**Universidad de Buenos Aires**

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería




**Maestría en Seguridad Informática**

Trabajo Final

**Tema**

**Ciberseguridad en la convergencia entre redes IT y OT.**

**Título**

# Transformación digital: Convergencia segura entre redes IT y OT.

**Autor: Esp. José Luis Mora Isaza**

**Directora TFM: Patricia Prandini**

**Cohorte 2023**

**2024**

**DECLARACIÓN JURADA**

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

**FIRMADO**

**José Luis Mora Isaza**

**DNI 95.970.106**

**Resumen.**

El nuevo paradigma de transformación digital en organizaciones industriales trajo consigo nuevas perspectivas para mejorar la sostenibilidad operativa. Sin embargo, profundiza la dependencia de estas empresas de los datos proporcionados por sus propios dispositivos para ayudar a tomar decisiones basadas en condiciones y en tiempo real mucho más cercanas a la realidad. Esto obliga a la convergencia entre los diversos equipamientos presentes en estas entidades.

Es así como la integración entre tecnologías informáticas y operativas se convierte en una necesidad que se debe alinear a las mejores prácticas conocidas en la industria y al negocio. Sin embargo, esta evolución plantea nuevos desafíos como el de la ciberseguridad y el del control de procesos operacionales, los cuales son fundamentales para gestionar la información, especialmente en infraestructuras críticas, esenciales para el desarrollo de una región.

En este trabajo final de maestría se presentan y analizan estos desafíos y se refleja la importancia de aprovechar la tecnología y los avances industriales para mejorar los procesos productivos manteniendo la continuidad operativa y desarrolla, uno de los principales desafíos en la convergencia IT y OT, el de la seguridad informática, basándose en las mejores prácticas conocidas en el mercado recomendando conocerlas, entender los avances para saber cómo aborda este nuevo escenario y mitigar todo riesgo asociado en las mismas.

***Palabras claves: Ciberseguridad Industrial, Convergencia IT y OT, Transformación digital, Estándares de Ciberseguridad Industrial.***

## Tabla de contenido

**Tabla de figuras.**

A **Dios** por nunca soltarme la mano.

A mi **familia y amigos**, gracias por el soporte.

**A Diego Romero, Karen Vega y Patricia Prandini,**

Gracias por su aporte a este documento y

a mi crecimiento personal y profesional.

## Introducción.

En la actualidad, numerosas compañías están implementando la digitalización de sus operaciones y sistemas en general. Este cambio se debe en parte a la búsqueda de innovación y al impacto de la cuarta revolución industrial o industria 4.0., la cual se centra en el uso de los datos generados por la maquinaria de la empresa, lo que permite obtener información detallada para análisis mucho más precisos. Una vez interpretados, estos datos proporcionan información veraz que facilita la toma de decisiones en tiempo real de manera oportuna y precisa.

A su vez, las Tecnologías operativas (en adelante OT) han experimentado considerables avances gracias a soluciones como el Internet Industrial de las Cosas (IIoT), la automatización, los sistemas de control de procesos (en adelante SCADA) y de los PLC, entre otros, logrando un mejoramiento en la eficiencia y la conectividad en las operaciones industriales. Por otro lado, se encuentran las Tecnologías de la Información (en adelante IT) que proporcionan a una organización la automatización de procesos, almacenamiento y gestión de datos, análisis y reportes y mejoramiento de la productividad, dando lugar al desarrollo de soluciones en forma de sistemas de información logren operar en infraestructuras con altos estándares de servicio, satisfaciendo las necesidades de transacciones lógicas.

En consecuencia, se originó la convergencia de las redes de IT y OT que, impulsada por la necesidad de integrar sistemas de control industrial con plataformas de TI para lograr una mayor eficiencia y visibilidad en las operaciones, han planteado desafíos en términos de ciberseguridad, ya que la interconexión de sistemas previamente aislados aumenta su superficie de ataque. Además, de tener en cuenta que la integración de tecnologías con equipamientos heredados con sistemas modernos requiere una gestión cuidadosa para garantizar la compatibilidad y el rendimiento óptimo de los mismos.

Es así como entran a jugar un papel importante los datos y la manera en que deben ser almacenados, y esto debería hacerse de acuerdo con las recomendaciones y controles establecidos por las mejores prácticas reconocidas por el mercado como las normas IEC-62443, las del NIST, o normas de nicho en entornos industriales, pero también contempla el cumplimiento del Reglamento General de Protección de Datos Personales (GDPR), y/o normativas puramente del área informática como la familia

de las ISO 27000 sobre el Gobierno de la seguridad de la información, entre otras. Por lo anterior, es crucial aprovechar estas recomendaciones para mejorar la calidad en los sistemas productivos, así como también para garantizar la seguridad de la información y la continuidad operativa, vital en la industria.

Este documento aborda la penetración de la transformación digital en entornos industriales, destacando los riesgos cibernéticos asociados a las redes OT y analizando su correlación con las redes de IT. Asimismo, presenta las mejores prácticas del mercado para integrarlas de manera segura, examina cada eslabón en la cadena de suministro y ofrece recomendaciones priorizar la ciberseguridad en esta convergencia.

## CAPITULO 1. Transformación digital en entornos Industriales.

Como el proceso de aprovechar la tecnología para mejorar los modelos de negocio, los procedimientos operativos y la experiencia del cliente en una organización es definida la transformación digital[1]. En entornos industriales, esta metamorfosis técnica y de procesos se refiere a la integración de tecnologías digitales en todos los aspectos de una operación industrial, lo cual implica la adopción de soluciones como el Internet de las cosas (IoT), la inteligencia artificial (AI), el análisis y procesamientos masivos de grandes flujos de datos, la nube, la ciberseguridad y la automatización de procesos, herramientas de eficiencia energética, productos y servicios amigables con el ambiente y también con la premisa de la reducción de costos y de la innovación.

En la práctica esto implica convertir a formato digital activos físicos y sus procesos, lo que permite la recopilación masiva de datos en tiempo real. Estos datos son luego analizados para obtener información valiosa que ayude a mejorar la toma de decisiones, predecir fallas en equipos, optimizar todo el proceso en la cadena de producción y permitir productos y servicios de mayor calidad. Además, proporciona la conexión y colaboración entre diferentes sistemas y actores dentro de una empresa, lo que conduce a una mayor agilidad, flexibilidad y capacidad de respuesta a las demandas del mercado.

En contraste, cuando una empresa industrial no se transforma digitalmente, puede enfrentar la pérdida de su competitividad, ya que puede quedar rezagada en términos de eficiencia operativa y de capacidad para satisfacer las demandas del mercado. La ausencia de automatización y digitalización puede resultar en procesos manuales, lentos y propensos a errores, lo que afecta directamente a la calidad. Al mismo tiempo, la obsolescencia de equipos y sistemas, junto con la falta de optimización de procesos, puede resultar en costos operativos más altos y en una menor rentabilidad y la falta de análisis de datos en tiempo real puede llevar a una toma de decisiones deficientes y a generar dificultades para identificar oportunidades de mejora.

[1] ¿Qué es la Transformación Digital en las Empresas? Tomado de: https://www.administracion.usmp.edu.pe/revista-digital/numero-1/que-es-la-transformacion-digital-en-las-empresas/ el 05/01/2024 a las 05:26


Figura 1. Modelo de Transformación digital de la industria 4.0

Por otro lado, se hace necesario hablar de cuarta revolución industrial[2] o industria 4.0. Este concepto hace referencia a la integración de tecnologías digitales avanzadas en los procesos de fabricación y producción, basándose en la interconexión de sistemas, la computación en la nube, el Internet de las Cosas (IoT), la Inteligencia Artificial (IA), la robótica, la realidad aumentada (AR) y otras tecnologías emergentes. A través de la recopilación y análisis de datos en tiempo real, las empresas pueden tomar decisiones más informadas, optimizar los procesos de producción, predecir fallas en la maquinaria y personalizar la producción según las necesidades del cliente.

[2] ¿Qué es la Cuarta Revolución Industrial? Tomado de: https://www.salesforce.com/mx/blog/cuarta-revolucion-industrial/?gclid=CjwKCAiA44OtBhAOEiwAj4gpOS_qPstvu_hR6xMlf-PzI7AFmEyCivdsdzGfR7RC9-M7v-lTuryMWRoCZFcQAvD_BwE&d=7013y000002EkCcAAK&nc=7013y000002EkKgAAK&utm_source=google&utm_medium=paid_search&utm_campaign=latam_growth_alllobaw&utm_content=pg-es-mash_7013y000002EkCcAAK&utm_term=CuartaRevolucionIndustrial&ef_id=CjwKCAiA44OtBhAOEiwAj4gpOS_qPstvu_hR6xMlf-PzI7AFmEyCivdsdzGfR7RC9-M7v-lTuryMWRoCZFcQAvD_BwE:G:s&gclsrc=aw.ds&&pcrid=674088412443&pdv=c&gad_source=1 el 20/12/2023 a las 18:21

## 1.1 Desafíos en la implementación de nuevas tecnologías en entornos industriales.

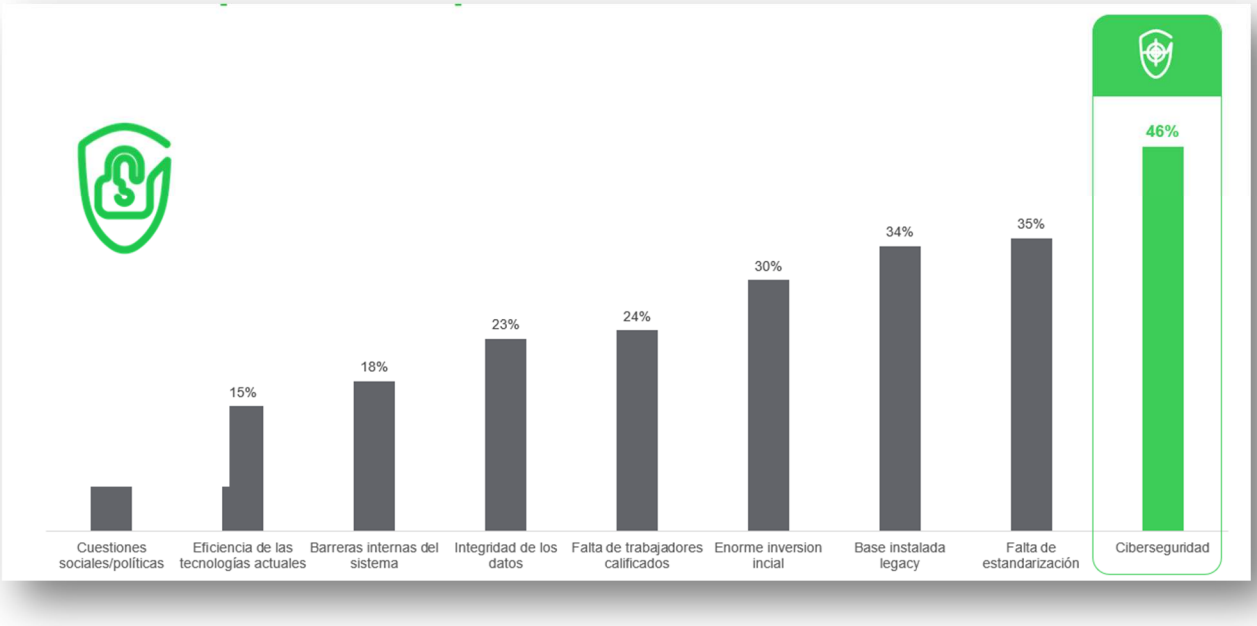


Figura 2. Retos de la adopción de nuevas tecnologías industriales.[3]

La integración de las nuevas tecnologías con los sistemas existentes trae consigo grandes retos, ya que las empresas industriales suelen tener sistemas legados y una infraestructura compleja, lo que dificulta la compatibilidad y la combinación adecuada de las nuevas tecnologías, requiriendo un enfoque cuidadoso para minimizar los tiempos de inactividad.

