueden dar lugar a la pérdida de secretos comerciales y/o datos sensibles, al deterioro de la disponibilidad de los datos, así como a incidentes de violación de datos (por ejemplo, la interrupción de la información). Estos sucesos se clasifican en las siguientes categorías:

C (confidencialidad)

I (integridad)

D (disponibilidad)

En el mundo operativo, la mayor parte de la atención de la defensa no se centra solo en la información confidencial y los datos sensibles, sino en los aspectos de seguridad y las consecuencias operativas del negocio relacionadas con el proceso de la línea de producción, que pueden ser causadas por un ataque cibernético, el cual puede dar lugar a daños a la vida humana, ambientales y económicos importantes (en caso de daños a la continuidad del negocio). En vista de ello, es necesario adaptar el modelo reconocido de CID a un lenguaje dedicado, que sea adecuado para el entorno TO, el personal operativo, los ingenieros de producción, los ingenieros de proceso, etcétera.

Al realizar un proceso de evaluación de riesgos, se puede trabajar, por ejemplo, con uno de los dos modelos que se presentan a continuación.

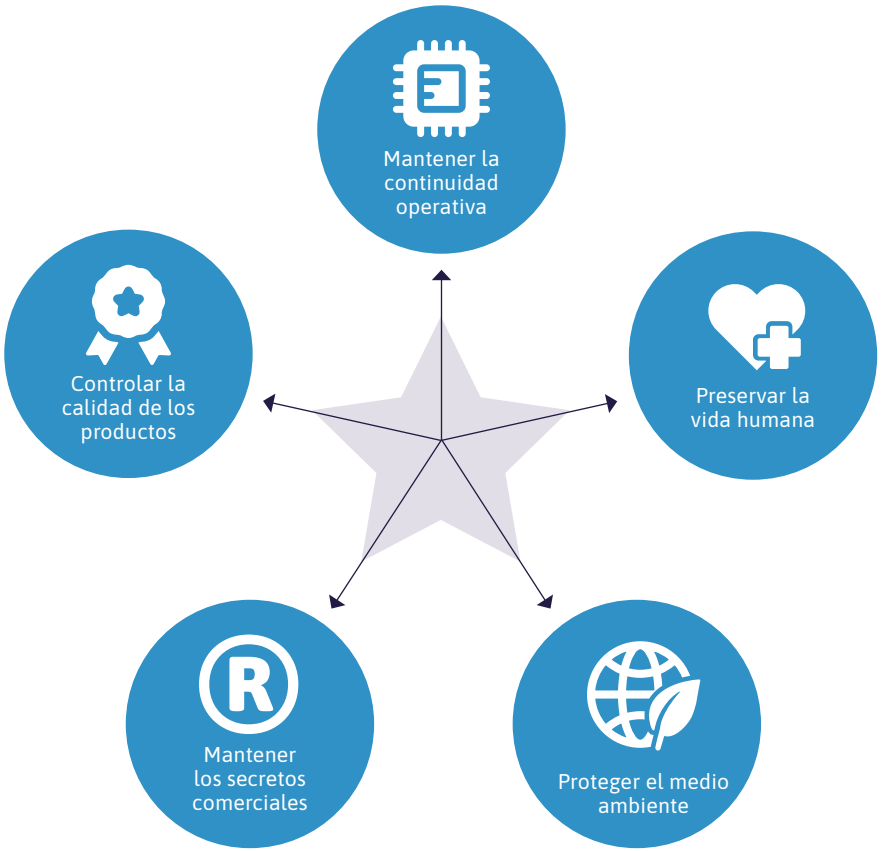
Modelo DIC

Este modelo invierte el orden de los parámetros del reconocido modelo CID. El cambio refleja la importancia de la disponibilidad y continuidad empresarial en la línea de producción. Dado que el objeto de defensa en el mundo de las TO es el proceso operativo, la primera prioridad es la capacidad de la organización de seguir produciendo. La confidencialidad de los datos y la información adquiere un nivel de prioridad un poco diferente. Hay que tener en cuenta que a veces la fiabilidad de los datos puede verse comprometida en casos de riesgo para la vida humana e incidentes de seguridad. En esas oportunidades, muchas entidades priorizarán el parámetro I al D o continuidad del negocio. También se aplicarán entradas para mantener la lógica del controlador y examinar los indicadores de campo y de verdad.

Modelo en estrella: basado en NISTIR 8183

Este modelo se centra en las consecuencias del daño. Estas se enfocan en el daño potencial como resultado de la realización de un evento cibernético sobre la continuidad operativa, la conservación de la vida humana, la protección del medio ambiente, el control de calidad y los secretos comerciales. Este modelo está representado por el diagrama que se muestra en el gráfico 10.

Gráfico 10. Modelo en estrella



Resumen de las diferencias entre el entorno TI y el entorno TO

Cuadro 3. Diferencias entre el entorno TI y el TO

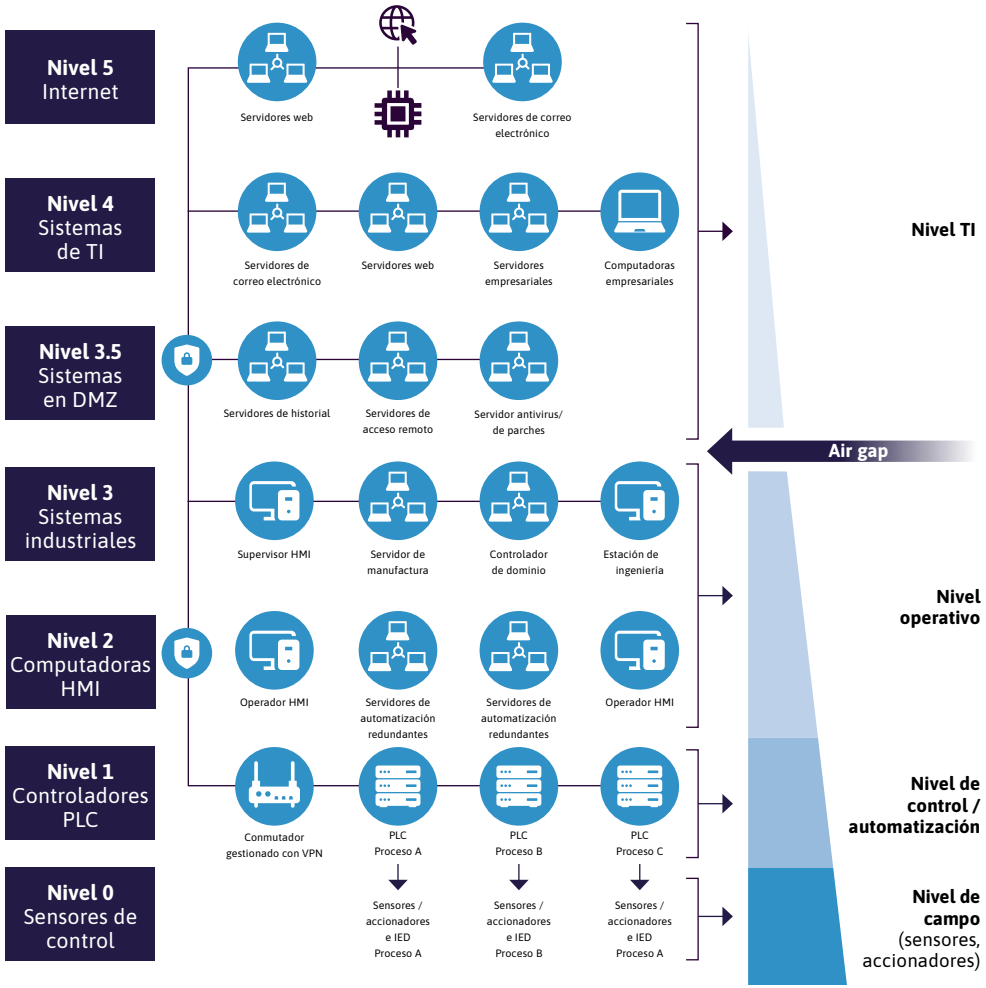
Categoría	Red de control industrial	Red de TI
Requisitos de rendimiento	Precisión en la sincronización horaria	La sincronización exacta puede ser comprometida (y actualizada en una frecuencia diferente)
Requisitos de disponibilidad	Debe haber una disponibilidad continua y cualquier tiempo de inactividad debe planificarse con suficiente anticipación	Es deseable una disponibilidad máxima (a veces sujeta a la disponibilidad, según la gestión de riesgos)
Gestión de riesgos	El riesgo para la vida humana es una prioridad absoluta, junto con los riesgos físicos, operativos, normativos y medioambientales	Mantener la información crítica y la privacidad, y el riesgo empresarial (financiero, de imagen)
Enfoque en la defensa	Protección de equipos finales, procesos de fabricación y producto acabado (en caso de que el producto pueda ser interrumpido, como dosis de alimentos, productos farmacéuticos)	Protección de los activos informáticos y de la información y datos almacenados en su organización

