

Gestión de riesgos cibernéticos en entornos de tecnologías operativas (OT) Guía para Juntas Directivas

Mejores Prácticas en Ciberseguridad



A.10

Volumen A:
Un enfoque metodológico



Cyber Israel
National Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título “Gestión de riesgos cibernéticos en el entorno OT”. © (2020) Dirección Nacional de Ciberseguridad de Israel.

© (2022) Banco Interamericano de Desarrollo por esta traducción.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. 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).

Esta publicación puede descargarse, copiarse y distribuirse, siempre que se otorgue la debida atribución a la Dirección Nacional de Ciberseguridad para la versión original en hebreo y al BID para la traducción en español, y que la publicación no se modifique. Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del BID, de su Directorio Ejecutivo, ni de los países que representa.

El documento original se encuentra disponible en el siguiente enlace: <https://www.gov.il/he/Departments/General/ot>. 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

/Pág. 2

Antecedentes

/Pág. 8

01. Impacto de los incidentes cibernéticos en los objetivos operativos y comerciales

/Pág. 10

02. Administración de ciberseguridad

/Pág. 12

03. Gestión de riesgos cibernéticos en el entorno OT

/Pág. 16

04. Identificación de riesgos cibernéticos típicos de la red OT

/Pág. 21

05. Seguimiento y respuesta a incidentes cibernéticos

/Pág. 23

Referencias

/Pág. 26

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. Prolifera-ron 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 de-

tectaron 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 refuerzen 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

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 orga-

nizaciones 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.



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/reforma-modernizacion-del-estado/cluster-de-datos-y-gobierno-digital>.

Antecedentes

En los últimos años se ha producido un aumento en el número de incidentes cibernéticos notificados en un entorno de red de tecnología operativa (OT, por sus siglas en inglés), en adelante redes OT. Los resultados de un estudio realizado entre 300 empresas industriales indican que en 2018 alrededor del 49% de las empresas encuestadas indicó haber experimentado incidentes cibernéticos en el entorno OT. Aproximadamente un año después, este porcentaje se elevó al 60% (Kaspersky Labs, 2019a). De manera similar, un estudio realizado en 2019 entre 700 empresas encontró que en los últimos dos años el 90% de ellas experimentó al menos un incidente cibernético en el entorno OT, y el 37% de las empresas experimentó cuatro o más incidentes (Ponemon Institute, 2019).

Otra encuesta realizada a alrededor de 350 operarios de tecnologías de la información (TI) y OT de todo el mundo encontró que alrededor del 83% de ellos definió el nivel de riesgo cibernético que representa el entorno OT como medio o superior, y de estos,

alrededor del 13% opinó que era crítico (Filkens, Wylie y Dely, 2019).

De ello se desprende que los riesgos cibernéticos se están convirtiendo en una parte importante de todos los riesgos operativos a los que están expuestas las organizaciones y cuya materialización puede tener diversas consecuencias comerciales, que incluyen, entre otros, daños a la vida humana, daños al medio ambiente, daños reputacionales, pérdida de ingresos y exposición legal. La gran escala de los incidentes cibernéticos obliga a la alta dirección a estudiar el tema en profundidad y a formular preguntas académicas y estratégicas al respecto. La ciberseguridad no es un problema que se limite a las paredes del departamento de TI.

El fuerte aumento en los últimos años en el número de incidentes cibernéticos ocurridos en el entorno operativo (OT) se debió en parte a la disponibilidad de herramientas de ataque y a la capacidad de utilizarlas, así como a la capacidad de aprovechar las redes administrativas (redes de TI) y OT (Kaspersky Labs, 2019b).