Y, es por lo cual se considera a la ciberseguridad[4] como un desafío crítico en la implementación de nuevas tecnologías. La resistencia al cambio[5] por parte de los empleados es otro de los retos más marcados en la era de la transformación digital, sumado a la adopción de nuevas tecnologías implica cambios en los procesos de trabajo, generando resistencia y temor a lo desconocido. Por esto es necesario implementar estrategias de capacitación y comunicación efectivas para asegurar una fácil transición a nuevas tecnologías.

[3]A report by Morgan Stanley cites Cybersecurity as the single biggest challenge to IIoT adoption.
[4]La ciberseguridad como uno de los desafíos más importantes en la transformación digital. Tomado de: https://makaia.org/ciberseguridad-en-la-transformacion-digital/ el 12/12/2023 a las 14:23
[5]Principales desafíos de la transformación digital y el papel crucial de la gestión del cambio para superarlos. Tomado de: https://www.linkedin.com/pulse/principales-desaf%C3%ADos-de-la-transformaci%C3%B3n-digital-y-el-papel-crucial/?originalSubdomain=es el 06/01/2024 a las 12:20

Al mismo tiempo, la inversión financiera representa otro desafío, ya que el proceso de transformación digital implica una asignación significativa de fondos en hardware, software, creación de nuevos equipos de trabajo y capacitación. Las empresas deben evaluar cuidadosamente el retorno de la inversión a largo plazo y diseñar un plan financiero adecuado. Por último, superar estos desafíos requiere un enfoque estratégico, una comunicación efectiva, una planificación cuidadosa y una colaboración cercana entre los equipos de IT, OT, los proveedores y los empleados. Sobre el desafío de la ciberseguridad, qué este documento profundizará más adelante.

## 1.2. Convergencia en redes IT y OT: ¿Qué se debe saber para empezar?

Para iniciar a hablar sobre la convergencia segura[6] de las redes de IT y OT en una organización, es crucial destacar la creciente importancia que está adquiriendo en varios sectores, como la fabricación de productos, la energía, la salud, la agricultura, la manufactura y la seguridad pública.

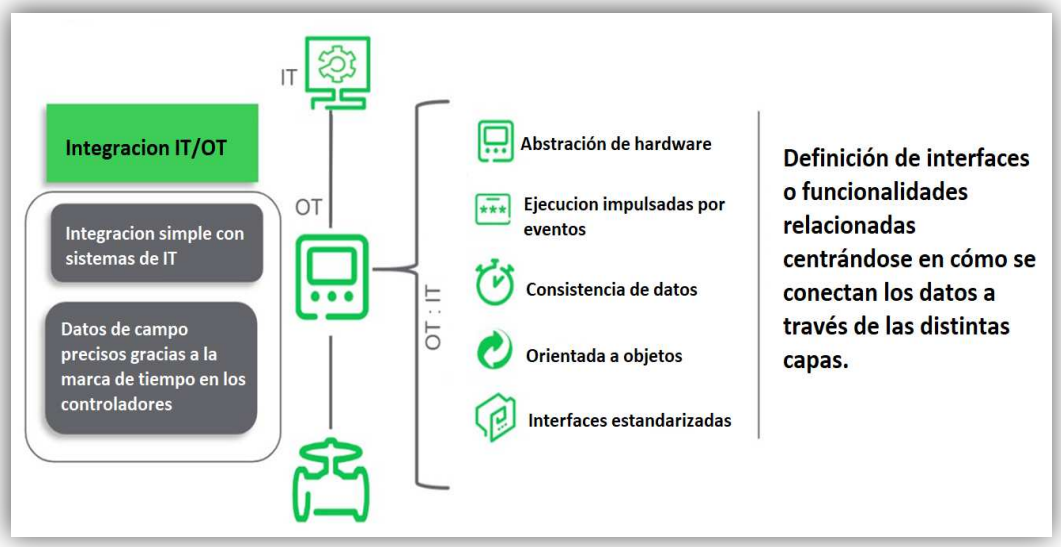


Figura 3. Integración de sistemas de IT y de OT.

[6] ¿Qué es la convergencia IT/OT? Tomado de: https://www.linkedin.com/pulse/qu%C3%A9-es-la-convergencia-itot-daniel-garrido/?originalSubdomain=es el 13/12/2023 a las 14:32

Es así como se habilita a las organizaciones a recopilar y analizar datos en tiempo real, mejorando la toma de decisiones y la capacidad de respuesta ante cambios empresariales. En la industria manufacturera, esta integración puede identificar problemas en la cadena de suministro y optimizar líneas de producción, pero también plantea desafíos de seguridad, ya que amplía la superficie de ataque, exigiendo sólidas medidas de protección cibernética.

Además, esta convergencia de redes IT y de OT debe tender a eliminar los cuellos de botella de los distintos sectores, que es básicamente lo que buscan muchos supervisores y operarios de los diversos procesos productivos, es que la abstracción del hardware y su sincronía con sistemas de información ofrezcan un análisis pormenorizado con datos proporcionados por sus propios dispositivos y que facilite la operación en el día a día, que dé lugar a la inspección regulada y separada del sitio físico y que se aproveche la ventaja del desarrollo tecnológico y a su vez, este se vea impactado en la calidad del servicio o del producto final ofertado.

### 1.3. Hechos históricos en la evolución de redes IT y OT.

La evolución de los sistemas IT y OT ha sido un proceso extenso y complejo, marcado por una serie de hitos significativos. Durante la revolución industrial en los siglos XVIII y XIX, surgieron los primeros sistemas de control y supervisión en tiempo real para manejar la producción y la distribución. A medida que avanzaba el siglo XX, se crearon sistemas de control automático, como los utilizados en la industria química y automotriz.

Con la introducción de los sistemas electrónicos[7] en los años 60 y 70, se logró una mayor precisión y control en los procesos industriales. En los años 80, se produjo el surgimiento de los sistemas de información y gestión empresarial[8], lo que permitió una mayor coordinación y eficiencia en las operaciones comerciales. Posteriormente, a finales de los años 90 y principios de los 2000, se desarrollaron sistemas

[7] Introducción a los sistemas digitales. Tomado de: https://www.mheducation.es/bcv/guide/capitulo/844817156X.pdf el 1/11/2024 a las 13:43

[8] Surgimiento de los sistemas de información y gestión empresarial. Tomado de: https://dyncsolutions.com/general/evolucion-de-los-sistemas-de-gestion-empresarial-erp/#:~:text=Origen%20de%20los%20sistemas%20de,materiales%20que%20demandaba%20el%20ej%C3%A9rcito. El 01/11/2024 a las 14:10

informáticos específicos para la industria, como la automatización industrial y los sistemas SCADA[9], que facilitaron una mayor integración y coordinación entre los sistemas de información y los sistemas de control operativo.

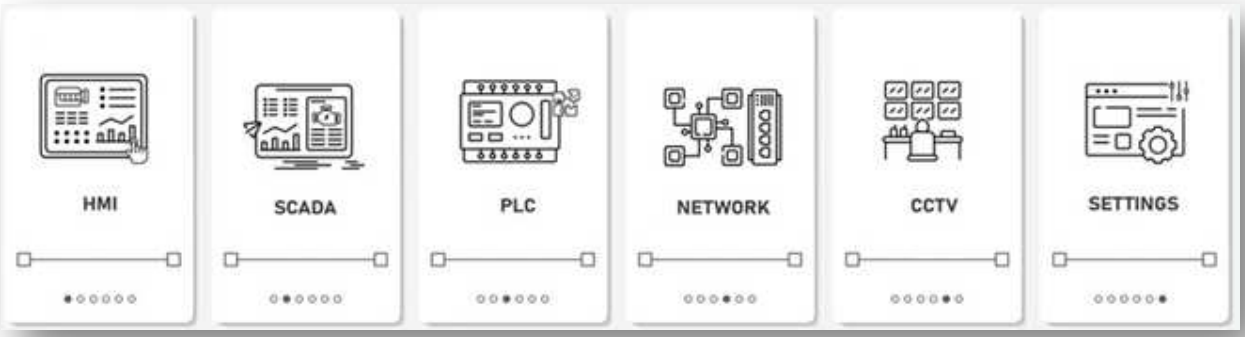


Figura 4. Algunos dispositivos que se encuentran en entornos industriales.

En los últimos años, se ha observado una creciente convergencia entre los sistemas IT y OT, impulsada por la necesidad de una mayor coordinación y eficiencia en las operaciones empresariales. Esta tendencia ha llevado a una mayor integración y sinergia entre dichos sistemas, generando nuevos paradigmas relacionados a la operatoria de estas organizaciones.

## 1.4. Diferencias para tener en cuenta y entender ambas redes.

Existen varias diferencias claves entre los sistemas de IT y OT. En primer lugar, los sistemas IT están diseñados para procesar, almacenar y transmitir información y datos, mientras que los sistemas industriales se centran en controlar y supervisar procesos físicos en tiempo real, como la producción, la distribución y la gestión de energía. Igualmente, utilizan tecnologías específicas para su industria o aplicación, como protocolos de comunicación serie o bus de campo.

En términos de requerimientos de tiempo real, los sistemas OT deben responder rápidamente a eventos y cambios en el entorno físico, ya que suelen estar

[9] ¿Qué es SCADA? Tomado de: https://www.nvtecnologias.com/blog/blog-1/que-es-scada-10 el 01/11/2024 a las 14:45 el 01/06/2024

involucrados en procesos en tiempo real. Por otro lado, los sistemas IT generalmente tienen plazos de respuesta menos críticos.

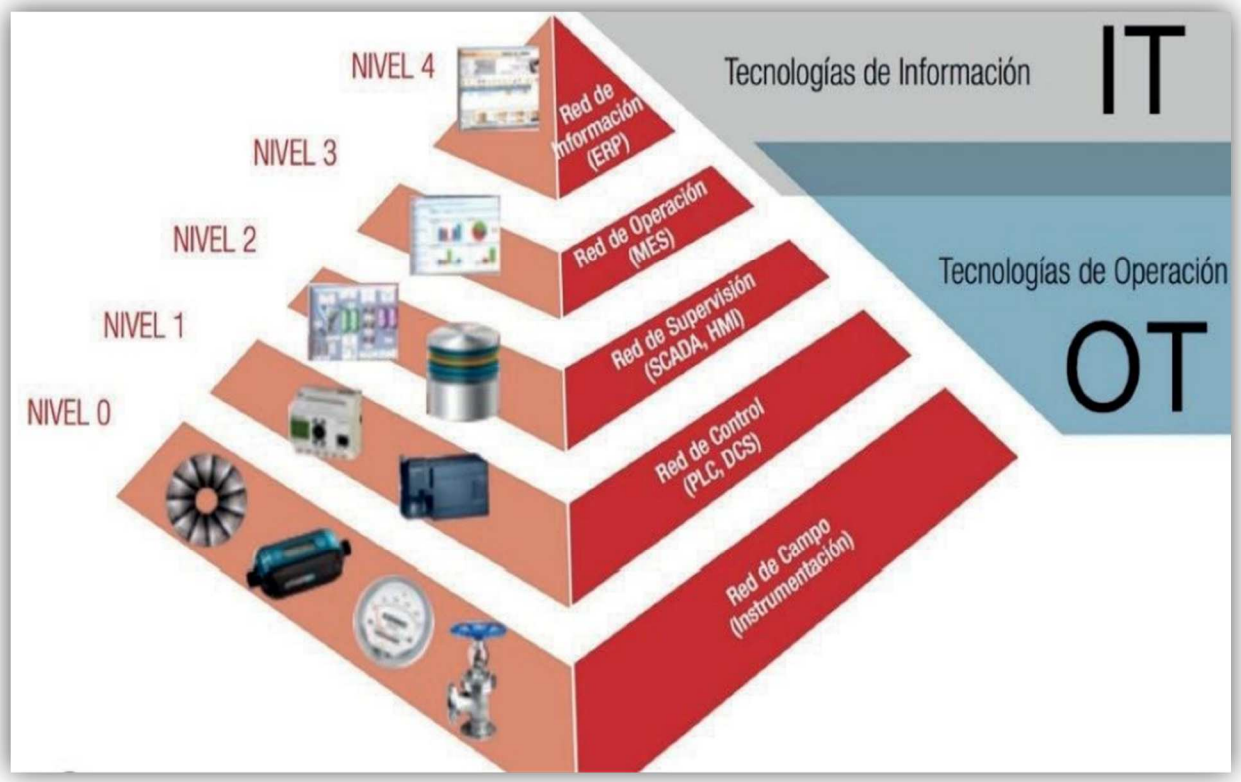


Figura 5. Pirámide de Automatización Industrial.[10]

En la figura anterior, se muestran distintos niveles vinculados a las redes IT y las OT, detalladas a continuación:

- **Capa 0:** Representa la capa física donde el foco son los dispositivos de campo y la transmisión de señales, ya sean analógicas o digitales. Esta capa incluye, por ejemplo, sensores de movimiento, temperatura, niveles y magnetismo, así como actuadores.
- **Capa 1:** Aquí se encuentran los dispositivos como los Controladores lógicos programables o PLC, la Unidad terminal remota o RTU y los Sistemas de Control Distribuido o DCS.
- **Capa 2:** Poseen herramientas como HMI y/o sistemas SCADA, en donde se recopila automáticamente toda la información de los PLC y/o RTU

[10] Guía de bolsillo: Ciberseguridad en la Pirámide de Automatización Industrial. Tomado de: https://www.cci-es.org/activities/guia-de-bolsillo-ciberseguridad-en-la-piramide-de-automatizacion-industrial/ el 01/15/2024 a las 21:42

distribuidos, y se comienza a utilizar el protocolo TCP/IP. Este es la interfaz utilizada por los operadores de planta.