Categoría	Red de control industrial	Red de TI
Ejecución de *software* y actualizaciones	La ejecución de *software* y actualizaciones debe probarse primero fuera del entorno de producción para no perjudicar el rendimiento del sistema, lo que supone un alto costo de creación de un entorno de laboratorio. Por otra parte, muchos sistemas instalados en redundancia, así como la configuración activa de redundancias, reducen estos riesgos, por ejemplo, mediante el traspaso de responsabilidades del PLC 1 al PLC 2, donde después de completar los trabajos programados en el primer controlador, se procede a revertir el traspaso y posteriormente a realizar las mismas labores ahora en el PLC 2. Los datos de planificación para la configuración y la modificación y el endurecimiento de los ajustes predefinidos deben comprobarse	El *software* y las actualizaciones están integrados en los entornos informáticos y, por lo tanto, están más adaptados
Interacciones de emergencia	La capacidad del proveedor o fabricante para facilitar la respuesta del operador y las operaciones de emergencia son fundamentales. A veces, este enfoque también se requiere de forma rutinaria para ofrecer asistencia (por ejemplo, para un evento ocurrido o para la supervisión de datos con fines operativos)	Capacidad de cerrar un enfoque de comunicación de emergencia, y de responder al incidente a través de varias partes independientes
Funcionamiento del sistema	Gestión cuidadosa del cambio, operación de una variedad de sistemas dedicados	Sistemas adaptados al cambio, los sistemas más conocidos
Comunicación	Variedad de protocolos	Comunicación estándar en protocolos conocidos
Gestión de cambios	Se requieren pruebas exhaustivas en entornos de prueba, se precisa una atenta planificación de todo cambio	Cambios estándar, procesos regulados y comunes
Soporte gestionado	Soporte de acuerdo a cada fabricante de forma individual	Permite una variedad de capacidades de soporte
Acceso a los componentes	Los componentes pueden encontrarse aislados o distribuidos a nivel nacional, normalmente se requiere seguridad física adicional	Los componentes suelen agruparse en el sitio en salas de servidores y son accesibles
Ciclo de vida de los equipos	Décadas	Años individuales
Tolerancia ante daños a la continuidad del negocio	Muy baja	Muy baja
Actualizaciones de *software*	Pocas	Frecuentes
Conciencia y conocimientos cibernéticos	Generalmente bajos	Generalmente existentes

Riesgos de ciberseguridad según las capas del modelo Purdue

Los ciberataques pueden explotar la vulnerabilidad de cada una de las capas (o zonas) del modelo Purdue y sus transiciones. Esta sección revisa los ataques que utilizan la comunicación o el canal que conecta las capas del modelo (por ejemplo, pasar de la capa 0 a la capa 1).

Gráfico 11. Zonas de solapamiento entre los modelos Purdue y triangular



Riesgos de ciberseguridad de la capa 0

En esta capa se encuentran los sensores y controladores que supervisan el funcionamiento de las máquinas o los medios activos de operación, como los contactos, sensores analógicos y otros. El riesgo en este nivel se manifiesta en la posibilidad de un ataque físico o lógico, el cual provocará cambios en algún componente (sensor, regulador de presión, temperatura, válvula, etc.) que medirá incorrectamente e introducirá datos erróneos en el análisis de los procesos y sus consecuencias.

Riesgos de ciberseguridad en la transición 0-1

La conexión entre los dispositivos de nivel 0 y el controlador de nivel 1 se realiza a través de conexiones eléctricas o de comunicación en serie. El riesgo en este nivel es la transmisión de datos ficticios y erróneos, así como la posibilidad de manipulación del cableado o la sustitución de un componente material.

Riesgos de ciberseguridad de la capa 1

Mapeo del controlador (PLC/RTU) que gestiona el proceso controlado. Los principales riesgos capaces de incapacitar el proceso son el cambio de la lógica, la configuración o la implantación de código alternativo en el controlador.

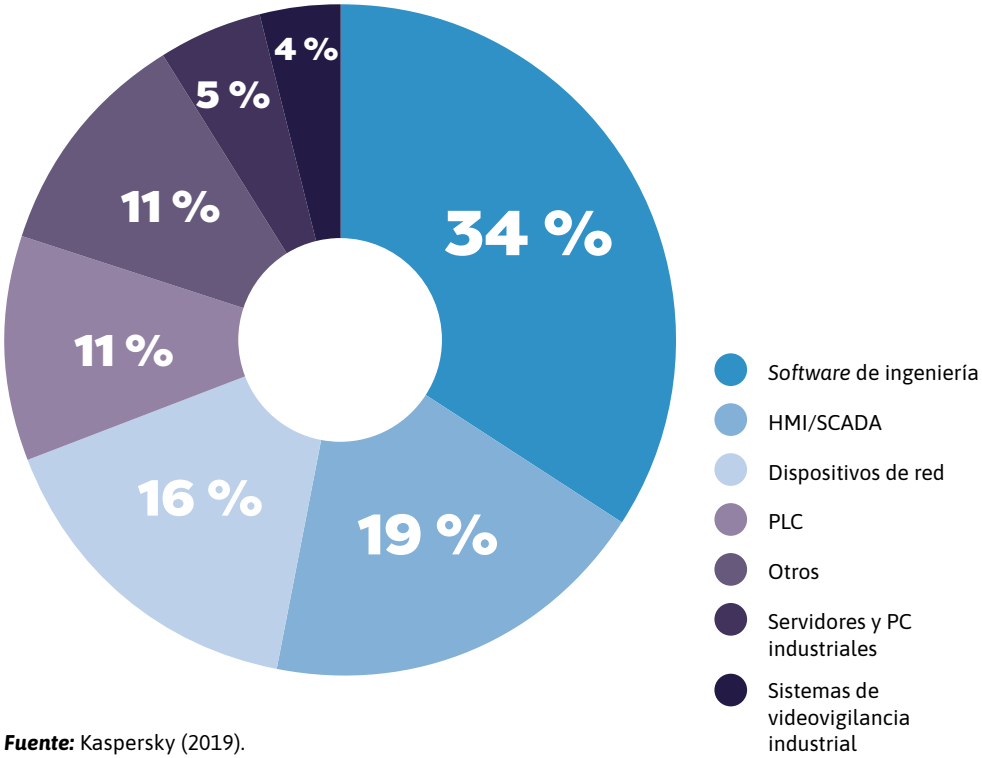
Riesgos de ciberseguridad en la transición 1-2

Esta transición se basa en comunicaciones de red de área local (LAN, por sus siglas en inglés) sobre protocolos (sobre TCP), como MODBUS, 3 DNP PROFINET, IEC 60870-5-104, etc. Los sistemas obsoletos utilizan la comunicación en serie (RS-232), que incluye protocolos como MODBUS, 1-DF, PROFIBUS, etc. El principal riesgo es la posibilidad de conectarse al sistema, especialmente si la comunicación es inalámbrica (sin cifrar), y también la posibilidad de puentear las redes e intervenir en el proceso. Una mala configuración de los sistemas de protección (como el cortafuegos) entre capas y componentes permitirá a un atacante explotar los puertos abiertos para seguir expandiendo y propagando la red.

Riesgos de ciberseguridad de la capa 2

En esta capa se encuentra el centro/servidor de control, que gestiona el proceso e incluye las computadoras HMI. Hay que tener en cuenta que hay sistemas HMI que no reciben actualizaciones de *software* (Windows XP), principalmente por el temor a que los sistemas se caigan después de la actualización. Estos sistemas se encuentran en la sala de control y existe el riesgo de que una persona no autorizada lleve a cabo una acción no autorizada, como insertar un dispositivo USB en una de las computadoras, y provoque la propagación del daño. Esta capa también contiene un servidor de ingeniería, que tiene información operativa sobre el *software* del controlador y también del *software* del centro de control.

Gráfico 12. Mapeo de vulnerabilidades por componentes en el entorno ICS



Fuente: Kaspersky (2019).

Capas adicionales del modelo

- **Capa 3:** la capa operativa en la que se encuentran las computadoras y los servidores operativos.
- **Transición DMZ-3 (zona desmilitarizada):** esta red transmite los datos del sistema de control en el protocolo TCP/IP.
- **Capa DMZ:** esta red cuenta con sistemas informáticos cuya función se encuentra dentro de la DMZ.
- **Transición DMZ-4:** en esta red se transmiten los datos del sistema de control en el protocolo TCP/IP al entorno de gestión, a los puestos de los ingenieros y a las estaciones de trabajo.
- **Capa 5:** esta red contiene los sistemas informáticos que sirven a los sistemas TO (a veces estas estaciones están conectadas a Internet).