En el pasado, cuando se diseñaron y construyeron las redes OT, no siempre se tuvieron en cuenta los temas de ciberseguridad. Esto se debió, entre otras cosas, a que se suponía que estas redes estaban aisladas del mundo exterior. Actualmente, en la era de la industria 4.0 (un concepto de gestión moderno que aboga por la integración de tecnologías y diversas interfaces de comunicación), los sistemas de redes OT están vinculados a los sistemas de información de la red de TI y también agentes de soporte y mantenimiento pueden acceder a ellos remotamente. Estos canales de comunicación exponen los sistemas de control de los procesos operativos a riesgos cibernéticos a los que estuvieron menos expuestos en otros tiempos.

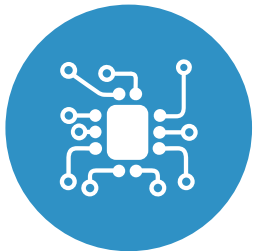
Esta publicación presenta los objetivos clave de defensa que caracterizan a las redes OT y proporciona a la Junta Directiva las herra-

mientas para llevar adelante una discusión que permitirá obtener una imagen inicial de cómo los riesgos cibernéticos pueden verse afectados. Además de una revisión concisa de los principios de la gestión del riesgo cibernético y una explicación focalizada de los objetivos típicos de protección, la publicación incluye preguntas esenciales que la Junta Directiva debe hacerse para evaluar la efectividad del proceso de gestión del riesgo cibernético en el entorno de la red OT.



/01. Impacto de los incidentes cibernéticos en los objetivos operativos y comerciales

La materialización del riesgo cibernético en el entorno OT puede dañar uno o más objetivos operativos y comerciales de la organización, como se observa en los ejemplos que siguen (Stouffer, Zimmerman y Tang, 2017: 8):



01

Seguridad de los empleados: utilización de un canal de acceso y control remoto que interrumpa la configuración en un controlador industrial y provoque la explosión de una caldera de vapor.

02

Protección del medio ambiente: interrupción de la función del sensor que genere un flujo de aguas residuales excesivo o un pro-

ceso químico no controlado que provoque la propagación de gas tóxico.

03

Calidad del producto: un cambio no autorizado en los datos de producción puede acortar la vida útil de un producto alimenticio.

04

Objetivos de producción: el cierre de una línea de producción durante un período de tiempo significativo como resultado de la infiltración de software de secuestro de datos (*ransomware*) puede dañar los objetivos de producción de la organización y las obligaciones con sus clientes.

05

Secretos comerciales: filtración de un documento que describa un proceso de fabricación exclusivo.

En general, a diferencia de un entorno TI, el enfoque en el entorno OT es mantener la integridad del proceso operativo y proteger la vida humana. A la luz de esto, existe la necesidad de un proceso de gestión de riesgos y la identificación de controles de seguridad apropiados. Por lo tanto, se presenta un desafío para realizar cambios, incluida la imple-

mentación de nuevos controles cibernéticos o la aplicación de aquellos existentes.

Con el fin de motivar el proceso de manera paulatina, con foco en los principales riesgos, deben considerarse, en primer lugar, los siguientes objetivos de defensa propios del entorno OT:

- Administración de ciberseguridad.
- Gestión de riesgos cibernéticos en un entorno OT.
- Identificación de riesgos cibernéticos típicos de la red OT
- Seguimiento y respuesta a incidentes cibernéticos.

En segundo lugar, es conveniente mantener el foco en áreas de actividad y objetivos de defensa adicionales, en función de su importancia para la organización. Para evitar dudas, se debe enfatizar en que para obtener una imagen completa de la resiliencia cibernética del entorno OT es apropiado realizar una encuesta integral de riesgos. Para obtener más detalles, consúltese la plantilla de encuesta de riesgos en entornos OT.²

2. La *Plantilla de trabajo para la realización de una encuesta de riesgo cibernético en sistemas de control industrial (ICS)* se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.

/02.