- **Capa 3:** Es la capa del Sistema de Ejecución de Manufactura ó MES, cuyo objetivo es evaluar la eficiencia del proceso a partir de la información recibida, en lugar de evaluar el proceso en sí mismo.
- **Capa 4:** Es la capa de Planificación de Recursos Empresariales. En esta capa se decide qué controles ejecutar y con qué frecuencia y esfuerzo, con el fin de disponer de una planificación coherente.

## 1.5. Recomendaciones en la convergencia segura de las redes IT y OT.

La integración de los mundos IT y OT aporta mejoras significativas a los procesos industriales. En el ámbito energético, permite adaptar el consumo de energía según los horarios de tarifas más económicas, gracias a la interconexión de nuevos dispositivos. En cuanto al medio ambiente, los dispositivos inteligentes pueden medir datos meteorológicos y energéticos, lo que facilita el cumplimiento de los niveles de contaminación establecidos por la ley, lo cual permite adaptar la producción para cumplir con los estándares medioambientales.

En el ámbito productivo posibilita la adaptación de la demanda del cliente a la producción, lo que optimiza la eficiencia y ahorra costos. Al mismo tiempo, en el control de calidad, permite fabricar con precisión y rapidez sin afectar el ritmo de producción. En el sector del mantenimiento, tanto la integración como la convergencia ofrecen la capacidad de realizar un mantenimiento predictivo, lo cual reduce las averías y permite diseñar un mantenimiento más eficiente para minimizar las pérdidas que estas puedan ocasionar.

En síntesis, esta convergencia cibersegura en entornos industriales brinda eficiencia, visibilidad y controles cada vez mejores y más tecnificados. Esto se traduce en la optimización de procesos, monitoreo remoto, toma de decisiones basada en datos y reducción de costos operativos. Sin embargo, esto requiere de una inversión que implica la implementación de firewalls industriales, segmentación de redes, autenticación en múltiples factores, monitoreo continuo de amenazas y vulnerabilidades, actualizaciones de seguridad periódicas y capacitación del personal en ciberseguridad.

## CAPITULO 2. Soluciones de Ciberseguridad para la Convergencia IT y OT.

El constante flujo de diversas tecnologías, dispositivos, software, puertos y comunicaciones en entornos industriales ha generado una nuevos paradigmas y variables para evitar una desorganización en el proceso de transformación digital. Esta situación se vuelve aún más complicada para los expertos provenientes de disciplinas no operativas, dificultando la comprensión del verdadero impacto que estas innovaciones tecnológicas tienen en las organizaciones y en la economía en general.

En este escenario, es crucial resaltar la importancia de la ciberseguridad, los dispositivos de IoT y la convergencia IT y OT, ya que se enfrentan a un cambio radical que resultará en transformaciones fundamentales en aspectos vitales como el modelo de negocio, los resultados, el talento y el propio ecosistema. Este verdadero desafío que solo ofrece dos posibles resultados: salir fortalecidos o quedarse rezagados en la cuarta ola de la globalización.

Hasta hace muy pocos años, estos entornos habían permanecido aislados, desarrollándose de manera independiente. En el futuro cercano, se espera que ambos se beneficien de los avances del otro. Sin embargo, no todo son beneficios; la mezcla de estos dos mundos aumenta la superficie de ataque y los riesgos, amenazas y vulnerabilidades de seguridad de sus dispositivos y sistemas.

Por otro lado, es esencial que todos los integrantes en las empresas comprendan a fondo las características de estas tecnologías, sus definiciones, aplicaciones e impacto y no se puede subestimar la importancia de asegurar cada etapa de implementación y uso de estas tecnologías, resguardando los datos, protegiendo los diferentes dispositivos, segmentando las redes, sistemas y activos empresariales de posibles ciberataques. De esta forma, podrán abordar estos desafíos con confianza y garantizar un desarrollo exitoso en este nuevo panorama tecnológico.

### 2.1 Soluciones de Ciberseguridad en la convergencia IT y OT.

En entornos industriales, se suelen utilizar una variedad de equipos de ciberseguridad especializados para proteger los sistemas y las operaciones. Algunos de estos equipos incluyen firewalls industriales, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), switches y routers, dispositivos de seguridad de redes y sistemas de gestión de seguridad y monitoreo de activos industriales, entre otros. A continuación, se incluye un breve resumen de algunos de los más importantes.

### 2.1.1 Firewalls industriales.

Estos dispositivos protegen las redes industriales de amenazas externas, controlan el tráfico entre las redes IT y OT y ofrecen una capa adicional de seguridad crucial para proteger las redes y sistemas de control en entornos industriales. Al establecer reglas de acceso y filtrar el tráfico de red, ayudan a prevenir intrusiones no autorizadas, ataques cibernéticos y el acceso no deseado a los dispositivos críticos de la infraestructura.


Figura 6. Cortafuego Industrial Schneider Electric.[11]

[11] CXM TOFINO FIREWALL INSPECCION E/IP. Tomado de: https://www.se.com/ar/es/product/TCSEFEA23F3F22/cxm-tofino-firewall-inspeccion-e-ip/ el 1/16/2024 a las 19:06

Además, al proporcionar visibilidad y control sobre el tráfico de red, los firewalls industriales permiten una supervisión constante y la capacidad de tomar medidas proactivas para mitigar las amenazas de seguridad. En resumen, su implementación fortalece la ciberseguridad y la fiabilidad de las operaciones industriales, contribuyendo a la protección de activos, la continuidad del negocio y la seguridad del personal.

### 2.1.2 Sistemas de detección de intrusiones (IDS).

Estos sistemas se encargan de monitorear y proteger las redes contra actividades sospechosas y ataques cibernéticos. En otras palabras, estos sistemas no solo detectan accesos no autorizados y supervisan el tráfico entrante, sino que también han avanzado para identificar dispositivos industriales específicos, como controladores lógicos programables o PLC e interfaces hombre-máquina conocidos HM), así como para comprender los protocolos de comunicación industriales como S7, Modbus y DNP3, entre otros.

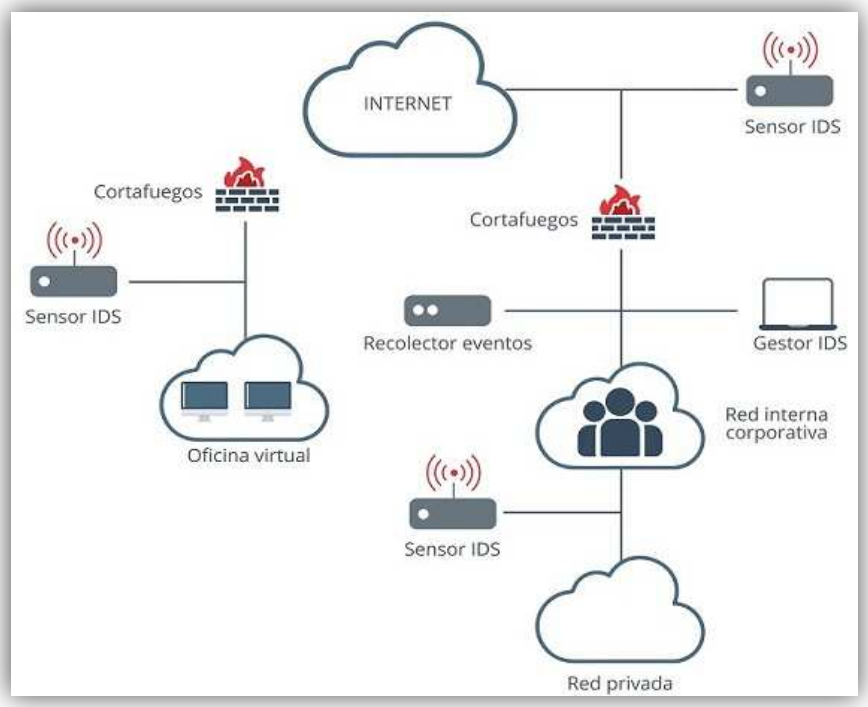


Figura 7. IDS en arquitectura de red.[12]

[12] Soluciones IDS en entornos industriales. Tomado de: https://www.incibe.es/incibe-cert/blog/soluciones-ids-en-entornos-industriales el 01/16/2024 a las 20:13

Los Sistemas de Detección de Intrusos han evolucionado significativamente para satisfacer las demandas de los entornos OT. Esta evolución es fundamental para asegurar la protección de los entornos de control industrial, proporcionando una capa de defensa especializada que se adapta a las necesidades y complejidades de las redes y sistemas en entornos de operaciones industriales.

### 2.1.3 Sistemas de prevención de intrusiones (IPS).

Los sistemas de prevención de intrusiones o IPS conforman la herramienta de seguridad que monitorea y analiza el tráfico de red en busca de actividades sospechosas o maliciosas. A diferencia de un IDS que solo detecta y alerta sobre posibles intrusiones, un IPS tiene la capacidad adicional de tomar medidas activas para bloquear o prevenir ataques en tiempo real. En ambientes de fabricación o manufactura, pueden proteger sistemas críticos al detener de manera proactiva actividades no autorizadas o maliciosas, garantizando la integridad y seguridad de la infraestructura operativa.

### 2.1.4 Seguridad de endpoints.

Para garantizar la ciberseguridad en los diversos dispositivos en entornos industriales o con tecnologías operativas, es fundamental comprender la naturaleza específica de cada sector empresarial. La estrategia de seguridad no es la misma para una empresa de gas y petróleo que para una del sector de alimentos y bebidas, ya que el enfoque de seguridad varía.

Sin embargo, es crucial implementar medidas como la segmentación de red, para limitar la propagación de amenazas, mantener actualizados los sistemas con parches de seguridad, controlar el acceso a los sistemas críticos, monitorear continuamente posibles amenazas, utilizar protección antivirus y antimalware y capacitar al personal en buenas prácticas de seguridad. Estas acciones combinadas fortalecerán la ciberseguridad y protegerán los endpoints y sistemas críticos, ofreciendo soluciones que protejan los dispositivos finales, como computadoras y dispositivos IoT, en las redes de IT y OT.

### 2.1.5 Seguridad de red.

La seguridad es fundamental en las redes industriales y el modelo de Purdue es una referencia importante para ello. Dividir la red en niveles y establecer una DMZ entre los entornos IT y OT es una práctica sólida para proteger los sistemas críticos. Implementar medidas como firewalls, VPN y autenticación de usuarios también es crucial para lograr una seguridad óptima, que incluyen herramientas para asegurar la integridad y confidencialidad de la comunicación entre dispositivos en las redes convergentes.