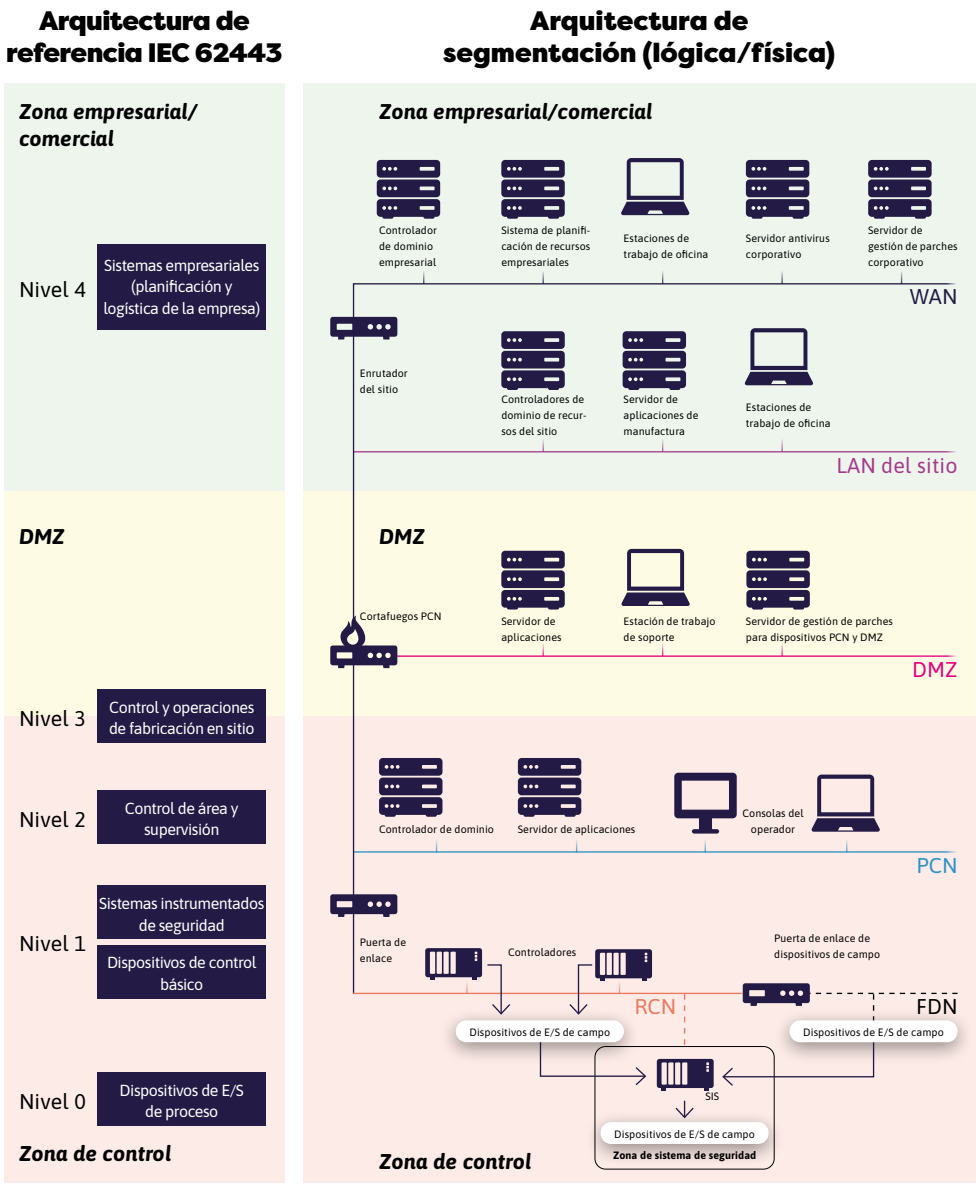
La configuración e implementación del cortafuegos en el entorno ICS es un evento complejo en un entorno TO, a veces por razones de seguridad, entre otras.

La distribución y configuración deben hacerse conforme el modelo Purdue y con las siguientes directrices:

- Diseñar el cortafuegos para que aborde los movimientos de datos entre los entornos TO y TI y los clásicos incidentes y problemas con el entorno ICS, incluidos los ataques dirigidos, los ataques de amenaza persistente avanzada (APT, por sus siglas en inglés), etcétera.[15]
- Definir reglas para evitar la comunicación interna y externa no autorizada.
- Restringir el acceso desde la red de la empresa a la red operativa de manera que se impidan las consultas o los comandos directos a los controladores.
- Garantizar los ajustes y la capacidad de detección de amenazas en los protocolos de TO.
- Establecer ajustes del cortafuegos que sean adecuados para el soporte de los proveedores fuera de la organización.

15. Más información disponible en: **https://www.energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf**.

Gráfico 13. Asignación de componentes en el modelo de capas (norma IEC-62443-3-1)



- Establecer los ajustes del cortafuegos relacionados con la conectividad inalámbrica (según sea necesario y tras un proceso de aprobación de la organización), para evitar las comunicaciones ilegítimas y la explotación de oportunidades de ataque en estos canales.

- Implantar un proceso para recopilar y analizar los identificadores de ataque y definir las definiciones correspondientes.

- Establecer insumos para gestionar los privilegios fuertes para los cambios en el sistema del cortafuegos.

- En el proceso para garantizar el cumplimiento de los requisitos de seguridad, asegurarse de que las medidas de protección y los ajustes del cortafuegos no creen puntos de fallo.

Aspectos destacados de las configuraciones del cortafuegos dedicado basadas en el modelo Purdue

- **Capas 4-5:** en ocasiones, se trata de un entorno conectado a Internet o a los sistemas conectados a Internet. Por ese motivo, en esta capa debe garantizarse la implementación y definición de reglas para la prevención de la comunicación directa y abierta (saliente y entrante) a Internet, con el fin de evitar la comunicación no deseada, los ataques de DoS, la corrupción o la prevención de la mensajería interna.

- **Capa 3:** se proporcionarán entradas dedicadas para la diferenciación frente a la capa 4.[16]

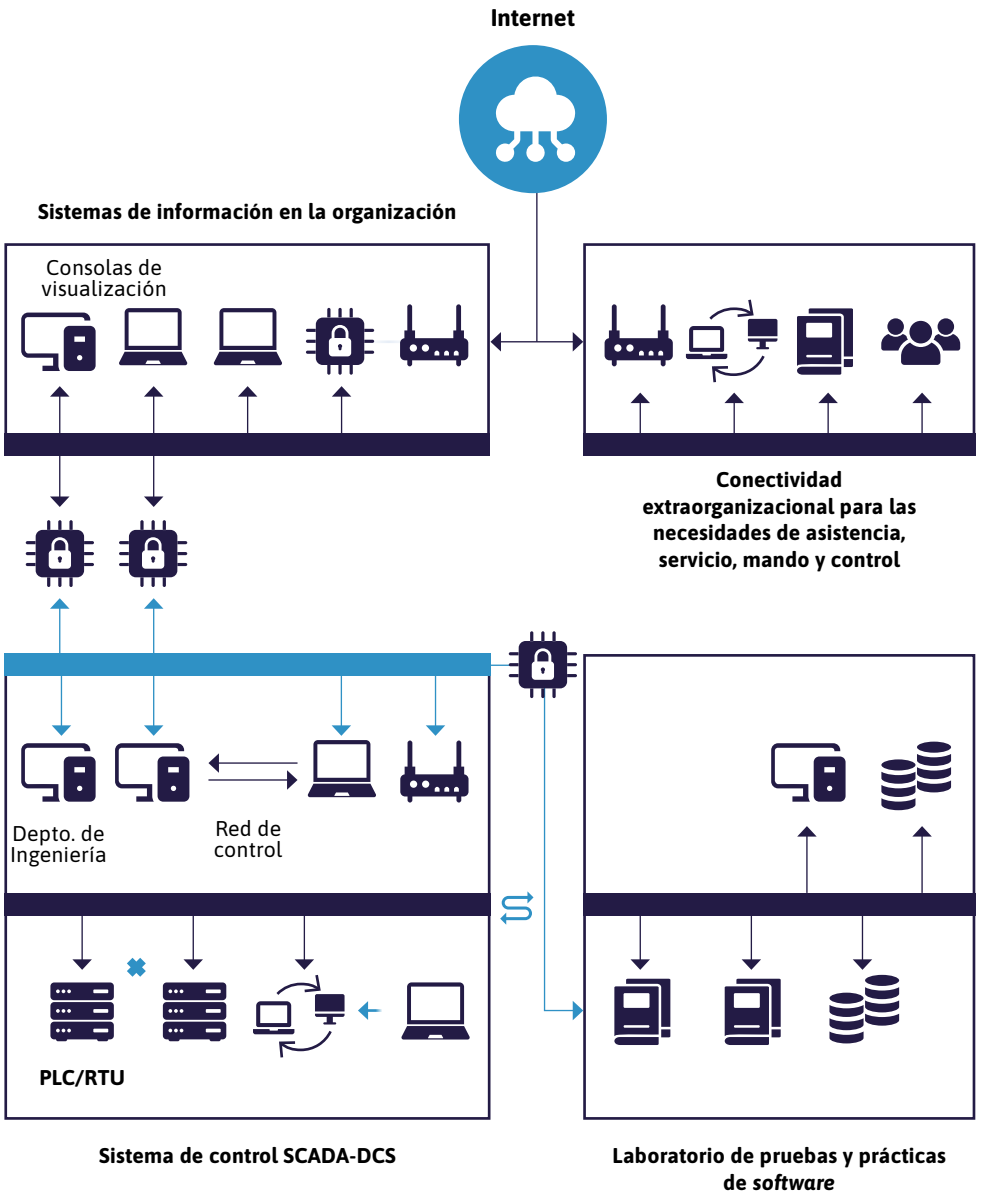
- **Capas 0-2:** compuesta por la capa de sistemas de control, la HMI y su función de permitir la supervisión y control de los procesos de mando y control, para facilitar la intervención del operador según sea necesario y los permisos que se le otorguen. Las definiciones y reglas del cortafuegos que deben aplicarse son contra la derivación de las comunicaciones, las posibles acciones que impliquen el riesgo de causar daños y las acciones no autorizadas (tanto en las leyes como en la restricción de la comunicación no deseada de las capas superiores e inferiores).