Administración de ciberseguridad

La gestión del riesgo cibernético en un entorno OT es un desafío especial, ya que un entorno OT típico combina tecnologías actualizadas del campo de la TI con tecnologías más antiguas, utilizadas en los sistemas de control industrial. Debido a esto, la responsabilidad de los sistemas operativos en las redes OT se divide entre los ingenieros de control, el gerente de ciberseguridad, personal operativo e informático. Por lo tanto, desde una perspectiva organizacional global, el conocimiento requerido para identificar y administrar los riesgos cibernéticos reside en varios empleados.

A modo de facilitar dicha gestión, muchas organizaciones se caracterizan por dividir los conocimientos entre sus funcionarios como se describe a continuación:

01

Ingenieros de control y personal de operaciones (generalmente en el entorno OT): se centran principalmente en garantizar la disponibilidad e integridad de los procesos operativos. Están profundamente familiarizados con la red OT y sus componentes tecnológicos. Son conscientes de la sensibilidad de estos componentes a los cambios y otras influencias externas, la cual puede conducir a fallas y deterioro de la disponibilidad del proceso operativo. En muchos casos, carecen del conocimiento pleno necesario para identificar los riesgos cibernéticos y evaluar la **probabilidad** de su materialización, lo que también puede conducir a un deterioro en la disponibilidad de los procesos operativos.

02

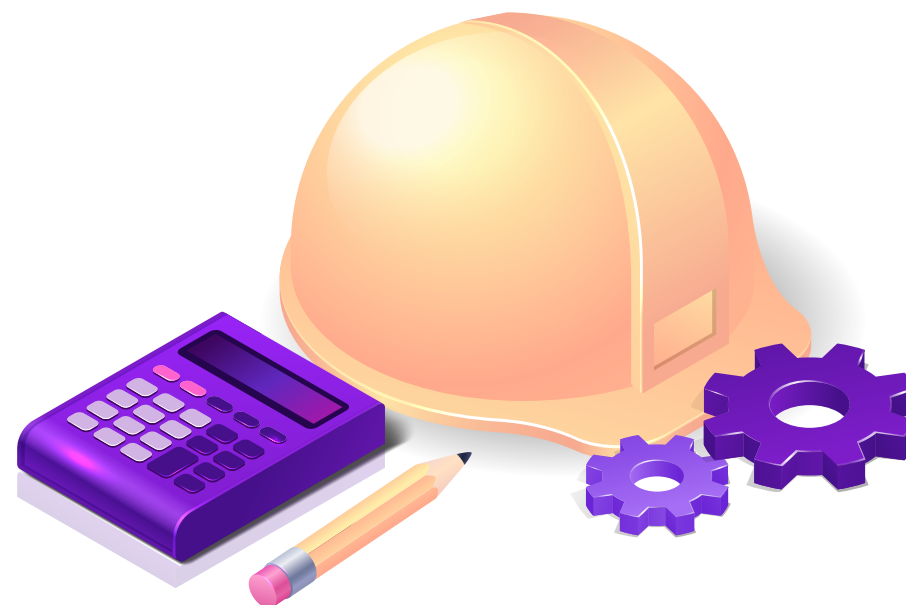
Gerente de ciberseguridad y personal de TI, que se enfocan principalmente en la gestión del riesgo cibernético en el entorno TI: están familiarizados con el mapa de amenazas cibernéticas y son competentes para controlar, operar y mantener sistemas de protección cibernética en el entorno de la red administrativa. En muchos casos, carecen del conocimiento necesario para comprender el entorno de la red OT y las sensibilidades que lo caracterizan.

A causa de esta separación, no existe claridad en muchas organizaciones con respecto a la división de autoridad y responsabilidad del

personal. Esta división puede afectar la eficacia del proceso de gestión de riesgos cibernéticos del entorno OT, lo que puede provocar daños potenciales a los objetivos operativos y comerciales de la organización.

Debido a todo lo mencionado anteriormente, es conveniente que la dirección de la organización designe un actor a quien se le confíe la ciberseguridad en el entorno de la red OT, defina sus áreas de autoridad y responsabilidad y se asegure de que cuenta con todas las habilidades necesarias para gestionar los riesgos cibernéticos.