### 2.1.6 Análisis de seguridad y gestión de eventos (SIEM).

Estos programas utilizan una variedad de tecnologías para recopilar, analizar y correlacionar datos de seguridad, que incluyen la recopilación de registros (logs) de dispositivos y sistemas, análisis de comportamiento de usuarios, detección de amenazas en tiempo real, gestión de incidentes de seguridad, inteligencia de amenazas, y capacidades de cumplimiento normativo.


Figura 8. Tecnología relacionada en un SIEM.[13]

[13] XDR vs SIEM. Tomado de: https://lab.wallarm.com/what/xdr-vs-siem-unveiling-the-next-generation-of-threat-detection-and-response/ el 01/16/2024 a las 21:26

Además, los SIEM (Administrador de eventos de seguridad e información) a menudo incorporan técnicas de aprendizaje automático y análisis de big data para identificar patrones anómalos que podrían indicar actividades maliciosas. En entornos industriales, el hecho de implementar un SIEM es crucial para monitorear y gestionar la seguridad de la red. Estos sistemas permiten recopilar, analizar y correlacionar datos de diferentes fuentes dentro del entorno industrial, como sistemas de control, dispositivos de red y aplicaciones. Esto proporciona una visión integral de la postura de seguridad, ayuda a detectar amenazas y facilita la respuesta a incidentes de seguridad de manera proactiva.

También es fundamental para cumplir con los requisitos de auditoría y las normativas de seguridad, brindando una capa adicional de protección para los sistemas críticos de la planta. Posee herramientas que recopilan, correlacionan y analizan datos de seguridad de múltiples fuentes para detectar y responder a amenazas.

### 2.1.7 Seguridad de acceso remoto.

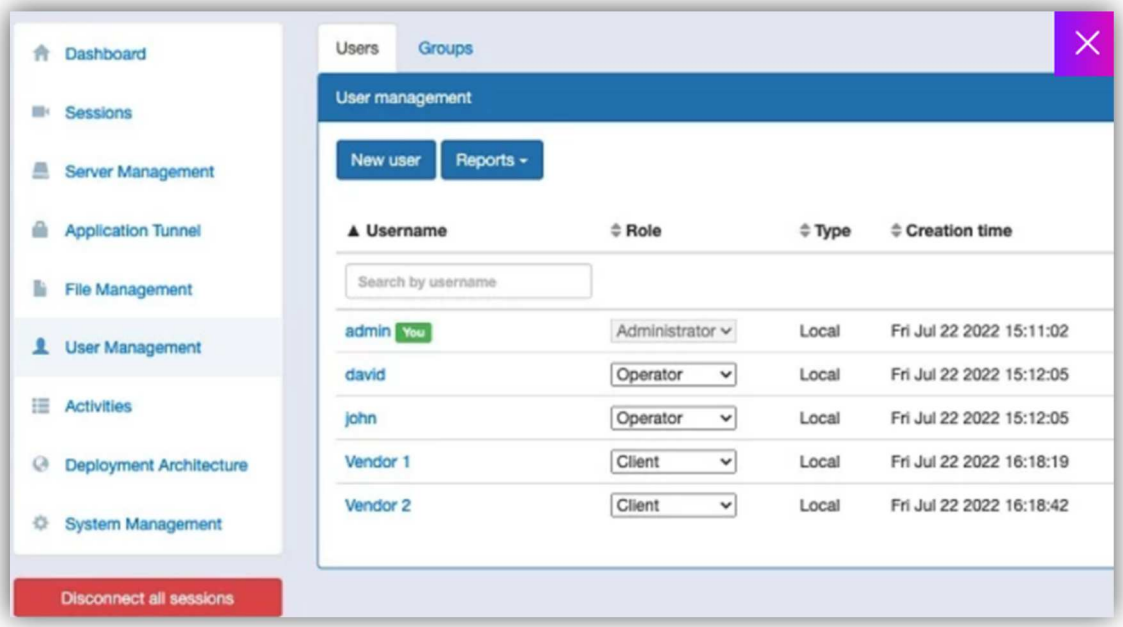


Figura 9. Acceso remoto seguro (SRA) de Claroty.[14]

[14] Secure Remote Access by Claroty, Tomado de: https://claroty.com/ndustrial-cybersecurity/sra el 01/02/2024 a las 02:46

Este tipo de soluciones permiten un acceso seguro a los sistemas de OT desde la red de IT, utilizando redes privadas virtuales (VPN) industriales. Un sistema de acceso remoto seguro es una infraestructura que permite a usuarios autorizados conectarse de forma segura a redes o sistemas desde ubicaciones externas. Este tipo de sistema emplea protocolos y tecnologías que garantizan la confidencialidad, integridad y autenticación de la información transmitida a través de la conexión remota.

Igualmente, suele incluir mecanismos de control de acceso para garantizar que solo usuarios autorizados puedan acceder a los recursos de la red. Algunas tecnologías comunes utilizadas para lograr un acceso remoto seguro incluyen VPN, autenticación multifactorial, encriptación de datos y monitoreo de la actividad de los usuarios.

### 2.1.8 Control de acceso físico y lógico.

Los sistemas de control de acceso físico se encargan de regular la entrada y salida a instalaciones físicas, como edificios, habitaciones o áreas restringidas, utilizando tecnologías como cerraduras electrónicas, tarjetas de acceso o sistemas biométricos, entre otros. Por otro lado, un sistema de control de acceso lógico se enfoca en regular el acceso a sistemas informáticos, redes o datos digitales, utilizando medidas como contraseñas, autenticación de dos factores o certificados digitales, entre otros.

Ambos sistemas comparten el objetivo de garantizar la seguridad y la protección de activos, ya sean físicos o digitales, controlando quién tiene acceso a ellos y en qué condiciones. La integración de ambos tipos de sistemas puede proporcionar una capa adicional de seguridad y control de acceso integral en entornos que requieren protección tanto física como digital.

Este sistema proporciona una forma conveniente y segura de gestionar el acceso a edificios, áreas restringidas o dispositivos, ya que elimina la necesidad de llaves físicas, y permite una gestión centralizada de los permisos de acceso. El sistema de control de accesos con tecnología de radio frecuencia (RFID) de Siemens, por ejemplo, funciona de la siguiente manera:

- **Identificación:** Los usuarios autorizados llevan tarjetas o etiquetas RFID que contienen información de identificación única.
- **Lectura:** Cuando un usuario se acerca a un lector de RFID, este lee la información de la tarjeta o etiqueta.
- **Verificación:** El lector envía la información al sistema de control de accesos, que verifica la identidad y los permisos del usuario.
- **Autorización:** Si la identificación es válida, el sistema de control de accesos otorga acceso al usuario a las áreas o recursos autorizados.


Figura 10. Sistema RFID de control de acceso de Siemens.[15]

### 2.1.9 Seguridad de protocolos de comunicación industrial.

Un protocolo consiste en un conjunto de reglas para la comunicación entre dispositivos que procuran la comunicación en red. En el contexto de la automatización de procesos en entornos operativos, las redes de comunicación industrial se emplean en sistemas de control para transferir datos entre dispositivos de campo, entre

[15] Sistema RFID de control de acceso de Siemens. Tomado de: https://www.digitalsecuritymagazine.com/2017/02/09/siemens-simplifica-el-control-de-acceso-en-entornos-industriales-con-un-sistema-rfid/ el 01/16/2024 a las 22:34

diferentes PLC o entre PLC y computadoras personales utilizadas para la interfaz del operario, procesamiento y almacenamiento de datos o información de gestión.

La ciberseguridad sobre los protocolos de comunicación industrial se logra mediante varias prácticas y medidas de protección. En primer lugar, se implementa una protección para la red a través de firewalls, segmentación de redes, VPN y detección de intrusiones para proteger el tráfico de datos industrial. Sin embargo, debido a su rendimiento limitado, los protocolos serie no son la mejor elección para aplicaciones de alta velocidad y otras más exigentes. Algunos de los protocolos más comunes utilizados en el ámbito industrial se muestran en la siguiente figura:

| PROTOCOLOS INDUSTRIALES POR APLICACIÓN FINAL | |
|---|---|
| **Automatización de procesos** | Modbus, PROFINET IO, RAPIEnet, Honeywell SDS, SERCOS III, SERCOS interface, SSCNET, GE SRTP, Sinec H1, SynqNet, TTEthernet, MPI |
| **Automatización de Edificios** | Smart-BUS (SBUS), ELAN-Net, 1-Wire, BACnet, C-Bus, CC-Link, DALI, DSI, Dynet, EnOcean, KNX, LonTalk, Modbus RTU or ASCII or TCP, oBIX, HDL-Bus, TIS-BUS, VSCP, xAP, x10, Z-Ware – WirelessRF Protocol, ZigBee, UPB, INSTEON |
| **Controles Industriales** | MTConnect, OPC, OPC-UA, Woopsa |
| **Automatización de sistemas eléctrico** | DNP3, IEC 60870-5, IEC 61850, IEC 62351 |
| **Lectura automática de contadores** | ANSI C12.18, DLMS/IEC 62056, IEC 61107, M-Bus, ZigBee Smart Energy 2.0, Modbus, ANSI C12.21, ANSI C12.22 |
| **Protocolo bases para automóviles/vehículos** | Controller Area Network (CAN), DC-BUS[3], flexRay, IDB-1394, IEBus, J1708, J1939 and ISO 11783, Keyword Protocol 2000 (KWP2000), Local Interconnect Network (LIN), Media Oriented Sustems Transport (MOST), SMARTwireX, Vehivle Area Network (VAN) |

Figura 11. Protocolos industriales por Aplicación final.[16]

[16] Guía de protocolos de conectividad industrial. Tomado de: https://www.arrow.com/es-mx/research-and-events/articles/industrial-connectivity-protocols el 01/17/2024 a las 18:12

La comunicación sigue siendo rápida al interactuar con varios dispositivos distintos en el mismo cable, gracias a la alta velocidad de Ethernet en comparación con las antiguas redes serie. También, se emplean mecanismos de autenticación fuerte y autorización granular para restringir el acceso a los dispositivos y sistemas industriales.

De lo anterior, Ethernet ha surgido como el estándar dominante para la capa física de muchos protocolos industriales, como EtherNet/IP, Ethernet TCP/IP, Modbus TCP/IP y Profinet. Al emplear Ethernet, conectar varios dispositivos como PLC, HMI, E/S de campo y bancos de válvulas no es demasiado complicado. Por último, se implementan sistemas de monitoreo y análisis de seguridad para detectar y responder a posibles amenazas cibernéticas en tiempo real. Estas prácticas ayudan a proteger los sistemas de control industrial, las redes de automatización y los protocolos de comunicación contra ciberataques, garantizando su funcionamiento seguro y confiable.

### 2.1.10 Seguridad de sistemas de Supervisión y adquisición de control de datos SCADA.

Figura 12. EcoStruxure™ Power SCADA Operation Schneider Electric.[17]

[17] EcoStruxure™ Power SCADA Operation. Tomado de: https://www.se.com/mx/es/product-range/63067-ecostruxure-power-scada-operation/ el 01/17/2024 a las 16:43

Hablar de un sistema de control y supervisión es pensar en la capacidad de una herramienta para mejorar la eficiencia y productividad en la industria. Los operadores pueden monitorear y controlar los procesos industriales a distancia, lo que les facilita la detección y resolución rápida de problemas. Son ampliamente empleados en diversas industrias, como la energía, manufactura, petróleo, gas y transporte. El propósito principal de un sistema SCADA[18] es habilitar a los operadores de una planta o fábrica para supervisar y controlar los procesos industriales de manera remota.

Estos sistemas generalmente constan de tres componentes principales: los dispositivos de adquisición y suministro de datos, las redes de comunicación, que transmiten los datos desde su origen hasta el centro de control y el software de supervisión, que visualiza los datos y permite a los operadores realizar ajustes en el sistema. Además, los sistemas SCADA pueden recopilar grandes cantidades de datos, lo que permite a las empresas optimizar sus procesos y mejorar la calidad de sus productos.

### 2.1.11 Soluciones de gestión de identidad y acceso (IAM) para entornos industriales.

Las soluciones de gestión de identidad y acceso (IAM) para entornos industriales se centran en controlar y asegurar quién tiene acceso a qué recursos en un entorno corporativo. Esto incluye la gestión de identidades de usuarios, autenticación, autorización y auditoría de actividades. Estas soluciones son fundamentales para garantizar la seguridad, la integridad de los datos y el cumplimiento de las normativas en entornos industriales.