Atención a la estructura global del sistema en la organización

A diferencia del modelo Purdue y de otros modelos, se consideran cuatro áreas conectadas entre sí (gráfico 14).

16. Más información disponible en: **https://www.sans.org/white-papers/36327/**.

Gráfico 14. Interfaces en las áreas de conexión



Conectividad de TI

La conectividad entre los entornos TI y TO también existe en los entornos industriales. Se trata de permitir que el entorno de gestión realice su trabajo. Sin embargo, la conectividad con la infraestructura de TI (y a veces la conexión a Internet) expone la red a muchos peligros.

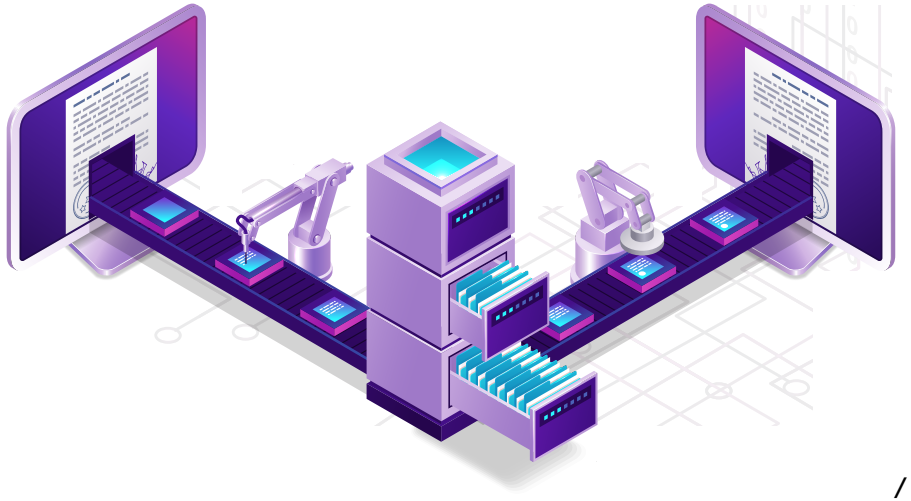
Laboratorio de pruebas del sistema

Este sistema incluye un sistema de control que simula el sistema real (*digital twin*). El entorno está conectado de forma segura al sistema de control y se usa para las pruebas de *software*, la formación de operadores y las pruebas de dispositivos. Si bien hay mecanismos de seguridad e interconexión seguros, existe el riesgo de vulneración de este entorno.

Conectividad extraorganizacional para necesidades de asistencia, servicio, mando y control

Esta área incluye las partes externas que deben conectarse a los sistemas, incluidos los distribuidores, los proveedores de servicios de soporte, los empleados que prestan asistencia fuera de la organización, etc. La preocupación y el peligro estriban en la explotación de esta conexión con fines de ataque, incluidas las amenazas de ataque de intermediario (MITM, por sus siglas en inglés), el ataque de DoS, la explotación por partes hostiles, etcétera.

El entorno de los sistemas operativos y de control (línea de producción) incluye el proceso de producción, los ordenadores de los ingenieros, los sistemas HMI y los controladores.



/03.
Evaluación y gestión de riesgos en los ICS y principios para tratarlos en un plan de trabajo

Proceso de gestión de riesgos de ciberseguridad como parte de la evaluación y gestión de riesgos

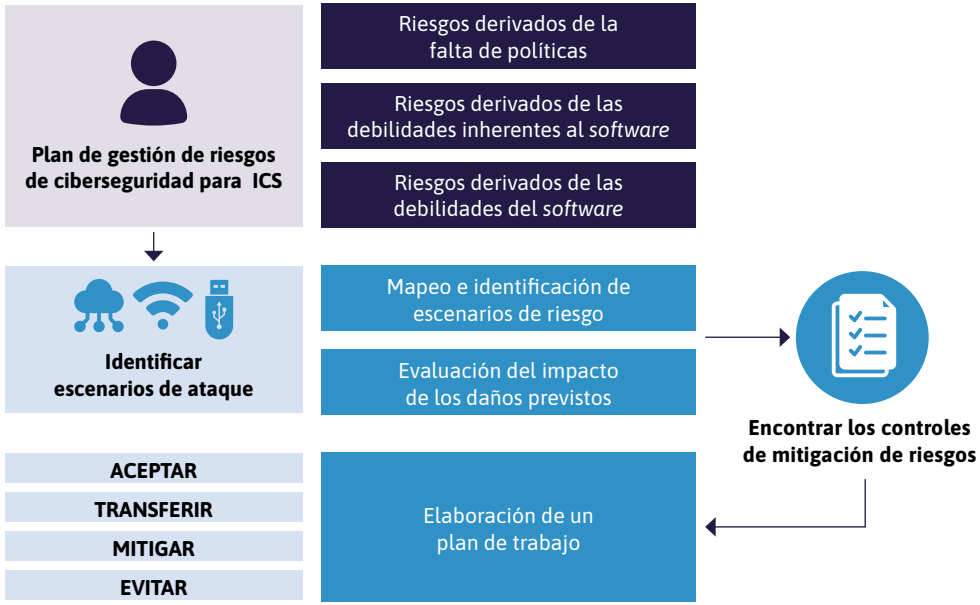
El objetivo del proceso de gestión de riesgos de ciberseguridad es examinar los riesgos de la organización y, posteriormente, reducir el impacto de eventos excepcionales. El proceso incluye la formulación de escenarios de riesgo que pueden perjudicar a la organización, la evaluación del potencial de daño durante su realización, la evaluación de la probabilidad de realización del escenario, la priorización de los escenarios para manejarlos de acuerdo con su intensidad, que es una combinación del impacto del riesgo y la probabilidad de realización, y finalmente la caracterización de un plan de mitigación de riesgos.[17]

17. Más información disponible en: **https://pdfs.semanticscholar.org/cb14/b23b9d0d4242edb1057b722e7a6f923d4885.pdf**.

El proceso de gestión de riesgos en los entornos ICS es importante y complejo. Los ICS son sistemas críticos diferenciados, que utilizan protocolos, *hardware* y *software* diferentes y a veces mixtos. Por otra parte, los conocimientos de los cuales disponen los profesionales informáticos, los costos de explotación, el mantenimiento, las actualizaciones y la evitación de daños continuos en el proceso de producción (como el dilema de la actualización de parches en un entorno de producción) constituyen un reto y son únicos en el proceso de gestión de riesgos en el entorno ICS en comparación con el entorno informático.

Este proceso se lleva a cabo de forma cíclica en función de los cambios tecnológicos, organizativos, amenazas, nuevas capacidades de ataque, etc. El propósito del proceso es llevar a cabo una evaluación adecuada del riesgo de forma aceptable para todas las partes de la organización (dirección, personal de la línea de producción y entidades informáticas) y, posteriormente, traducirlo en un plan de trabajo específico para reducir el impacto de eventos excepcionales y prevenir daños como incidentes de seguridad, daños a la vida o daños a la línea de producción.

Gráfico 15. Proceso de gestión de los riesgos de ciberseguridad y plan de trabajo para el entorno ICS



Mapeo de los riesgos

El mapeo de riesgos se basa en los siguientes procesos (y su sinergia):