También es recomendable que este actor tenga conocimiento en las siguientes áreas (Weiss, 2017):



01

Comprensión del proceso operativo.

02

Comprensión de los sistemas de control y sus características distintivas.

03

Familiaridad con las metodologías de gestión de riesgos en general y la gestión de riesgos cibernéticos en el entorno OT en particular.

04

Comprensión del mapa de amenazas y los métodos de ataque más comunes.

05

Familiaridad con los estándares profesionales y entendimiento de cómo asimilarlos entre personas, procesos y componentes tecnológicos.

06

Capacidad para resolver de manera práctica las diferencias entre el mundo de los sistemas de información y el mundo de las operaciones.

El puesto puede ser cubierto tanto por un empleado que haya recibido capacitación en el campo de la ciberseguridad como por un profesional de TI que haya recibido capacitación en el entorno de OT.

Como parte de sus actividades de ciberseguridad en el entorno OT, este actor debe ayudar a la Gerencia a establecer políticas y formular procedimientos de seguridad (ISACA, 2015: 6).

Preguntas para la Junta Directiva

Estas preguntas se centran en las políticas de gestión de riesgos cibernéticos:

01

¿Cuál es la situación general de ciberseguridad en la organización y entorno OT?

02

¿Se designó dentro la organización una persona responsable de la ciberseguridad del entorno OT?

03

¿A quién le fue asignada la ciberseguridad de la organización en el entorno OT: a un actor del ámbito operacional, del campo empresarial o de ciberseguridad?

04

¿Se han definido las áreas de autoridad y responsabilidad de la persona a cargo del entorno de la ciberseguridad, de manera que

se asegure la implementación, aplicación y monitoreo efectivos de los controles de ciberseguridad en el entorno OT?

05

¿Se ha dotado al responsable de la ciberseguridad con las habilidades necesarias para gestionar e implementar la ciberseguridad en el entorno OT?

06

¿Se han asignado al responsable de la ciberseguridad los recursos y herramientas necesarios para cumplir su función?

07

¿Se han formulado políticas y procedimientos para la ciberseguridad en el entorno OT?



/03.

Gestión de riesgos cibernéticos en el entorno OT

Principios rectores para la gestión de riesgos cibernéticos

Para monitorear de manera efectiva el proceso de gestión de riesgos cibernéticos, la Asociación Nacional de Directores Corporativos (NACD, por sus siglas en inglés) de Estados Unidos ha definido cinco principios que los miembros de la Junta Directiva deben aplicar (NACD, 2020: 6):

01

Abordar el tema de la ciberseguridad en el contexto de la gestión general de riesgos organizacionales y no solo como un tema relevante en el ámbito de los sistemas de información. En este contexto, vale la pena

asegurarse de que la organización también analice el impacto de la materialización de los riesgos cibernéticos en el logro de los objetivos operativos y comerciales.

02

Comprender las consecuencias legales de la materialización de los riesgos cibernéticos con relación a las circunstancias específicas de la organización.

03

Adquirir los conocimientos necesarios para llevar a cabo discusiones efectivas sobre la gestión de los riesgos cibernéticos, asignando tiempo adecuado para este propósito.

04

Presentar sus expectativas de que la administración implemente una política de gestión de riesgos transversal a la organización, que tenga asignados los recursos y la dotación de personal adecuados.

05

Discutir junto con la Gerencia sobre el manejo de los principales riesgos y la aprobación del mapa de riesgos.

Marcos de referencia destacados para la gestión de riesgos cibernéticos en el entorno OT

Existen varias metodologías para gestionar los riesgos cibernéticos en el entorno OT, entre ellas, las siguientes (ISO, 2018; NIST, 2018):

01

El Marco de Ciberseguridad para el entorno de fabricación (Cybersecurity Framework Manufacturing Profile) del Instituto Nacio-

nal de Estándares y Tecnología (NIST, por sus siglas en inglés) de Estados Unidos (Stouffer et al., 2017).