Estas abordan desafíos específicos, como la necesidad de gestionar múltiples sistemas de control y monitoreo, controlar el acceso a activos críticos, y garantizar la trazabilidad y la responsabilidad de las acciones realizadas en entornos industriales. Estas soluciones suelen incluir funciones de gestión de credenciales, autenticación de múltiples factores, control de acceso basado en roles y privilegios, y generación de informes de auditoría para cumplir con los estándares de seguridad y normativas industriales.

[18] ¿Qué es un SCADA? Tomado de: https://ceiinc.co/que-es-un-scada/ el 01/17/2024 a las 16:49

Con este tipo de soluciones para integrar la seguridad en el desarrollo de aplicaciones y para adoptar el enfoque de *DevSecOps.* Es un componente fundamental para establecer un sólido enfoque de seguridad en entornos virtuales, *bare metal*[19], nube y contenedores. Es importante que el sistema IAM pueda adaptarse a diferentes entornos y cargas de trabajo, desde el desarrollo hasta la supervisión de las aplicaciones.


Figura 13. Componentes de la gestión de acceso e identidades.[20]

Una vez definidas las necesidades de seguridad de la empresa, es necesario implementar una solución IAM, que puede ser independiente, un servicio gestionado de identidades o un servicio de suscripción a la nube de un tercero, como *Identity as a Service* (IDaaS). Este sistema IAM asegura que solo las personas autorizadas tengan acceso a funciones críticas, como el monitoreo y control de procesos industriales, garantizando la seguridad y la integridad de las operaciones.

## 2.2 Recomendaciones para implementar seguridad en la convergencia IT y OT.

Para comprender la diferencia fundamental entre estas redes, es crucial señalar qué en las redes industriales, la implementación de sistemas antivirus, por ejemplo,

[19] El término "bare metal" se utiliza para describir entornos en los que el software se ejecuta directamente sobre la infraestructura física, sin una capa adicional de virtualización o sistema operativo de por medio. Esto es común en el caso de máquinas virtuales, servidores y dispositivos embebidos.
[20] 5 hechos fundamentales que debe conocer acerca de la gestión de identidades y acceso. Tomado de: https://blogs.manageengine.co.m/espanol/2017/12/03/cinco-aspectos-sobre-control-de-acceso-identidades-iam.html el 01/17/2024 a las 18:40

es desafiante y poco común en ciertos sectores de la industria. También, los componentes de estas redes tienen una vida útil de 10 a 30 años, lo que resulta en una aplicación poco frecuente de parches de aplicaciones y pruebas de seguridad. En cambio, en los entornos de redes con tecnologías informáticas, los componentes tienen una vida útil de 3 a 5 años, se utilizan servicios de outsourcing y antivirus con mayor frecuencia, se aplican parches a las aplicaciones de forma regular y se realizan pruebas de vulnerabilidad con mayor periodicidad. Es así como protocolos industriales salvo algunas versiones de DNP3 plantean encriptación como opción, en contraste Modbus, Profibus y Profinet no incluyen ese tipo de protección adicional.

En este punto, se hace necesario detallar los puertos de comunicación más seguros en entornos industriales y recomendados por el mercado, que son los siguientes:

- **Modbus TCP (puerto 502):** Utilizado en sistemas de automatización y control.
- **OPC UA (puertos 4840 y 4841):** Se usa para el intercambio de datos.
- **DNP3 (puerto 20000):** Protocolo comúnmente utilizado en sistemas de control y monitoreo de infraestructuras críticas, como electricidad y agua.

Estos puertos suelen estar asociados con protocolos de comunicación diseñados específicamente para entornos industriales y suelen ser seguros cuando se implementan adecuadamente. Sin embargo, es importante tener en cuenta que la seguridad no solo depende del puerto en sí, sino también de las prácticas de configuración, autenticación, cifrado, control de acceso, monitoreo de tráfico y actualización regular de sistemas y dispositivos para garantizar la protección de la infraestructura crítica.

Con respecto a cómo aplicar ciberseguridad en sistemas SCADA, se pueden implementar varias prácticas que aumenten su nivel de protección, entre las cuales se encuentran:

- **Segmentación de red:** Separar la red de sistemas SCADA de otras redes corporativas para reducir la superficie de ataque y limitar el acceso no autorizado.
- **Autenticación:** Implementar autenticación de múltiples factores y políticas de contraseñas robustas para controlar el acceso a los sistemas SCADA.

- **Actualizaciones y parches:** Mantener actualizados todos los componentes del sistema SCADA, incluyendo software, firmware y sistemas operativos, para mitigar vulnerabilidades conocidas.
- **Monitoreo de tráfico:** Utilizar herramientas de monitoreo de red para detectar y responder a actividades anómalas o no autorizadas en los sistemas SCADA.
- **Capacitación del personal:** Educar a los operadores y personal de mantenimiento sobre las mejores prácticas de seguridad cibernética y concientizar sobre las amenazas potenciales.
- **Control de Acceso:** Limitar el acceso físico y lógico a los dispositivos y sistemas SCADA solo a personal autorizado.
- **Respaldo de datos:** Implementar procedimientos de respaldo y recuperación regulares y seguros para proteger la integridad de los datos en caso de un incidente de seguridad.

A la par, se le puede sumar el paradigma de la seguridad por defecto, en donde se aclara que una seguridad efectiva no se puede simplemente aplicar superficialmente a los procesos operativos del sistema existente, sino que debe ser integrada de manera inherente en los diseños y configuraciones, a los procedimientos operativos y a las tecnologías informáticas.

Este enfoque limita las funciones de operación, administración y registro de actividad solo a personal autorizado, aplicando restricciones de horario y ubicación, y eliminando funciones innecesarias o inapropiadas. Esto abarca varios aspectos, como el diseño de los componentes, las implementaciones de software, la configuración de los sistemas, las configuraciones de red, los procedimientos de planificación y la gestión de datos.

Es crucial estar al tanto de las posibles amenazas y vulnerabilidades a través de un análisis de riesgo que considere los entornos en los que se desplegará el componente. A través del monitoreo continuo y 24/7 de las redes informáticas y operativas, proporcionará una visión más completa de las vulnerabilidades, amenazas, riesgos y nuevos vectores de ataque a los que se enfrentan estas redes dentro del marco de la convergencia.

En cuanto a los dispositivos conectados en entornos industriales, los Centros de Control son críticos para la supervisión, detección de fallos y garantía de seguridad por lo cual, es fundamental desarrollar sistemas de operación seguros que protejan estos centros ante posibles intrusiones. Un acceso no autorizado podría tener consecuencias devastadoras, como la interrupción del suministro eléctrico en múltiples localidades.

En conclusión, se debe reconocer la importancia de salvaguardar estos entornos críticos, ya que un acceso no autorizado a los centros de control podría resultar en consecuencias catastróficas para la supervivencia de la organización y para vastos sectores de la sociedad. Por lo tanto, implementar medidas de protección que garanticen su integridad y continuidad operativa es un imperativo.

## CAPITULO 3. Estándares y/o mejores prácticas aplicadas a la Ciberseguridad en la convergencia IT y OT.

La aplicación de normas, estándares y mejores prácticas de ciberseguridad industrial y de IT en los procesos productivos donde convergen redes y que es esencial por varias razones. En primer lugar, ayuda a proteger los activos críticos involucrados en estos procesos, como sistemas de control y robots industriales, contra amenazas internas y externas. Esto minimiza el riesgo de interrupciones operativas o daños a la infraestructura, además, garantiza la integridad de los datos que se transfieren entre los mencionados sistemas. La manipulación no autorizada o la corrupción de datos críticos pueden generar consecuencias graves tanto a la reputación como a la producción intelectual de una organización. Las normas y mejores prácticas de ciberseguridad establecen controles y medidas de protección para asegurar la integridad de los datos en tránsito y en reposo.

La interconexión de estas redes incrementa las amenazas y posibles ataques cibernéticos y las vulnerabilidades de un sistema por lo que la aplicación de estas normas y mejores prácticas ayudan a identificar y mitigar los riesgos asociados, como agresiones causadas por malware o intrusiones no autorizadas. Esto permite mantener la confidencialidad, integridad y disponibilidad de los sistemas y datos involucrados.

Por último, muchas industrias están sujetas a regulaciones y estándares específicos dependiendo sea su rubro en cuanto a la ciberseguridad, y que en países norteamericanos y/o europeos, se exigen como requisito para hacer negocios por lo que se hace casi una necesidad se tenga en cuenta su implementación y esencial para evitar sanciones legales y mantener la confianza de los clientes y socios comerciales. A continuación, se presentan algunas de estos estándares y mejores prácticas.

### 3.1 ANSI/ISA-95: Enfocado en la integración de la empresa y los sistemas de control.

El estándar ISA-95[21] es reconocido a nivel internacional por su enfoque en la integración de sistemas empresariales y de control. Sin embargo, el título de las normas no refleja completamente su valor. La implementación de este estándar puede proporcionar una perspectiva integral de la empresa para la integración de sistemas, permitiendo la recopilación y resumen de una gran cantidad de acciones y datos en un marco comprensible.

También conocido como ISA-95, se centra en la integración de sistemas empresariales y de control en entornos de fabricación y producción, proporcionando un marco para la integración de sistemas de control de procesos (nivel de planta) con los sistemas de información empresarial (nivel de empresa).

Dentro de sus principales aportes, se encuentra el de definir modelos para interfaces y flujos de información entre sistemas de control y sistemas empresariales, lo que facilita la interoperabilidad y la integración efectiva de datos en toda la empresa y tiene aplicaciones diversas, como guía para la definición de requisitos de usuario, para la selección de proveedores y en el desarrollo de sistemas y bases de datos.

### 3.2 La norma IEC/ISO 62443.

Este estándar, ampliamente reconocido en el campo de la ciberseguridad industrial, proporciona directrices detalladas para la protección de sistemas de automatización y control industrial contra amenazas cibernéticas. Es uno de los más usados en este tipo de organizaciones. Asimismo, aborda aspectos claves como la gestión de riesgos, la seguridad en el diseño y la implementación de controles seguros. Al seguir la IEC/ISO 62443, las organizaciones pueden fortalecer la seguridad de sus sistemas industriales, garantizando la integridad, confidencialidad y disponibilidad de los datos y procesos críticos, así como la continuidad de estos últimos.

Además, promueve la segmentación de redes, la gestión de identidad y acceso, el monitoreo de seguridad y la respuesta a incidentes, ayudando a mitigar y prevenir posibles ataques cibernéticos en entornos industriales. Implementar la IEC

[21] ISA 95 y Gestión de Operaciones de Fabricación. Tomado de: https://www.plm.automation.siemens.com/global/en/our-story/glossary/isa-95-framework-and-layers/53244 el 01/17/2024 a las 20:28

62443 es esencial para garantizar la resiliencia y la protección de los sistemas industriales frente a las crecientes amenazas cibernéticas actuales.

Es importante destacar que la implementación de la IEC-62443 requiere un enfoque holístico y la colaboración de diferentes partes interesadas, incluyendo a los fabricantes de equipos, proveedores de servicios, integradores de sistemas y usuarios finales. Al adoptar este estándar, las organizaciones pueden fortalecer su resiliencia ante amenazas cibernéticas y mantener un entorno industrial seguro y protegido.