01

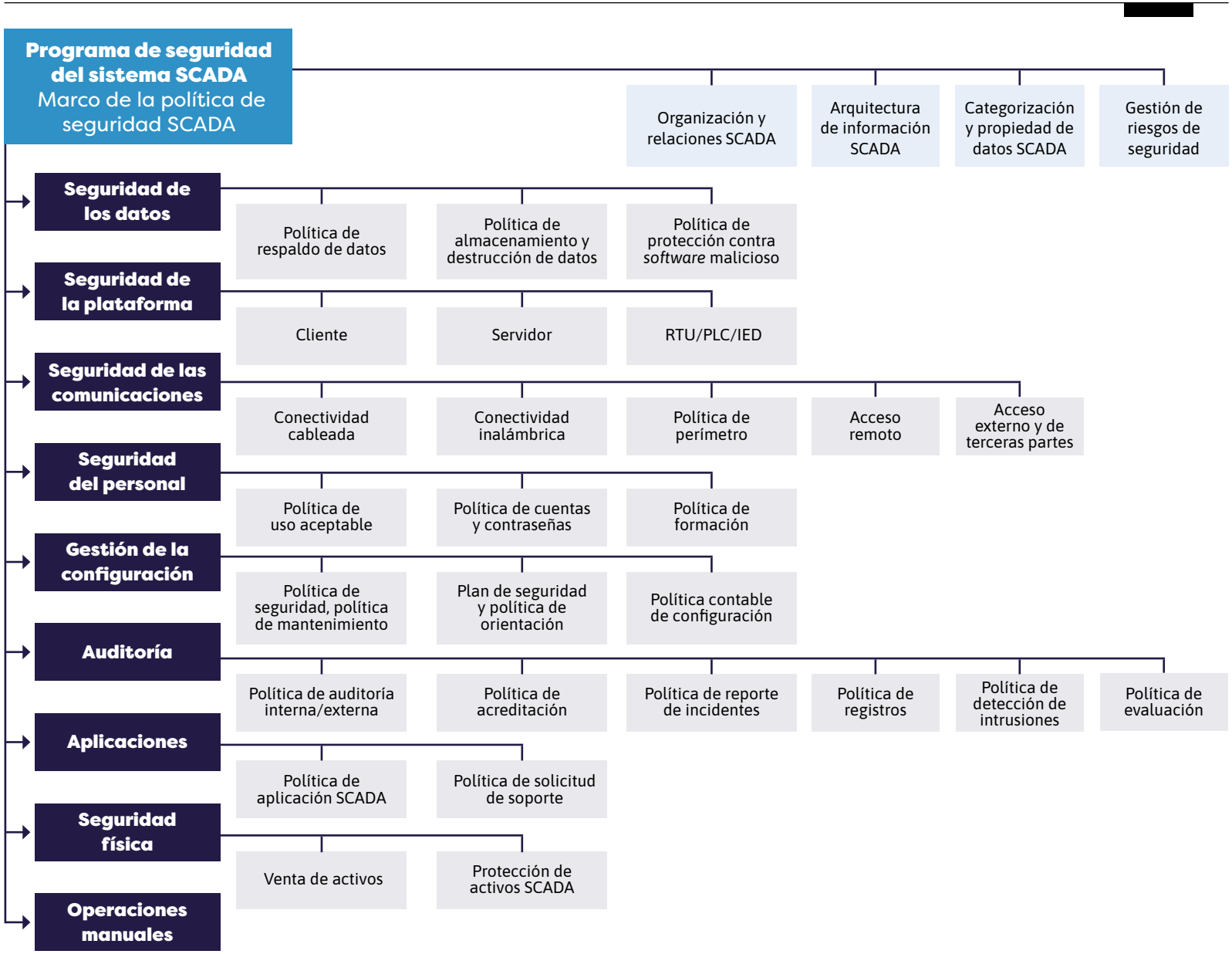
Mapeo de activos: la fase de mapeo también vincula los activos de TI/TO (véase la sección **"Aplicación de la metodología de ciberdefensa en organizaciones de categoría B"** de la ***Metodología de ciberdefensa para organizaciones 1.0***).[18]

02

Mapeo de riesgos resultantes de la falta de políticas (mediante el mapeo de regiones y problemas sin política).

El gráfico 16 permite, por un lado, formular políticas por áreas de actividad y, por otro, identificar los riesgos en las áreas en las que no existe ninguna política.

Gráfico 16. Marco de la política de seguridad SCADA en la organización



18. Puede encontrarse la ***Metodología de ciberdefensa para organizaciones 1.0*** en **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad**.

El proceso de mapeo será el siguiente: se realizará una descripción de la arquitectura del sistema y de la interfaz de los componentes. Esto **permitirá obtener una imagen visual instantánea del entorno de red y de la dependencia de varios componentes** y de diferentes tipos (por ejemplo, varios controladores diferentes), comunicación y protocolos, **y señalar los riesgos derivados de las políticas, los puntos débiles del *hardware* y del *software*, etcétera.**

El proceso de mapeo de riesgos relativos a estos procesos requiere:

- **Conocimiento del proceso empresarial y de los componentes utilizados** (incluidos el mapeo de sensores, redes y subredes, tipo de comunicación, componentes participantes y topología lógica del entorno).

- **Identificación de los escenarios de riesgo,** que también se basan en la inteligencia y el historial de eventos en la organización y en el sector. Este proceso también va acompañado de una revisión de los procesos críticos de la organización y de cómo la viabilidad puede afectar a estos procesos. Los escenarios de riesgo dependen, entre otras cosas, de quiénes tienen interés en atacar la organización, sus capacidades y las herramientas a su disposición, y los ataques pasados. Para tal fin, se puede utilizar un banco de escenarios, un cuadro de riesgos común, como el que se incluye en ***Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)***,[19] o el cuadro 4.

- **Evaluación del impacto de los daños previstos,** si procede, en el proceso operativo, en los eventos de seguridad, en los daños operativos, como la desactivación de un sistema o controlador único de forma que se dañe la línea de producción, en los daños financieros, etcétera.

- **Definición de la reacción defensiva** y los controles compensatorios necesarios.

> **Nota**
> Para obtener una plantilla de muestra para realizar un estudio de riesgos en entornos operativos y para concienciar a la Dirección de la organización sobre el tema, consulte los documentos complementarios de la colección ***Mejores Prácticas en Ciberseguridad,*** desarrollados por la INCD y disponibles en la web del Banco Interamericano de Desarrollo.[20]

19. Este documento será publicado próximamente dentro de esta serie de guías de buenas prácticas en ciberseguridad.
20. Pueden encontrarse los documentos en: **https://publications.iadb.org/es/publicaciones?keys=incd**.

Cuadro 4. Escenarios de riesgo comunes en el sector ICS

1	Riesgo derivado del uso de sistemas antiguos sin soporte que no tienen capacidades de seguridad avanzadas, y de la falta de disponibilidad de actualizaciones de seguridad al final de su vida útil.
2	Riesgos en la conexión de componentes con interfaces inalámbricas.
3	Aumento de la superficie de ataque debido al uso frecuente de la interconexión (canales de toma de posesión [*takeover*], soporte y descargas de actualizaciones).
4	Escasez de expertos en ciberseguridad en la línea de producción (planificación, soporte, gestión de riesgos, etc.).
5	Entornos no regulados, que permiten el salto de las implementaciones de *air gap* y la propagación entre redes.
6	Riesgos de ciberseguridad derivados de los procesos de la cadena de suministro (como puertas traseras y procesos con potencial de riesgo en el eje de la cadena de suministro, incluido el uso de un técnico de TI compartido entre varios clientes).
7	Lagunas de seguridad y puertas traseras integradas en el *software* (imposibilidad de integrar soluciones de protección de terceros).
8	Oportunidades de penetración física y falta de aportes para la prevención.
9	Políticas irregulares de actualización de antivirus y parches (seguridad y operaciones).
10	Error humano (operador), que puede provocar brechas de seguridad y oportunidades atractivas para los atacantes.

Gestión de riesgos en el entorno ICS frente a la gestión de riesgos en el entorno TI

El proceso de gestión de riesgos en el entorno ICS es diferente del proceso de gestión de riesgos en el entorno TI.

Cuadro 5. Consideraciones para la gestión de riesgos en los entornos ICS frente a los entornos TI

Factor	TI	TO/ICS	Notas
Conexión con los procesos empresariales	Importante	Obligatoria	La evaluación de riesgos en este entorno no puede realizarse sin que el proceso se reconozca tal y como se desprende de conversaciones con el ingeniero de procesos y las partes operativas. La detección de amenazas y vulnerabilidades no es posible sin un conocimiento profundo del flujo de información y de los componentes del proceso.
Capacidades de defensa	Existen soluciones de protección comercial y se dispone de muchos conocimientos profesionales en este campo	Muchas soluciones de protección no son adecuadas, son engorrosas y/o irrelevantes para este entorno. La capacidad legal y operativa para instalar una solución de defensa y herramientas de monitorización para realizar escaneos entre otros procesos en este entorno es muy limitada	Hay soluciones comerciales dedicadas al mundo de los ICS, pero son menos robustas y más laboriosas que las soluciones para el entorno TI, donde hay una mayor oferta y más experiencia en el campo. Además, la resistencia de los operadores a las interferencias y al impacto en los procesos operativos es mayor que la resistencia que hay a veces ante la instalación de componentes de protección de servidores y redes en el entorno TI. La solución suele depender del proveedor de control. No se puede insertar una solución externa.
Consideraciones sobre la variabilidad del entorno complejo	Entorno unificado	Entorno complejo	Hay diferencias entre los entornos y consideraciones complejas del entorno TO en donde suelen tener equipos con una vida útil de 15 años, así como un contexto en el que no existen actualizaciones regulares de *software* y protocolos. Estas características se deben, en parte, a las necesidades operativas de las líneas de producción,[21] que a veces no son compatibles con las soluciones de seguridad tradicionales y no son bien conocidas por los profesionales de informática.

Factor	TI	TO/ICS	Notas
Potencial de daños	La mayoría de los daños serán financieros, con daños secundarios de reputación, privacidad y otros	Los daños también aparecen como interrupción de la línea de producción y daños a la vida humana	Daños que suponen un perjuicio para el estilo de vida normal (también a nivel estatal).
Conclusión	**Protección de los entornos ICS:** la organización se enfrenta a una capacidad de defensa muy limitada con respecto a las partes propietarias de los recursos, con intereses no necesariamente alineados a la ciberseguridad que pueden causar un daño inmenso. Esto subraya la necesidad de que las organizaciones consoliden principalmente su capacidad de vigilancia y reacción para proteger dichos entornos.		

21. Para más información, véase ***Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds*** disponible en: **https://ieeexplore.ieee.org/document/7428063**.

/04. Controles del entorno ICS

La ciberprotección del entorno ICS requiere integrar la protección en "circuitos de seguridad" utilizando varios métodos y tecnologías de ciberprotección. Dado que no existe una tecnología única para todos los tipos de sistemas, se necesita una variedad de controles adaptados específicamente al nivel de riesgo, a la implementación del sistema, su funcionamiento y estructura, a las tecnologías de comunicación, al espacio geográfico en el que se implementa el sistema (ciudad, fábrica, edificio), etc.