02

El estándar ISA/IEC 62443.³

03

Reducción de los riesgos cibernéticos para los sistemas de control industrial (ICS), disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.

04

Metodología de Ciberdefensa para Organizaciones de la Dirección Nacional de Ciberseguridad (2017).

De acuerdo a las metodologías más destacadas, los pasos clave en el proceso de gestión de riesgos se presentan en el gráfico 1.

3. Más información acerca de este estándar disponible en: <https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/>.

Gráfico 1. Pasos clave en el proceso de gestión de riesgos

Formulación de indicadores clave de riesgo

Los índices de riesgo son datos medibles que se pueden comparar con umbrales predefinidos. Su propósito es identificar cambios en las tendencias. Esto permite a la organización responder con eficacia antes de que esas tendencias se materialicen como resultado de un mal funcionamiento o un incidente cibernético.

Los indicadores clave de riesgo (KRI, por sus siglas en inglés) ayudan en la gestión continua del riesgo, al identificar un cambio en las tendencias a lo largo del tiempo. Por lo tanto, constituyen un nivel adicional a las encuestas de riesgo que se realizan de forma periódica. A continuación, se listan algunos ejemplos posibles de KRI en el entorno OT:

01

Varios intentos de intrusión detenidos por el cortafuego (*firewall*) de la empresa durante el mes.

02

Cálculo de la proporción relativa de tiempo de inactividad en línea de producción.

03

Varios brotes virales y otros daños durante el trimestre.



Preguntas para la Junta Directiva

Estas preguntas se focalizan en la gestión de riesgos cibernéticos en un entorno OT:

01

¿Se ha adoptado un marco o metodología de gestión?

02

¿Existen riesgos cibernéticos en el entorno OT?

03

¿Cómo se integra la gestión de riesgos cibernéticos en un entorno OT a la gestión de riesgo general de la organización?

04

¿Cómo se decidieron los objetivos de protección y áreas de actividad organizativa que se incluirían en las actividades de gestión de riesgos cibernéticos en el entorno OT?

05

¿Se han identificado y mapeado los riesgos cuya materialización tienen consecuencias legales?

06

¿La organización realiza pruebas de resiliencia proactivas?

07

¿Los recursos asignados para reducir los riesgos cibernéticos en el entorno OT satisfacen las necesidades de la organización?

08

¿Cuál es el estado del plan de trabajo en relación con los riesgos identificados? ¿Se tratan de acuerdo a los cronogramas establecidos?

09

¿Se han definido KRI que permitan identificar cambios en las tendencias y tomar medidas efectivas para reducir la probabilidad de que ocurra un incidente que afecte a la ciberseguridad?

/04. Identificación de riesgos cibernéticos típicos de la red OT

En la actualidad, en muchos casos, las redes OT están conectadas a redes adicionales: la red de TI y la de Internet. Este enlace puede permitir a un atacante que se introduzca en la red corporativa/administrativa extender su ataque a otras redes.

Esto contrasta con el pasado, ya que tradicionalmente las redes OT y TI se ejecutaban por separado y sin interfaces, por lo que la red OT estaba completamente aislada de la red administrativa de la organización y la red pública de Internet.

En los últimos años, tras la cuarta revolución industrial, la industria 4.0, se ha producido un cambio. En la actualidad, las modernas tecnologías de información y comunicación (TIC) se están fusionando con las tecnologías de fabricación para dar lugar a una nueva fase de creación de valor.

La disponibilidad de información en tiempo real a través de la comunicación entre todas

las partes involucradas en el proceso conduce a redes dinámicas, que se optimizan en tiempo real, se organizan de forma independiente, son transorganizacionales y agregan valor (VDMA, 2016: 3).