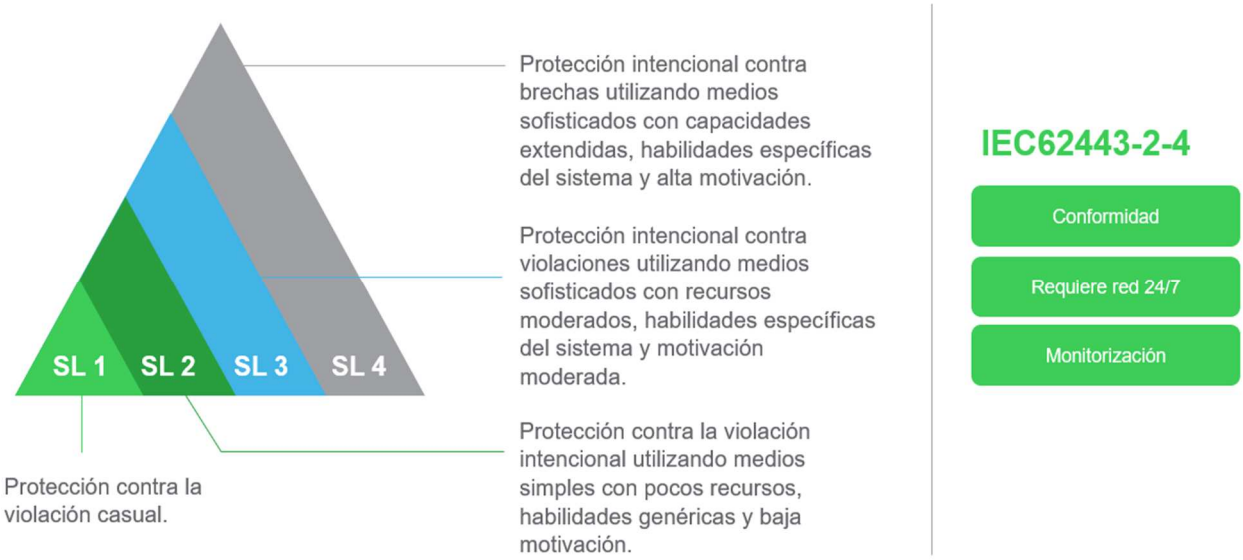


Figura 14. Niveles de seguridad dentro de IEC62443.[22]

Este fue desarrollado por la Sociedad Internacional de Automatización (ISA) y aprobado por el Instituto Nacional Estadounidense de Estándares (ANSI), y establece un enfoque de múltiples capas para la seguridad cibernética, abarcando desde la evaluación de riesgos hasta la implementación de medidas de protección. Proporciona directrices claras sobre cómo identificar y mitigar los riesgos de seguridad en los entornos industriales, abordando aspectos como la seguridad de la red, la gestión de accesos, la detección y respuesta a incidentes, y la seguridad física de los sistemas.

[22] Estándar IEC 62443. Tomado de: https://www.bureauveritas.es/certificacion/ciberseguridad-y-proteccion-de-datos/IEC-62443 el 01/23/2024 a las 16:48

La Comisión Electrotécnica Internacional IEC adoptó la norma ISO 62443 en 2013 para proporcionar un marco integral de ciberseguridad para sistemas de automatización y control industrial. Esta adopción fue motivada por la necesidad de establecer estándares de ciberseguridad específicos para el entorno de operaciones industriales, con el fin de proteger los activos críticos y garantizar la continuidad operativa. En la siguiente figura, se ilustra los cuatro niveles de protección que ofrece esta norma y explica la profundidad al que apunta su defensa en cada una:

### 3.3 NIST SP 800-82

Se trata de una publicación especial del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos que aborda la seguridad de los sistemas de control industrial. Este documento, titulado "Guide to Industrial Control Systems (ICS) Security", proporciona pautas y mejores prácticas para proteger los sistemas de control industrial contra amenazas cibernéticas.

Este documento se centra en la protección de los sistemas de control industrial, que abarcan desde infraestructuras críticas como plantas de energía y refinerías, hasta sistemas de control de procesos en sectores como la manufactura y la distribución de agua y gas. Este estándar ofrece un enfoque detallado para evaluar los riesgos, implementar controles de seguridad y gestionar incidentes en entornos de control industrial. Los principales puntos del marco de trabajo del NIST 800-82 incluyen:

- Identificación y autenticación de usuarios y dispositivos.
- Protección de datos y control de acceso.
- Detección y respuesta a incidentes de seguridad.
- Seguridad de la red y de la arquitectura de sistemas.
- Gestión de la configuración y mantenimiento de la seguridad.

Estos puntos forman un marco integral para mejorar la ciberseguridad de sistemas de control y automatización industrial. La publicación proporciona directrices sobre la seguridad de la red, la segmentación de redes, la autenticación y autorización, la gestión de parches y actualizaciones y la monitorización de seguridad.

También aborda aspectos específicos relacionados con la seguridad de los protocolos de comunicación y la protección de los sistemas de control industrial frente a amenazas físicas.

### 3.4 NERC CIP: Estándares de Ciberseguridad para el sector eléctrico en los EEUU.

El conjunto de normas NERC CIP propuestos por la Corporación Norteamericana de Fiabilidad Eléctrica[23] consiste en un compendio de mejores prácticas en ciberseguridad diseñadas para proteger los activos y sistemas necesarios para operar el sistema eléctrico de alta tensión de América del Norte. Estas normas tienen como objetivo mitigar los riesgos de ciberseguridad y garantizar la fiabilidad y seguridad de la red eléctrica. Su propósito es mejorar la seguridad de los sistemas de distribución eléctrica. Para lograrlo, se desarrollan controles y se supervisa su implementación, se llevan a cabo evaluaciones de riesgos para identificar y abordar vulnerabilidades y se asegura la prestación de los servicios de distribución de electricidad.

Esto implica identificar activos críticos en las infraestructuras de producción y distribución de electricidad, establecer mecanismos de control y seguimiento para prevenir y alertar sobre eventos de seguridad, aplicar mecanismos de control de acceso a estos activos y a los sistemas de control industrial (SCI) y establecer procedimientos de gestión y respuesta a incidentes con planes de recuperación y contingencia. Estos esfuerzos buscan garantizar la continuidad en la prestación de los servicios frente a ataques intencionados, accidentes industriales o desastres naturales.

Las normas NERC CIP abarcan una amplia gama de requisitos relacionados con la gestión de la seguridad, el personal y la formación, los controles de seguridad, la respuesta a incidentes y más. El cumplimiento de estas normas es obligatorio para las entidades responsables de la operación fiable del sistema eléctrico de alta tensión en los EEUU, por ejemplo, y sirven de guía para muchos países de la región.

[23] Nerc, North American Electric Reliability Corporation Critical Infrastructure Protection. Tomado de: https://www.nerc.com/ el 01/17/2024 a las 19:34

## 3.5 Controles del Centro de Seguridad para Internet: Buenas prácticas para asegurar sistemas de IT y datos.

El Centro de seguridad para internet ha desarrollado los Controles de Seguridad Crítica, los cuales constituyen un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas. Estas prácticas, formuladas por expertos en tecnología de la información a partir de datos sobre ataques reales y sus defensas efectivas, pueden ayudar a prevenir ataques peligrosos, respaldar el cumplimiento y proporcionar orientación específica para alcanzar metas y objetivos descritos por marcos jurídicos, reglamentarios y normativos.

Es un conjunto de mejores prácticas para ayudar a las organizaciones a asegurar sus sistemas de tecnología de la información y proteger sus datos. Estos controles, se dividen en 20 acciones prioritarias que cubren desde la prevención de amenazas hasta la detección y respuesta a incidentes de seguridad. Estas prácticas ofrecen un marco sólido para mejorar la postura de seguridad cibernética de una organización, ayudando a mitigar riesgos y fortalecer la protección de sistemas y datos.

## 3.6 COBIT: Marco para la gobernanza y la gestión de las Tecnologías y la Información empresariales.

Este marco de trabajo es un conjunto de mejores prácticas, herramientas y modelos diseñados para la gobernanza y la gestión de la tecnología de la información empresarial. Ayuda a las organizaciones a alinear las actividades de sus redes informáticas con los objetivos comerciales, implementar la gobernanza y el control, garantizando el uso responsable de los recursos de IT.

En la mayoría de las empresas, la gobernanza es responsabilidad de la Junta Directiva, Consejo de Dirección o como se denomine el máximo nivel de autoridad, bajo el liderazgo de un presidente. Por otro lado, la gestión implica planificar, construir, ejecutar y monitorear actividades en línea con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa. En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del director general ejecutivo (CEO). La siguiente figura muestra los factores de diseño

del gobierno de IT que recomienda este marco de trabajo para lograr mejores resultados en el manejo de la tecnología informática:

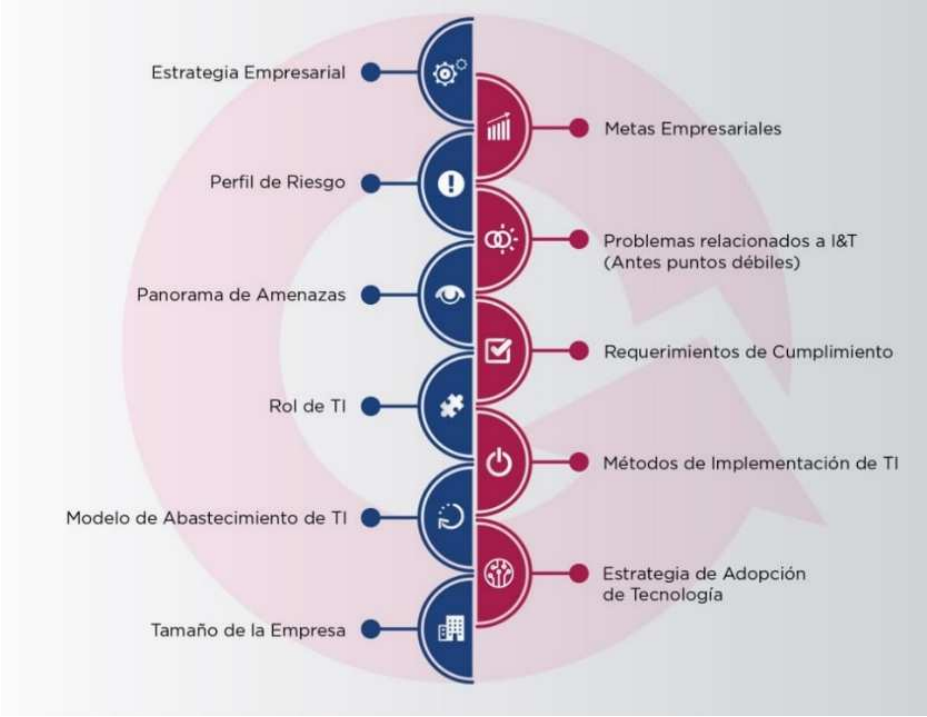


Figura 15. Factores de Diseño del gobierno de TI con COBIT.[24]

En términos de gobernanza, COBIT permite asegurar que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar objetivos empresariales equilibrados y acordados. Además, habilita el establecimiento de una dirección a través de la priorización y la toma de decisiones y el monitoreo del desempeño y del cumplimiento en relación con la dirección y los objetivos acordados.

### 3.7 IEEE 802.1X: Norma para el control de acceso a la red basado en puertos.

El estándar IEEE 802.1X[25] se originó en el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) como parte del grupo de trabajo 802.1, que se enfoca en arquitecturas de redes locales y metropolitanas. El mismo fue desarrollado para

[24] ¿Qué hay de nuevo en cobit 2019? Tomado de: https://www.cynthus.com.mx/que-hay-de-nuevo-en-cobit-2019/ el 01/17/2024 a las 21:11
[25] IEEE 802.1 working group. Tomado de: https://1.ieee802.org/ el 24/01/2024 a las 3:00

proporcionar un mecanismo de autenticación de puertos a nivel de red, con el fin de reforzar la seguridad y controlar el acceso a las redes cableadas e inalámbricas.

El protocolo 802.1X se emplea para asegurar redes a través de la autenticación de acceso a puertos. En el contexto de entornos Wi-Fi, esta forma de autenticación resulta sumamente beneficiosa debido a las características de este medio. Al autenticarse mediante esta, se establece un puerto virtual en el punto de acceso, permitiendo así la comunicación. En caso de una autorización incorrecta, no se generará un puerto virtual disponible, lo que resultará en la interrupción de las comunicaciones.

## 3.8 ISO 27001:2022: Seguridad de la Información, ciberseguridad y protección de la privacidad.

La norma ISO 20071 estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI) dentro del contexto de los riesgos generales de la organización. Esta norma se centra en la protección de la información, incluyendo aspectos como la seguridad en el manejo de datos, la gestión de activos de información y la seguridad en el acceso a la información.