El banco de controles que se presenta en el cuadro 6 está dedicado y es adecuado para el entorno ICS. Esos controles se han seleccionado en función del entorno ICS, los componentes informáticos, los sistemas de interconexión y las tecnologías. El éxito de la implementación y puesta en práctica de los controles de seguridad para mitigar los riesgos depende de la organización, su tamaño, su naturaleza y complejidad (de este modo, algunos controles pueden reducir los riesgos en entornos mixtos, mientras que en entornos aislados se puede prescindir de algunos).

Un proceso adecuado de selección e implementación de controles apropiados implica una gestión de riesgos adecuada.

Controles de ciberseguridad en entornos ICS

Cuadro 6. Controles de seguridad adecuados para controladores industriales (extraídos de la ***Metodología de ciberdefensa para organizaciones 1.0***)

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.1	Política de controladores industriales	Redactar, gestionar y auditar las políticas de la organización para la protección de los entornos de control industrial. Esta política responde al nombramiento y la definición de un rol, que incluye determinar la división de responsabilidad entre los titulares y responsables de la red TO y las redes tangentes.	La organización definirá su política de sistemas operativos, incluyendo lo referente a las políticas de acceso remoto, las actualizaciones de versiones, las actualizaciones de *software*, el mantenimiento de terceros, etc.	La redacción de políticas y procedimientos de soporte puede implementarse. Se deben definir los requisitos únicos para el entorno de los controladores industriales (producción, logística, control ambiental, generación de energía, entre otros). Deben tratarse los aspectos normativos existentes en estos entornos (por ejemplo, Administración de Alimentos y Medicamentos [FDA, por sus siglas en inglés], Dirección Nacional de Ciberseguridad de Israel). Compruebe que el documento normativo regule y defina el organismo responsable dentro de la organización. La división de responsabilidades abarcará varias áreas, como quién es el responsable de las actualizaciones de *software*,	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
				del inicio de sesión de los proveedores, de la carga de archivos para las actualizaciones recomendadas, etc., porque el fideicomiso de ciberseguridad del entorno ICS tendrá una carta de nombramiento oficial firmada y aprobada por la Gerencia de la organización.	
12.2	Política de controladores industriales	Definir las normas de uso adecuado de los equipos en el entorno de producción y colocar la señalización que las explique.	Se definirá la señalización que explique las prácticas de seguridad de los datos en los puestos de trabajo que administran y supervisan el entorno de producción.	La señalización puede incluir el uso de estaciones de trabajo compartidas, dispositivos de medios extraíbles, desconexión de los usuarios, etc.	1
12.3	Política de controladores industriales	Definir los procesos sensibles donde hay entornos de control industrial según su nivel de sensibilidad.	La organización mapeará los procesos en los que hay entornos de control y definirá los principales procesos empresariales que implican estos controles con el fin de comprender el nivel de daño empresarial y normativo que podría resultar de dichos entornos.	Documentar los procesos de mapeo y los entornos según la gravedad.	2
12.4	Política de controladores industriales	Separar las redes de control de otros sistemas y redes externas.	La organización separará las redes de control, las de los usuarios o las de los servidores para restringir el acceso directo entre las redes.	La separación puede llevarse a cabo utilizando cortafuegos y VLAN separadas para cada red de control. Si se tiene la opción, es preferible separar mediante un diodo unidireccional y permitir solo la salida de datos e información fuera de la organización.	2
12.5	Comunicación de controladores industriales	Separar el sistema de gestión de controladores de equipos industriales y los componentes operativos del sistema.	Implementar una separación adecuada entre la red de controles operativos y el sistema de gestión de los controles.	En todos los casos en que el sistema conecte la planta de producción con otros entornos elevados (de acuerdo con el modelo Purdue) para la elaboración de informes de gestión u otras necesidades, y especialmente en los casos en que el entorno TO esté conectado a la nube, los controles deben establecerse de acuerdo con la sección "**11. Computación en la nube pública**" de la ***Metodología de ciberdefensa para organizaciones 1.0*** o alguna norma equivalente.	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.6	Comunicación de controladores industriales	No conectar a la red de controles de producción aquellos dispositivos que no sean controles del entorno de producción.	La organización no instalará en la red de controles equipos que no formen parte del ICS. Los equipos que deban conectarse lo harán a una red separada y la comunicación se habilitará individualmente.	Si es necesario hacerlo a fin de conectar diferentes equipos para las interfaces con los sistemas de producción, se debe conectar por segmento de red separado detrás del cortafuegos.	1
12.7	Comunicación de controladores industriales	Habilitar el acceso de los proveedores de soporte a la red de producción únicamente con autorización previa y utilizando una comunicación segura e identificada, que permita registrar las acciones del proveedor.	La organización implementará una red de comunicaciones segura para el acceso de los proveedores y revisará este acceso a la organización al otorgar una autorización previa para cualquier conexión del proveedor a la red de control.	Puede aplicarse mediante un sistema de gestión de servidores VPN para usuarios dedicados a cada proveedor (prioridad de usuario para cada empleado del proveedor), que normalmente estará bloqueado y se abrirá solo cuando sea necesario.	2
12.8	Comunicación de controladores industriales	No permitir el acceso directo o indirecto a Internet desde los controladores industriales, así como desde las interfaces del entorno hombre-máquina.		Las redes de control en el cortafuegos se pueden restringir y no se permite el acceso a Internet desde estas redes. También se deben integrar sistemas de blanqueo de archivos para un proceso seguro en la transferencia del entorno.	2
12.9	Comunicación de controladores industriales	Limitar los servicios innecesarios en el entorno de producción y los sistemas de soporte, como las HMI y los sensores inteligentes.	La organización cancelará y/o limitará los servicios innecesarios para todos los sistemas del entorno de control, ya sea a nivel de sistema operativo, de comunicaciones y de aplicaciones.	Puede basarse en los documentos de seguridad de los fabricantes del sistema operativo y las aplicaciones, y cerrar servicios, bloquear puertos, limitar el acceso de las aplicaciones a determinadas funciones, entre otras acciones.	2
12.10	Comunicación de controladores industriales	De ser posible, utilizar una comunicación fiable entre los controles industriales y los equipos terminales.	Usar protocolos que permitan la autenticación de origen y destino y la encriptación del medio que soporta el equipo.	En caso de que se puedan usar versiones seguras de estos protocolos, utilizar estas versiones (SFTP, HTTPS, SNMPv3 y otros).	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.11	Comunicación de controladores industriales	Establecer un sistema de comunicación unidireccional al entorno TO.		Las herramientas de comunicación unidireccional entre los sensores y sistemas deben definirse en entornos sensibles.	4
12.12	Comunicación inalámbrica	Separar las redes inalámbricas en el entorno de producción de las redes inalámbricas empresariales.	La organización implementará una red inalámbrica dedicada y separada de la red inalámbrica empresarial, que se utilizará únicamente para las comunicaciones de la red de control. Esta red no se redirigirá a la red de la empresa y viceversa.	Es preferible evitar el uso de la red inalámbrica en las redes de control, pero de ser necesario para la empresa, esta red se creará por separado y su gestión será también independiente y no estará vinculada a ninguna red interna de la VLAN.	1
12.13	Comunicación inalámbrica	Limitar la comunicación inalámbrica en el entorno de producción mediante el uso de protocolos seguros.		Se debe usar el protocolo de acceso protegido a wifi 2 con una clave previamente compartida (WPA2-PSK, por sus siglas en inglés), siempre que se pueda. Se recomienda emplear una versión basada en certificado digital para estas redes inalámbricas.	1
12.14	Comunicación inalámbrica	Definir un usuario independiente para cada cliente final que utilice la red inalámbrica en el entorno de producción.		Se recomienda conectar la red inalámbrica a un servidor RADIUS dedicado, que autenticará a los usuarios y los gestionará.	2
12.15	Gestión de controladores hombre-máquina	Habilitar el acceso a las HMI por usuarios personales, para cada operador.	La organización definirá un usuario personal para cada persona que trabaje frente a una HMI. Si es un puesto compartido, se podrá usar la identificación mediante tarjeta inteligente.	Si por razones de seguridad el puesto no puede bloquearse, deberán considerarse controles compensatorios (como colocación de cámaras, documentación de acceso a la sala, etc.).	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.16	Gestión de controladores hombre-máquina	Habilitar el acceso a las HMI utilizando una autenticación fuerte.	La organización establecerá una autenticación fuerte con acceso a la HMI.	Se pueden utilizar diversas medidas, como la biometría, las tarjetas inteligentes, contraseña de un solo uso (OTP, por sus siglas en inglés) y otras. Además, debe asegurarse de que las interfaces de equipos sensibles, como el puesto de gestión/ingeniería, las HMI, etc., empleen nombres de usuario únicos y gestionados. Es deseable que el uso de estas cuentas se base en una identificación fuerte en la medida de lo posible.	4
12.17	Gestión de controladores hombre-máquina	Instalar sistemas de monitorización y realizar un registro de actividad en los servidores de gestión.	La organización establecerá sistemas de registro de actividad o registro con énfasis en el entorno de gestión del entorno de producción.	Se pueden utilizar diversas medidas y herramientas, como las herramientas de grabación de la actividad de los usuarios en pantalla, registros de aplicaciones, etc.	2
12.18	Control de códigos maliciosos	Instalar utilidades como herramientas de detección de intrusos en el entorno de las redes de gestión del entorno de producción.		Se puede aplicar usando herramientas como el sistema de prevención de intrusiones (IPS, por sus siglas en inglés), una trampa de tarro de miel (*honeypot*), entre otras. Recuerde que, por motivos de seguridad y funcionalidad, estas herramientas no siempre pueden instalarse en entornos operativos. En estos casos, a veces el uso de herramientas como el sistema de detección de intrusiones (IDS, por sus siglas en inglés) puede ser una respuesta parcial o alternativa.	3