Para hacer realidad la visión de una organización conectada, muchas organizaciones optan por establecer interfaces entre Internet, la red OT y la red TI. Además, tienden a conectar activos finales a través de la comunicación inalámbrica: el Internet Industrial de las Cosas (IIoT, por sus siglas en inglés) conduce al establecimiento de muchas interfaces adicionales entre la red OT y otras redes de la organización y también públicas.

Junto con los beneficios operativos y comerciales, estas interfaces constituyen un posible vector de ataque para los elementos hostiles y, por lo tanto, es de gran importancia mapear y asegurar estas interfaces.

Acceso remoto

La necesidad operativa de mantenimiento y soporte de los sistemas por parte de empleados, proveedores y fabricantes ajenos a la organización, implica, entre otras cosas, la concesión de permisos de acceso remoto. En ocasiones, la posibilidad de acceso remoto a la red OT con el fin de brindar servicio y soporte está sujeta a un acuerdo contractual, según lo requieran los proveedores de equipos.

Para garantizar que el acceso remoto esté protegido y se permita únicamente a partes autorizadas, se debe cuidar que todos los accesos se realicen a través de un componente de red dedicado que refuerce la identificación y encriptación del medio de comunicación, al tiempo que evite el acceso directo a controladores y otros componentes en la red OT. Este proceso se llevará a cabo de forma proactiva y bajo total supervisión.



Utilización de un medio de comunicación inseguro

Para la comunicación entre la sala de control y los componentes de la red OT dispersos en diferentes edificios o sitios remotos, se utilizan a menudo tecnologías como radio (VHF, UHF), comunicación celular, satélite y wifi. En algunas de ellas existen debilidades y brechas conocidas.

Mapeo de sistemas y componentes en redes OT

Mapear sistemas y componentes en redes OT es un desafío, dado que en muchos casos se trata de redes distribuidas que se establecieron hace décadas y que incluyen una variedad de componentes de diferentes fabricantes. La falta de ese mapeo complica el proceso de identificación de activos vitales mediante una encuesta de riesgo cibernético y afecta la capacidad del monitoreo continuo para identificar incidentes excepcionales en la red OT, que pueden resultar de un mal funcionamiento operativo o de un ataque cibernético.

/05. Seguimiento y respuesta a incidentes cibernéticos

Cambio de percepción en ciberseguridad

En épocas pasadas, el concepto de acción en seguridad de la información se ha centrado en **prevenir la intrusión** en los activos informáticos de la organización. Fruto de esta percepción, muchas organizaciones han orientado sus recursos principalmente hacia actividades de **identificación**, como realizar encuestas de riesgo, implementar herramientas y acciones de **protección**, controlar el acceso a la información, instalar cortafuegos, antivirus y concientizar a los empleados.

Actualmente, debido a que la intensidad y sofisticación de los ataques han aumentado de manera significativa, ha surgido un nuevo enfoque

de ciberseguridad, que asume que un ataque determinado eventualmente ocurrirá en la organización. Por lo tanto, el énfasis en el tratamiento de los riesgos cibernéticos combina capacidades de **prevención** con un conjunto de capacidades de detección, respuesta y defensa proactivas.

A la luz de lo anterior, junto con las actividades de identificación y protección que deben continuar, se requiere más que nunca que las organizaciones fortalezcan las capacidades de **detección**, como la implementación de sistemas de monitoreo, y de **respuesta**, incluida la formulación de procedimientos y el establecimiento y capacitación práctica de un equipo de respuesta frente a incidentes. Esto es para identificar los ataques lo más cerca posible de su inicio y responder a ellos de manera efectiva para minimizar el daño del ataque tanto como sea posible.

Seguimiento e identificación de fallos e incidentes cibernéticos

Según el NIST, el monitoreo se define como: “Verificación, supervisión, observación crítica o determinación continua del estado para identificar cambios respecto al nivel de desempeño requerido o esperado” (NIST, s.f.). Además, el monitoreo de incidentes cibernéticos debe identificar anomalías que puedan indicar la materialización de un incidente causado por un factor hostil y no como resultado de un mal funcionamiento.