La aplicación de la norma ISO/IEC 27001:2022 en la convergencia IT y OT es de vital importancia por diversas razones. En primer lugar, esta norma proporciona un marco de referencia para establecer y mantener un sistema de gestión de seguridad de la información (SGSI), lo cual permite identificar y gestionar los riesgos asociados con la convergencia IT y OT, protegiendo así la información sensible y los activos de la organización. También, al aplicar esta norma, se pueden establecer controles y medidas de seguridad adecuados para garantizar la integridad, confidencialidad y disponibilidad de los datos compartidos entre los sistemas de información y los sistemas operativos en entornos industriales.

Asimismo, la aplicación de la norma ISO/IEC 27001:2022 facilita el cumplimiento de los requisitos legales y normativos relacionados con la seguridad de la información y la protección de datos, asegurando que la convergencia IT y OT se realice de manera segura y siguiendo las mejores prácticas reconocidas a nivel

internacional. Por último, brinda un enfoque estructurado para identificar, evaluar y tratar los riesgos de seguridad de la información asociados con la convergencia IT y OT, lo cual ayuda a tomar decisiones informadas para mitigar estos riesgos y proteger los activos críticos de la organización.

## 3.9 Aplicación de normativas en la convergencia IT y OT en la industria.

Las diversas normas, mejores prácticas y/o estándares de seguridad establecen un incremento en los niveles de madurez que una organización precisa en términos de seguridad de la información. Resulta además crucial para considerar la convergencia de redes de tecnología de la información y tecnología operativa en el campo industrial. A medida que la madurez de la organización aumenta, aumenta su capacidad para implementar normativas de seguridad de manera efectiva.

En general, es fundamental establecer un marco de seguridad sólido que se amolde a las necesidades de cada organización, con normativas reconocidas, como NIST, IEC 62443, ISA-95 y la serie ISO 27000, entre otras. A medida que la organización avanza en sus niveles de madurez, es importante realizar evaluaciones de riesgos y aplicar controles de seguridad más avanzados, como la segmentación de redes, la detección de intrusiones y la gestión de accesos. Además de considerar el nivel de madurez de la organización, es importante evaluar varios factores al elegir el estándar adecuado para aplicar a la convergencia de estas redes en el campo industrial. Algunos de estos factores incluyen:

- **Requisitos regulatorios:** Identificar las normativas y regulaciones específicas de la industria y el país en el que opera la organización, y asegurarse de que el estándar elegido cumpla con estos requisitos.
- **Interoperabilidad:** Evaluar la capacidad del estándar para facilitar la interoperabilidad entre sistemas de IT y OT, así como su capacidad para integrarse con tecnologías existentes en el entorno industrial.
- **Seguridad:** Considerar la robustez de las medidas de seguridad y protección de datos proporcionadas por el estándar, así como su capacidad para mitigar riesgos de ciberseguridad en un entorno de convergencia de redes.

- **Escalabilidad:** Evaluar si el estándar es escalable y puede adaptarse al crecimiento y la evolución de la infraestructura de IT y OT de la organización a lo largo del tiempo.
- **Mejores prácticas de la industria:** Investigar las mejores prácticas y recomendaciones de la industria en cuanto a estándares para la convergencia de redes, y considerar cómo se alinean con las necesidades y objetivos específicos de la organización.

Al considerar estos factores, la organización estará en una mejor posición para seleccionar el estándar más adecuado al integrar redes de IT y OT en su entorno industrial. Tanto los equipos de ciberseguridad informática como industrial necesitan realizar una evaluación exhaustiva de las soluciones tecnológicas convergentes, identificando riesgos, amenazas y vulnerabilidades asociadas a dichos dispositivos. Esto debe realizarse siguiendo las recomendaciones de normativas reconocidas en el mercado, como las pertenecientes a la serie ISO 27000 para redes informáticas o la IEC62443 para gestión de sistemas de automatización industrial, o marcos de trabajos como el del NIST y Cybook, entre otros.

## CAPITULO 4. Seguridad en la cadena de suministro.

Cuando se habla de transformación digital en entornos operativos, es necesario mencionar la importancia de todos los eslabones que hacen parte de la cadena de suministro. Tanto el hardware como el software y las personas deben ser tenidas en cuenta en todo este proceso que, entre otras cosas, se enfoca en la gestión de riesgos relacionados con proveedores, en la logística y en el transporte externo.

En otras palabras, consiste en identificar, analizar y mitigar los riesgos asociados con colaboradores externos en todo el proceso de la cadena de suministro, abordando tanto la seguridad física como la cibernética. Tal como lo menciona Gartner en uno de sus estudios *"Es importante que los líderes tecnológicos de la cadena de suministro acojan una mentalidad que acepte y adopte el cambio perpetuo a largo plazo".* Las tendencias actuales en la gestión de la cadena de suministro priorizan la protección contra ciberataques, la flexibilidad y adaptabilidad de las cadenas de suministro, la economía circular, los estándares ESG, la transformación digital, y el uso de inteligencia artificial y machine learning para mejorar la productividad y obtener ventajas competitivas. Tal como lo muestra la siguiente figura:


Figura 16. Tendencias tecnológicas de la cadena de suministro 2020.[26]

[26] Gartner Top 8 Supply Chain Technology trends for 2020.

Además, se destaca la emergente gestión de la cadena de suministro 5.0, que se centra en la combinación de la visión humana, la tecnología avanzada y la sostenibilidad. Para una gestión eficiente de la cadena de suministro, es recomendable integrar sistemas e información, invertir en tecnología, enfocarse en la mejora continua, optimizar la gestión de inventario e implementar la gestión de riesgos.

Las vulnerabilidades en la cadena de suministro pueden afectar significativamente las tecnologías operacionales, por ejemplo, si un proveedor de componentes de OT sufre un ciberataque, podría retrasar la entrega de componentes críticos. Esto a su vez puede impactar la producción, la calidad del producto final y la seguridad de las operaciones. Por lo tanto, es crucial gestionar las vulnerabilidades de la cadena de suministro para mitigar el riesgo de interrupciones en las operaciones de tecnología.

A la par de interrupciones en la entrega de componentes críticos, las vulnerabilidades en la cadena de suministro pueden exponer las Operaciones de Tecnología a riesgos de seguridad cibernética, como la inserción de malware en el software de control industrial o la manipulación de dispositivos antes de su entrega. Estas amenazas pueden comprometer la integridad, disponibilidad y confidencialidad de los sistemas en entornos industriales, lo que potencialmente podría resultar en daños operativos, financieros y de reputación para la organización.

Asimismo, los retrasos en la entrega de equipamiento informático y/o piezas de software pueden impactar los proyectos al afectar la implementación, ciertos procesos o la actualización de sistemas críticos. También, la integridad de los datos y la confiabilidad de los sistemas pueden verse comprometidas si los componentes de la cadena de suministro no cumplen con los estándares de calidad y seguridad necesarios.

Por tanto, es crucial gestionar de manera efectiva las vulnerabilidades en la cadena de suministro para proteger las tecnologías informáticas y garantizar la continuidad de las operaciones.

## 4.1 Funcionamiento de la Seguridad en la cadena de suministro.

En este tópico lo que siempre se busca es resguardar la integridad física y proteger toda la cadena contra amenazas cibernéticas. Con respecto a los riesgos físicos se abarcan todas situaciones como robo, sabotaje y terrorismo, los cuales las organizaciones pueden mitigar mediante el seguimiento y verificación de la documentación regulatoria.

Por otro lado, las amenazas cibernéticas han adquirido importancia en la seguridad de la cadena de suministro, exponiendo vulnerabilidades en sistemas informáticos a través de malware, piratería informática y accesos no autorizados. Para enfocarse en la ciberseguridad en todos los niveles, se requiere el uso de software de terceros y una estrecha colaboración entre empresas, proveedores y distribuidores. Cuando se comparten datos confidenciales y las redes se entrelazan, una sola brecha puede afectar a un público mucho más amplio.

En este contexto, la ciberseguridad debe ser una prioridad, ya que las brechas en el sistema pueden causar daños, paradas de planta y/o en el peor de los casos de destrucción de vidas humanas. Las vulnerabilidades en la cadena de suministro pueden ocasionar costos descontrolados, retrasos en la entrega y la pérdida de propiedad intelectual. Además, los productos comprometidos pueden resultar perjudiciales tanto para los clientes como para el negocio, lo que a su vez podría generar litigios inesperados si la cadena de suministro no está protegida. Los sistemas de gestión de la seguridad pueden contribuir a proteger las cadenas de suministro, garantizando una entrega de bienes más segura y eficiente y facilitando una pronta recuperación en caso de interrupciones.

Con respecto al software en la cadena de suministros, se integran prácticas recomendadas de gestión de riesgos y ciberseguridad para resguardarlo de posibles vulnerabilidades. Esta cadena abarca todo lo relacionado con el código a lo largo del ciclo de vida de desarrollo del software (SDLC), desde el diseño de la aplicación hasta los canales de CI/CD a su implementación. Involucra información sobre elementos del software, como la infraestructura, el hardware, los sistemas operativos, los servicios de la nube, etc.; las personas involucradas en su creación; y las fuentes de las que provienen, como registros, repositorios de GitHub, bases de código u otros

proyectos de código abierto. También contempla los posibles puntos vulnerables que podrían afectar la seguridad del software. Es aquí donde entra en juego la protección de la cadena de suministro.

Igualmente, la seguridad de las aplicaciones empieza con el desarrollo del software y abarca todo el ciclo para prevenir el acceso no autorizado a los sistemas y proteger los datos confidenciales. Reforzar la integridad de la cadena de suministro también mejora la seguridad de las aplicaciones. Algunas medidas para evitar que los piratas informáticos pongan en riesgo las aplicaciones incluyen fortalecer las configuraciones, reducir las superficies de ataque, restringir los permisos, firmar el software y distribuir las compilaciones en distintas partes del sistema.

Es válido afirmar que, si algún componente de la cadena de suministro de software está en peligro, es probable que los demás elementos que dependen de él también lo estén. Los piratas informáticos aprovechan estas oportunidades para introducir malware, virus backdoor u otro código malicioso que afecte a los componentes y sus respectivas cadenas de suministro. Los ataques a las cadenas de suministro de software, perpetrados por individuos en busca de lucro o agentes estatales, son cada vez más frecuentes y pueden tener un gran impacto tanto en el ámbito digital como en el físico. Por lo general, se clasifican de la siguiente manera:

- **Puntos vulnerables:** fallas en el código del software que pueden ser explotadas, dando lugar a fugas de datos. En este caso, se deben aplicar parches y actualizaciones en sus componentes para reducir este riesgo.
- **Licencias:** suponen un riesgo legal que podría obligar a convertir cualquier componente de software en código abierto y anular los derechos de patente. Ante esta situación, es conveniente buscar asesoramiento especializado en este ámbito.
- **Dependencias de terceros:** se da cuando los proveedores externos que forman parte de la cadena de suministro de software, su identificación puede ser un proceso complejo. Por lo tanto, es necesario analizar el código de terceros y contactar a sus proveedores para conocer las prácticas de seguridad que aplican.
- **Procesos y políticas:** es fundamental implementarlos en la empresa para prevenir contratiempos. Por lo tanto, se deben establecer políticas para los

desarrolladores y procesos (o guías de actuación) que les permitan responder ante puntos vulnerables.

## 4.2 Mejores prácticas para la seguridad en la cadena de suministro.

### 4.2.1 ISO 28000:2022

La norma ISO 28000:2022 sobre seguridad y resiliencia se centra en la gestión de la seguridad en la cadena de suministro, abordando aspectos como la protección de los activos y la reducción de riesgos. Si bien no se enfoca directamente en la ciberseguridad, su enfoque en la seguridad integral de la cadena de suministro puede contribuir a la prevención de ciberataques al fortalecer los procesos de seguridad física, la gestión de riesgos y la resiliencia de la cadena de suministro. Integrar los principios de esta norma con medidas específicas de ciberseguridad puede fortalecer la protección de la cadena de suministro contra amenazas cibernéticas.