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.19	Control de códigos maliciosos	Instalar herramientas de verificación de firmas de archivos (*integrity checking*) para escanear los archivos que se transfieren al entorno de gestión o que se instalan en el entorno de gestión.		Puede implementarse utilizando una variedad de herramientas de verificación de integridad de archivos.	3
12.20	Control de códigos maliciosos	Instalar herramientas *antimalware* dedicadas en las HMI.		Puede aplicarse usando herramientas *antimalware* dedicadas, adecuadas al tipo de sistema.	1
12.21	Actualizaciones de *software*	Instalar las actualizaciones de *software* del fabricante en los entornos inferiores (prueba antes de instalar en el entorno de producción).	La organización garantizará la instalación de las actualizaciones en el entorno de prueba y las ejecutará a lo largo del tiempo, con el fin de probar la estabilidad del sistema y del proceso.	Puede realizarse al establecer un entorno inferior (al menos parcialmente), desviando la comunicación a este entorno durante la ventana de mantenimiento en el entorno de producción y probando el proceso.	2
12.22	Actualizaciones de *software*	Instalar en el entorno de producción las actualizaciones del sistema operativo soportadas por el proveedor.	La organización aplicará en un plazo razonable las actualizaciones del sistema operativo y de las aplicaciones que reciba del proveedor del sistema y exigirá al proveedor las actualizaciones de seguridad para los fallos graves a medida que se publiquen.	Como parte de este proceso, se debe hacer referencia al método seguro de ingreso de nuevos equipos (como dispositivos y máquinas para la red TO y el entorno operativo). Dada la sensibilidad del asunto, la capacidad de restaurar el sistema operativo y el *software* al estado inicial (estado 0) debe comprobarse usando el *firmware*/sistema operativo de una fuente fiable y reescribiendo los datos históricos que venían con el equipo.	2
12.23	Actualizaciones de *software*	Instalar herramientas de bloqueo de la configuración en los sistemas al final de su vida útil, incluidos los sistemas operativos obsoletos.	La organización implementará herramientas que bloqueen la configuración del sistema en una configuración "limpia", si no hay otras opciones para actualizar el equipo.		3

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.24	Medios extraíbles en el entorno de producción	Limitar la posibilidad de conectar medios extraíbles a los equipos de producción, incluidos los controladores, las HMI y los sensores.	Deberá asignarse una capa de almacenamiento de datos designada para el uso de la red TO a fin de minimizar el área de exposición y reducir el riesgo de salto de la red y del *air gap*. Se debe prestar atención a los casos en los que se conectan los equipos privados de los empleados. Para ciertos puestos, como los trabajadores de la línea de producción, se conecta la telefonía, etc., para la carga o las actualizaciones de versión, etc. La gestión se realizará mediante mecanismos de gestión de dispositivos. Todo componente que se conecte será identificado y aprobado previamente (*white-list*).	Se puede implementar mediante la desactivación de dispositivos USB físicamente (bloqueo de puertos) o lógicamente por política del sistema operativo o las políticas de directiva de grupo (GPO, por sus siglas en inglés). En general, se debe evitar la conexión de medios extraíbles que no pertenezcan a la organización, que serán revisados y aprobados por los equipos cibernéticos de la organización.	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.25	Medios extraíbles en el entorno de producción	Realizar la transferencia de archivos de medios extraíbles a los sistemas de producción únicamente después de sanear los datos de los archivos transmitidos.	La organización implementará un conjunto de archivos blanqueados y los examinará con cuidado usando varias herramientas antes de transferirlos al entorno del controlador. Por ejemplo, puede basarse en una tecnología incorporada o en un proceso de trabajo para la comprobación y el registro previo de: la fuente del archivo (usuario o sitio), la fecha y la hora, la documentación y el motivo por el que se trae el archivo, la identificación única para cada blanqueo, capacidad de investigar eventos de transferencia de archivos.	Puede realizarse mediante la adquisición de una estación especializada de saneamiento de datos o, alternativamente, mediante el establecimiento de una estación dedicada, que incluya varios motores de escaneo diferentes.	2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.26	Redundancia en el entorno de producción	Establecer un conjunto de sistemas de redundancia para los componentes críticos en el entorno de producción.	La organización implementará un sistema de redundancia de servidores y sensores críticos en los entornos de control para la continuidad del proceso.	Para construir la redundancia se recomienda consultar con el proveedor del sistema de control.	2
12.27	Acceso físico al entorno de producción	Restringir el acceso físico en función de las necesidades empresariales y acceder únicamente de forma segura al entorno del controlador industrial, así como a los equipos de comunicación en este entorno.	La organización restringirá el acceso físico a los gabinetes de medios, los concentradores y los puestos de gestión del entorno del controlador. Debe tenerse en cuenta que, incluso cuando se conecta legítimamente (por ejemplo, en beneficio de la ejecución de una prueba de concepto [PoC, por sus siglas en inglés]), el proceso de conexión de componentes ha de realizarse de forma segura.	Puede hacerse mediante salas dedicadas a concentrar comunicaciones y servidores. También se puede realizar el control de acceso mediante etiquetas de acceso y biometría para este entorno.	2
12.28	Separación del enfoque lógico y las redes	Limitar el acceso lógico para las necesidades de la empresa únicamente al entorno de los controles industriales, así como a los equipos de comunicaciones en este entorno.	La organización limitará el acceso de los usuarios corporativos que no tengan relevancia empresarial para el sistema de control e impedirá su acceso a estas redes y equipos.		2
12.29	Separación del enfoque lógico	Limitar el acceso lógico (funcional), en la medida de lo posible, a los sistemas de producción, incluidas las interfaces de control, interfaces de muestra y HMI.	El acceso a los sistemas de gestión se limitará en función de los perfiles de los usuarios. El controlador del sistema no modificará los ajustes y parámetros del mismo. Un usuario administrativo realizará la modificación de los parámetros.	Se puede comprobar con el fabricante del sistema si este puede utilizar diferentes perfiles de usuario.	3