La práctica común en los entornos de fabricación es monitorear el funcionamiento anormal o incorrecto de las operaciones de los componentes para garantizar la integridad del proceso operativo. El aumento en el volumen de amenazas cibernéticas requiere expandir la capacidad de monitoreo, de manera que también proporcione una solución para identificar incidentes cibernéticos.

Respuesta a incidentes cibernéticos en el entorno de la red OT

Muchas organizaciones han formulado procedimientos de respuesta y han establecido equipos dedicados para hacer frente a incidentes extremos resultantes de fallas operativas o de seguridad en el entorno de la red OT. Estos procedimientos se enfocan en reducir el daño a la vida humana y/o el daño ambiental, así como en restaurar el proceso operativo para que funcione correctamente en el menor tiempo posible.

En la mayoría de los casos, los procedimientos de respuesta formulados no abordan escenarios cibernéticos y, por lo tanto, los equipos de respuesta no incluyen personal de ciberseguridad ni brindan una solución a las características únicas de los incidentes cibernéticos. En

el caso de un mal funcionamiento operativo, un incidente cibernético en el entorno de la red OT puede continuar y provocar más daños debido a la incapacidad de identificar la causa raíz para contener el ataque.

Una respuesta eficaz a un incidente cibernético aborda, entre otros, los siguientes aspectos (NIST, 2012: 21).

01

Integración de un equipo cibernético en un incidente desde la primera etapa de su reporte.

02

Análisis de eventos y priorización del tratamiento en casos de incidentes múltiples.

03

Detención de la propagación del ataque, identificación de su origen y recopilación de pruebas relevantes.

04

Aprendizaje de lecciones y retención de evidencia recopilada.

Preguntas para la Junta Directiva

Estas preguntas se centran en el seguimiento y respuesta a incidentes cibernéticos:

01

¿Cómo y con qué herramientas la organización monitorea los incidentes cibernéticos en el entorno OT?

02

¿Cómo está preparada la organización para hacer frente y responder a los incidentes cibernéticos en el entorno OT? ¿Se han definido criterios y un mecanismo de reporte inmediato para la Gerencia y el Consejo de Administración ante un incidente extremo?

03

¿Se ha formulado un proceso para investigar, extraer lecciones y aplicarlas tras la ocurrencia de incidentes cibernéticos en el entorno OT?



Referencias

- Dirección Nacional de Ciberseguridad. 2017. Metodología de Ciberdefensa para Organizaciones. Disponible en: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf (en inglés).
- CISCO. 2018., IT/OT Convergence. Moving Digital Manufacturing Forward. Disponible en: https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf.
- Filkins, B., D. Wylie y J. Dely. 2019. SANS 2019 State of OT/ICS Cybersecurity Survey. Disponible en: <https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/>.
- ISACA (Asociación de Auditoría y Control de Sistemas de Información). 2014. Cybersecurity: What the Board of Directors Needs to Ask. Disponible en: <https://store.isaca.org/s/store#/store/browse/detail/a254w000004KoGFEAO>.
- ———. 2015. The Cyberresilient Enterprise: What the Board of Directors Needs to Ask. Rolling Meadows, IL: ISACA. Disponible en: https://assets.ctfassets.net/82ripq7fjls2/5VE-6C6a3ABbbp3e8cfZVx3/de4d299f3c46f82a248925796b16af8a/ISACA_The-Cyberresilient-Enterprise_eBook-2015.pdf.
- ISO (Organización Internacional de Normalización). 2018. ISO 31000:2018 - Risk Management-Guidelines. Disponible en: <https://www.iso.org/iso-31000-risk-management.html>.
- Kaspersky Labs. 2019a. The State of Industrial Cybersecurity. Disponible en: https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf.
- ———. 2019b. Threat Landscape for Industrial Automation Systems. Disponible en: https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf.
- NACD (Asociación Nacional de Directores Corporativos). 2020. NACD Director's Handbook on Cyber-Risk Oversight. Disponible en: <https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298>.
- NIST (Instituto Nacional de Estándares y Tecnología). s.f. Glossary. Disponible en: <https://csrc.nist.gov/glossary/term/monitoring>.
- ———. 2012. Computer Security Incident Handling Guide. Special Publication 800-61, Revision 2. Gaithersburg, MD: NIST. Disponible en: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
- ———. 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Special Publication 800-37, Revision 2. Gaithersburg, MD: NIST. Disponible en: <https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-fpd.pdf>.
- Ponemon Institute. 2019. Cybersecurity in Operational Technology: 7 Insights You Need to Know. Columbia, MD: Tenable. Disponible en: https://static.tenable.com/marketing/research-reports/PonemonReport-Cybersecurity_in_Operational_Technology.pdf.
- Stouffer, K. A., T. A. Zimmerman, C. Y. Tang et al. 2017. Cybersecurity Framework Manufacturing Profile, NIST Interagency/Internal Report (NISTIR) 8183. Gaithersburg, MD: NIST. Disponible en: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf>.
- VDMA (Mechanical Engineering Industry Association). 2016. Guideline Industrie 4.0: Guiding Principles for the Implementation of Industrie 4.0 in Small and Medium Sized Businesses. Frankfurt, Alemania: VDMA, Technical University Darmstadt y Karlsruhe Institute of Technology. Disponible en: https://www.vdma.org/c/document_library/get_file?uuid=71502bd7-5549-7033-5237-549253f1ef0f&groupId=34570.
- Weiss, J. 2017. What Executives Need to Know About Industrial Control Systems Cybersecurity. Research Triangle Park, NC: International Society of Automation (ISA). Disponible en: https://www.isa.org/getmedia/4b3f6d2e-8d9e-45ed-a563-6ddfc42d0ae3/ISA_WP_Executives-Cybersecurity.pdf.



En los últimos años se ha incrementado el número de incidentes cibernéticos denunciados en el ámbito de las redes operativas, lo que ha intensificado la conciencia sobre el tema y su importancia. Los riesgos cibernéticos ocupan un lugar importante en la gestión de riesgos organizacionales a la luz de sus posibles consecuencias: daño a la vida humana, daño ambiental, daño reputacional, pérdida de ingresos y exposición legal. Esta guía fue elaborada especialmente para uso de una Junta Directiva, como parte de un proyecto integral de la Dirección Nacional de Ciberseguridad en el campo de los sistemas de control industrial (ICS, por sus siglas en inglés), dentro del cual se elaboró un documento de expansión profesional⁴ y una plantilla de trabajo para la realización de una encuesta de riesgo cibernético en el sector industrial. Esta publicación tiene como objetivo proporcionar la infraestructura para un diálogo continuo entre la Junta Directiva y la Gerencia sobre cómo gestionar los riesgos cibernéticos en el entorno de la red de tecnología operativa (OT, por sus siglas en inglés).

4. El documento *Reducción de los riesgos cibernéticos para los sistemas de control industrial (ICS)* se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.

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

A.01 Metodología de Ciberdefensa para Organizaciones Versión 1.0

A.02 Metodología de Ciberdefensa para Organizaciones Versión 2.0

A.03 Uso de servicios en la nube: Adenda a la Metodología de Ciberdefensa para Organizaciones

A.04 Recomendaciones de defensa: La amenaza interna

A.05 Preparación organizacional para una crisis cibernética

A.06 Cadena de suministro

A.07 Preguntas de orientación para formuladores de políticas cibernéticas

A.08 Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas

A.09 Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones

➤ **A.10** Gestión de riesgos cibernéticos en entornos de tecnologías operativas (OT)

A.11 Plantilla de evaluación de riesgo en el sector minorista

A.12 Práctica cibernética: creación de planes de concientización para organizaciones

Volumen B: Un enfoque técnico

Volumen C: Desarrollo seguro de *software*