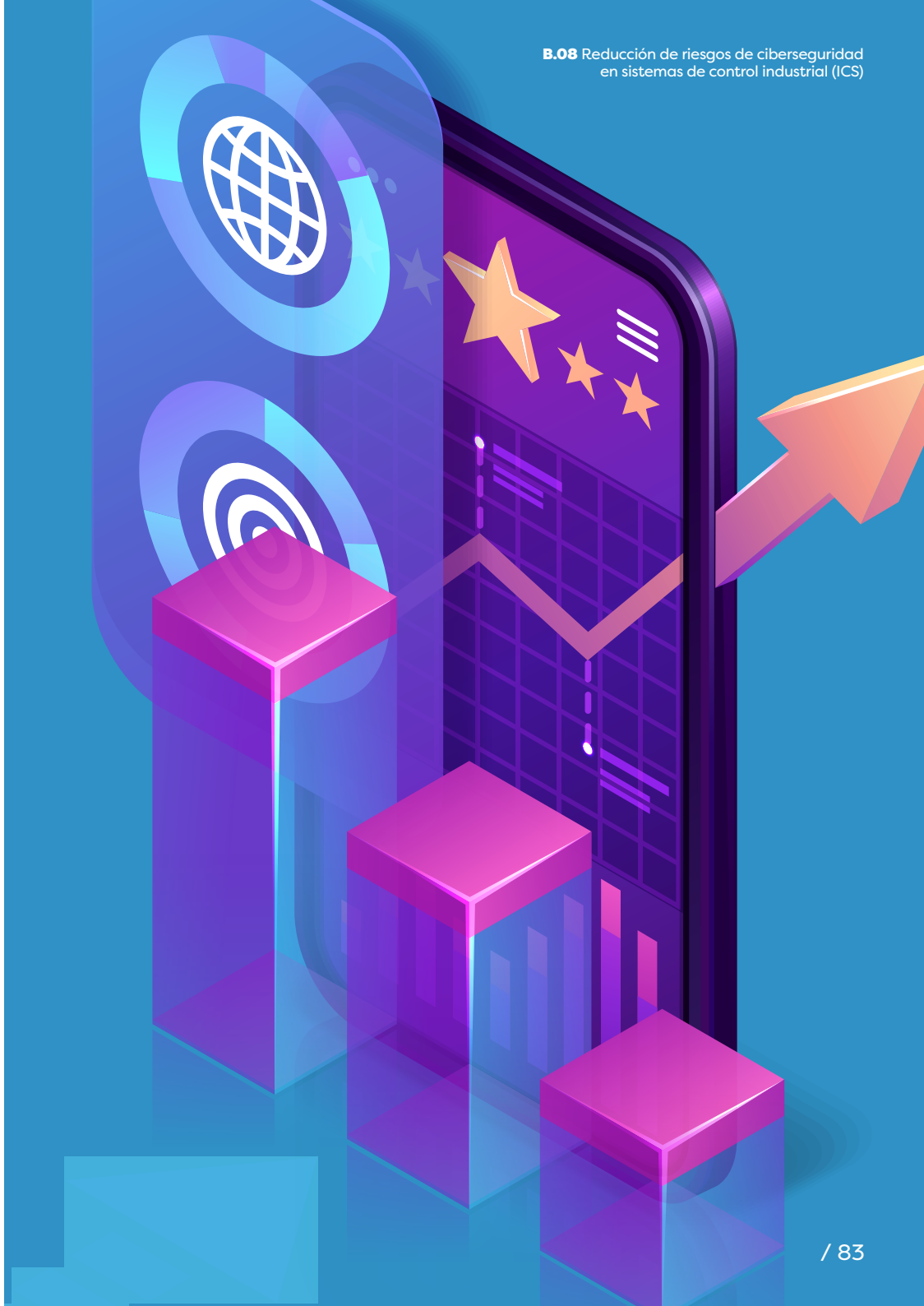
ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.30	Pruebas de solidez	Realizar pruebas de seguridad de la información en los entornos de producción y de gestión y en la interfaz, incluidas las pruebas de penetración.	La organización definirá las pruebas integrales, el esquema para las pruebas que incluirá la variedad de componentes de la red de control, con énfasis en las pruebas de seguridad de la información integral para todos los componentes, con el fin de mantener la continuidad del proceso empresarial.	Pueden llevarse a cabo mediante la comprobación de la configuración del entorno, la realización de simulaciones durante las ventanas de inactividad y la realización de pruebas de penetración en estas redes si es posible y/o durante las operaciones de mantenimiento.	2
12.31	Monitoreo de la seguridad de la información	Establecer escenarios de monitoreo únicos en el entorno de producción y supervisarlos a través de una medida de monitoreo de la organización.	La organización definirá una variedad de escenarios de monitoreo dedicados para el entorno de control según el esquema de amenazas y la importancia del sistema para el proceso empresarial. Debe garantizarse que los sistemas de monitoreo y registro activo se instalen en los activos críticos, como los servidores de gestión o los puestos de ingeniería.	La supervisión de la red en las redes de control es diferente de la supervisión de los sistemas ordinarios, ya que el umbral de sensibilidad es inferior. Cualquier desviación de la cantidad de comunicación normal entre los controles y las interfaces de gestión y los sensores puede indicar un posible incidente cibernético, ya que la actividad en estos entornos es continua y monótona.	2
12.32	Monitoreo de la seguridad de la información	Disponer de una capacidad de supervisión independiente en la red operativa y/o en la red informática.	Este monitoreo examina un cambio en el espacio físico, que es una indicación independiente de la arquitectura de la organización y constituye una anomalía, lo cual requiere una evaluación del personal operativo para la excepción.	Esto puede realizarse, por ejemplo, con la capacidad de leer valores (analógicos y digitales) para medir los cambios de los sensores y accionadores (nivel 0) en una configuración completamente desconectada, que es independiente de la red de explotación (fuera de banda) y no se ve afectada. Estos cambios pueden detectarse midiendo la electricidad, presión, temperatura, etc.	4
12.33	Desactivación de equipos	Al retirar un equipo o al desconectarlo de una fuente externa, verificar los procesos de eliminación de archivos y datos sensibles (como archivos lógicos, contraseñas, etc.) de los sistemas y equipos informáticos.	Al retirar un equipo o al desconectarlo de una fuente externa, deben verificarse los procesos de eliminación de archivos y datos (como archivos lógicos, contraseñas, etc.) de los sistemas informáticos y equipos informáticos y de transferencia, incluidos los procesos de intercambio en las intersecciones, los cambios de entorno, etc.		2

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.34	Ciberinteligencia	Recopilar periódicamente ciberinteligencia y ataques en el mundo de TO (información visible, publicaciones, etc.).	Debe hacerse un seguimiento dedicado de las publicaciones profesionales para la protección de los sistemas informáticos y de los sistemas operativos. Se debe garantizar un proceso regular de recopilación y análisis de la información pertinente procedente de fuentes internas y externas, que sirva de plataforma para los ataques; acciones emprendidas (publicaciones del equipo de respuesta ante emergencias informáticas [CERT, por sus siglas en inglés], fabricantes, proveedores, etc.). Este seguimiento ayudará a la organización a reforzar la seguridad y a endurecer los sistemas con el fin de minimizar la superficie de ataque.		3

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.35	Preparación para emergencias	Redactar, implementar, revisar y actualizar la política de continuidad del negocio en lo que respecta a la ciberdefensa.	Debe crearse un equipo de respuesta a incidentes dedicado para gestionar los incidentes cibernéticos en entornos operativos e industriales. Este equipo incluirá representantes de diversas disciplinas y recibirá la formación correspondiente en los ejercicios. En el marco de la formación deberían revisarse ciberincidentes significativos. Si no se puede capacitar al personal, estas capacidades deberían contratarse en empresas especializadas.	Un puesto de recuperación rápida, que incluya un puesto de ingeniería, con licencias y aplicaciones instaladas en una computadora portátil/red estacionaria que no esté conectada a la red (debe actualizarse una vez cada seis meses y garantizar su operatividad y disponibilidad para el servicio).	3

ID	Familia	Control	Explicación complementaria	Ejemplo de implementación del control	Nivel de control*
12.36	Preparación para la recuperación de desastres	Dedicar los recursos adecuados a crear una continuidad empresarial y prevenir los riesgos de ciberseguridad en el proceso de sincronización temporal.	Se llevará a cabo un proceso para analizar el nivel de efectos de precisión entre los componentes dentro de la red y de otras redes y las redes exteriores. Garantizar la existencia de un proceso de sincronización temporal en la red TO y proteger el proceso con el grado de fiabilidad, precisión y redundancia compensa en la red.		4

Nota: * Complejidad del nivel de control de 1 (bajo) a 4 (complejo).



Anexos

Referencias

- BSI (Oficina Federal de Seguridad de la Información). 2019. Industrial Control System Security: Top 10 Threats and Countermeasures 2019. Disponible en: **https://www.hannovermesse.de/apollo/hannover_messe_2021/obs/Binary/A1087894/Top-10-ICS-Threats_and_Countermeasures.pdf**.

- Di Pinto, A., Y. Dragoni y A. Carcano. 2018. TRITON: The First ICS Cyber Attack on Safety Instrument Systems. Understanding the Malware, Its Communications and Its OT Payload. Disponible en: **https://www.nozominetworks.com/downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf**.

- EnCompass. 2018. Top 10 Automation Trends in 2018. Disponible en: **https://www.encompass-inc.com/top-10-automation-trends-in-2018**.

- INCD (Dirección Nacional de Ciberseguridad de Israel). 2017. Metodología de ciberdefensa para organizaciones 1.0. Disponible en: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad**.

- Kaspersky. 2019. Threat landscape for industrial automation systems. H2 2018. Disponible en: **https://ics-cert.kaspersky.com/publications/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/**.

- Yasinskiy, A. 2016. Dismantling BlackEnergy, Part 3 – All Aboard! Disponible en: **https://socprime.com/blog/dismantling-blackenergy-part-3-all-aboard/**.

Material de lectura complementario

- ANSI/ISA 62443. *Security for Industrial Automation and Control Systems.*

- Bodungen, C. E., B. Singer et al. 2016. *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions.*

- Ginter, A. 2013. *13 Ways through a Firewall: What You Don't Know Can Hurt You.*

- Ginter, A. 2018. *Secure Operations Technology.*

- ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). *Standards and References: Establishing and Conducting Asset, Vulnerability, and Risk Assessments*. Disponible en: **https://web.archive.org/web/20190522215540/https://ics-cert.us-cert.gov/Standards-and-References#conduct**.

- ISO/IEC 27001-2013. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.*

- ISO/IEC 27002. *Information Security, Cybersecurity and Privacy Protection – Information Security Controls.*

- NERC-CIP. *Requirements for Power Utilities – Bulk Power Systems (BPS).*

- NIST SP 800-82 Rev. 2. 2015. *Guide to Industrial Control Systems (ICS) Security.*

- Nunez, M. 2012. *Cyber-Attacks on ERP Systems: An Analysis of the Current Threat Landscape.*

- Sobzak, B. 2018. *Hackers Force Water Utilities to Sink or Swim.*

Esta publicación se propone ayudar a los departamentos profesionales y técnicos de la organización, encargados del escenario de tecnología operativa (TO) en general y de los sistemas de control industrial (ICS) en particular. El documento no pretende sustituir a dichos departamentos, sino servir de herramienta para identificar las cuestiones clave relacionadas con los riesgos de la protección cibernética en el ámbito de los ICS.

La publicación ofrece recomendaciones de protección profesional basadas en normas internacionales, investigaciones y documentos profesionales. Con estas consideraciones en mente, se entiende que la implementación de controles profesionales en el ámbito de los ICS, en una organización específica, requiere un proceso dedicado de gestión de riesgos y el ajuste de esos controles para la organización realizado por profesionales adecuados.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación
- **B.22** Protección de los servicios de nube pública ante amenazas de *ransomware*

Volumen C: Desarrollo seguro de *software*