### 4.2.2 BASC

La norma BASC, o Business Alliance for Secure Commerce, se enfoca en la seguridad y la gestión de riesgos en la cadena de suministro, con énfasis en la prevención de actividades ilícitas y el fomento de prácticas comerciales seguras. Aunque no está directamente relacionada con la ciberseguridad, su enfoque en la integridad, seguridad y protección dentro de la cadena de suministro puede complementar los esfuerzos de ciberseguridad al promover una cultura de seguridad integral. Al integrar los principios de la norma BASC con medidas específicas de ciberseguridad, se puede fortalecer aún más la protección de la cadena de suministro contra amenazas, tanto físicas como cibernéticas.

## 4.3 Casos de estudio de Ciberataques en la cadena de suministro.

Los ciberataques a proveedores no son ajenos a la historia reciente de las organizaciones industriales y empresas de tecnología informática. El crecimiento de la superficie de ataque ha convertido a estas entidades en blancos atractivos para

hackers y ciberdelincuentes. En muchos casos, un ataque a un proveedor ha permitido el acceso a plataformas mucho más amplias, afectando no solo a uno de sus clientes, sino incluso a naciones enteras o a los usuarios que utilizan sus productos o servicios. A continuación, se presentarán un par de casos que ilustran cómo, en el contexto de la transformación digital, la afectación de un solo eslabón de la cadena de suministro puede generar daños colaterales incalculables.

### 4.3.1 Caso empresas varias de Automotores en 2018.

En este caso, investigadores de la empresa Upguard[27], la cual se dedica a temas de ciberseguridad, descubrieron que datos altamente confidenciales de gigantes automotrices, como Tesla, Ford, Toyota, GM, Fiat, ThyssenKrupp y Volkswagen, fueron expuestos públicamente en un servidor de Level One Robotics. La brecha fue detectada el 1° de julio de 2018, exponiendo 157 gigabytes de archivos con secretos comerciales, datos bancarios e información confidencial.

Varios expertos aclararon que los datos expuestos abarcan más de 10 años de esquemas de líneas de ensamblaje, planos y diseños de plantas de fábrica, configuraciones y documentación robótica. También se encuentran formularios de solicitud de credenciales de identificación, de privilegios de acceso VPN e irónicamente, acuerdos de confidencialidad que detallan la sensibilidad de la información expuesta. Además, se incluían datos personales de algunos empleados de Level One, como escaneos de licencias de conducir y pasaportes, así como datos comerciales de la empresa, como facturas, contratos y detalles de cuentas bancarias.

Según la publicación del blog, los datos se expusieron a través de Rsync, un protocolo común de transferencia de archivos utilizado para duplicar o respaldar grandes conjuntos de datos, permitiendo la sincronización eficiente de archivos y directorios entre sistemas. Sin embargo, en este caso, la ausencia de restricciones de seguridad en el servidor Rsync, provocó la exposición de datos confidenciales. El servidor no contaba con restricciones por IP o usuario, lo que permitía la descarga del

[27] Exposed: 157 GB of sensitive data from Tesla, GM, Toyota & others. Tomado de: https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies el 08/02/2024 a las 20:55

conjunto de datos por cualquier cliente Rsync que se conectara al puerto correspondiente.

Aunque Level One desconectó los archivos después de ser informado del incidente de seguridad, no está claro si fueron accedidos por terceros no autorizados. La mayoría de estas empresas automotrices afectadas no hicieron público el alcance del ataque. Incidentes como este podrían tener graves repercusiones, ya que la confidencialidad es crucial en la industria automotriz y podría afectar directamente la continuidad operativa de la organización víctima del ataque.

### 4.3.2 Caso IFX Network en Colombia en 2023.

Este caso fue considerado como el primer mega secuestro de datos ocurrido en la historia reciente de Colombia. IFX Network[28] es una empresa destacada en América Latina, especializada en servicios gestionados de TI, con una amplia red de conectividad en la nube público-privada, más de 23 años de experiencia y presencia en más de 17 países de la región. La empresa provee servicios bajo tres líneas de negocios de administración en la nube, que se refiere al desarrollo de estrategias con base en la nube; administración en redes, que ofrece soluciones para la integración de redes sin alterar la continuidad del negocio, y paradójicamente, servicios de administración de soluciones para profesionales de seguridad que protegen la información y la transmisión de datos por internet.

El 12 de septiembre de 2023 el ransomware llamado RansomHouse bloqueó una de las plataformas de gestión de IFX Network[29] y la información de sus clientes, afectando a más de 700 máquinas, incluyendo entidades estatales. Este bloqueo fue posible por la falta de actualización de un VMWare. En Colombia, la compañía suministra sus servicios a entidades como la Rama Judicial, el Ministerio de Salud, la Superintendencia de Industria y Comercio, la Superintendencia de Salud, el Centro

[28] ¿Qué hace la multinacional colombiana IFX Network? Tomado de: https://www.semana.com/empresas/articulo/que-hace-la-empresa-colombiana-ifx-networks/266504/ el 02/08/2024 a las 21:58

[29] Activan protocolo de emergencia en Colombia por ciberataque a proveedor de telecomunicaciones. Tomado de: Ciberataque a IFX Networks activa protocolo de emergencia en Colombia (cnn.com) el 08/02/2024 a las 21:45

Nacional de Memoria Histórica, la Cruz Roja Colombiana y Coljuegos, entre otras. La siguiente figura fue la notificación que la empresa publicó sobre este incidente.


**Septiembre 18 de 2023**

Con el propósito de que el público en general esté correctamente informado sobre el ataque de Ransomware ocurrido, comunicamos lo siguiente:

El pasado 12 de septiembre, en IFX Networks tuvimos una afectación en algunas de nuestras máquinas virtuales a raíz de un ataque de ciberseguridad externo conocido como Ransomware. En cuanto tuvimos conocimiento del incidente, activamos los protocolos de seguridad pertinentes e iniciamos una investigación desde nuestro Centro de Operaciones de Seguridad (SOC).

Entendemos la complejidad de este incidente y el impacto que ha representado para algunos de nuestros clientes y sus ecosistemas. Sin embargo, destacamos que gracias a la detección y actuación de forma oportuna por parte de nuestro equipo, logramos limitar el potencial alcance del ataque y contener considerablemente el número de sistemas afectados.

Adicionalmente, nuestro equipo ha trabajado de forma diligente junto con nuestros expertos internos y externos en ciberseguridad y asesores externos para investigar y responder a este incidente, lo cual nos ha permitido obtener información relevante para avanzar en el proceso de restablecimiento del servicio, con sistemas seguros y en funcionamiento.

En ese sentido, confirmamos que ya hemos comenzado a reestablecer los primeros servicios y continuamos trabajando para que todos los sistemas vuelvan a estar en línea en los próximos días y en consecuencia, la prestación del servicio estará normalizada lo antes posible.

Reiteramos que todas las decisiones y acciones que estamos tomando para enfrentar el ataque recibido las hacemos pensando en nuestros clientes y la seguridad de su información, con el objetivo de cumplir con nuestra promesa de valor como proveedor en telecomunicaciones.

*Para cualquier inquietud, favor remitirse a www.ifxnetworks.com/updates/ en donde estaremos aportando avances e información de interés para nuestras audiencias.*

Figura 17. Notificación de incidente de seguridad IFX Network.[30]

En el evento en particular del Ministerio de Salud bloqueó su plataforma misional del Sistema Integrado de Información de la Protección Social (Sispro) y su aplicativo Mipres, utilizados por médicos para ordenar medicamentos, tratamientos y cirugías, fueron secuestrados. Esto obligó a instituciones como empresas prestadoras de servicios de salud o EPS, hospitales y otras instituciones vinculadas, a recurrir a métodos manuales. Se tuvieron que registrar y documentar nacimientos, defunciones, cirugías, consultas de alta complejidad, citas, tratamientos y terapias de forma manual.

[30] Actualizaciones de estado. Tomado de: https://ifxnetworks.com/updates/ el 09/02/2024 a las 16:44

Aunque los hospitales y demás empresas prestadoras de los servicios de salud, con sistemas activos pueden funcionar, al requerir datos del Ministerio de Salud, su operatoria queda bloqueada. Tan solo entre las entidades estatales, se menciona que la afectación se dio en 46 de ellas; de las cuales 25 tienen servicios de conectividad contratados con IFX Networks, mientras que otras 21 tienen servicios y/o aplicativos en la nube de esa empresa y por ende, son las más comprometidas.

Por su parte, IFX recomendó a sus proveedores y clientes que implementen las siguientes medidas de manera preventiva:

- Forzar un escaneo completo con su antivirus.
- Revisar los logs del sistema operativo.
- Verificar que no exista algún software sospechoso en sus sistemas.
- Chequear las cuentas existentes en su servidor.
- Auditar el rendimiento de procesamiento y discos duros.
- Revisar si existe alguna alteración en la información o fuga de datos.
- Auditar su tráfico de red y conservar un registro actualizado de sus sistemas.

Este caso ilustra directamente cómo logra afectar a una sociedad una vulnerabilidad, por un eslabón en la cadena de suministro y así impactar los servicios neurálgicos de un país, como en el caso del Ministerio de la salud de Colombia. Por tanto, es crucial tomar precauciones e implementar medidas que mitiguen estos riesgos potenciales, los cuales amenazan la disponibilidad, integridad y confidencialidad de los datos de una organización. Asimismo, es fundamental aumentar el nivel de seguridad en todas las empresas, donde convergen no solo tecnologías operativas y de información, sino también proveedores y sistemas de información específicos.

## 4.4 Recomendaciones de Ciberseguridad en la cadena de suministro.

La ciberseguridad en la cadena de suministro es fundamental para proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas que intervienen en el flujo de productos y servicios. Ayuda a prevenir ataques cibernéticos, robo de información, interrupciones operativas y garantiza la confianza entre los distintos

actores de la cadena. Además, contribuye a mantener la calidad, seguridad y fiabilidad de los productos y servicios ofrecidos, fortaleciendo la resiliencia ante posibles amenazas cibernéticas, así como también, la continuidad operativa. Estos atributos son centrales en organizaciones industriales.

Por esta razón, en diciembre de 2018, el Departamento de Seguridad Nacional de Estados Unidos creó el Grupo de Trabajo SCRM, una asociación público-privada para abordar desafíos y desarrollar soluciones que mejoren la resiliencia de la cadena de suministro. Formado por representantes del gobierno federal y de la industria de todos los sectores, este grupo juega un papel crucial en la gestión de riesgos en la cadena de suministro.

También en el marco de este grupo de trabajo SCRM, creó la orden ejecutiva 13873[31], promulgada el 15 de mayo de 2019, la cual busca que se intensifiquen los esfuerzos para prevenir que adversarios extranjeros aprovechen las vulnerabilidades en la cadena de suministro en empresas de origen estadounidense o en su propio suelo. Esto se hace con el fin de proteger la gran cantidad de información confidencial que se maneja a través de dichos productos y servicios. Ese documento es un modelo por seguir para implementar medidas de seguridad para fortalecer todos los elementos que intervienen en la cadena.

Es esencial realizar evaluaciones de riesgos y auditorías de seguridad de manera regular en todos los proveedores y socios comerciales para identificar posibles vulnerabilidades. Además, es necesario establecer estándares de seguridad claros y exigir su cumplimiento en todos los contratos y acuerdos comerciales ayuda a garantizar un nivel consistente de protección en toda la cadena de suministro. Adoptar controles sólidos de acceso, el cifrado de datos, la capacitación en concienciación sobre seguridad para empleados y socios y la monitorización continua de la red, se contribuye a fortalecer la ciberseguridad en la cadena de suministro.

Asimismo, seguir estándares reconocidos internacionalmente, como el de la ISO 27001 para la gestión de la seguridad de la información, y cumplir con regulaciones específicas del sector, brinda un marco sólido para establecer medidas de seguridad efectivas. La IEC 62443, por su parte, proporciona directrices para

[31] ICT Supply Chain Risk Management Task Force. Tomado de: Grupo de Trabajo sobre Gestión de Riesgos de la Cadena de Suministro de TIC | CISA el 03/09/2023 a las 22:30

proteger los sistemas de control y automatización en entornos industriales contra ciberataques, ayudando a mitigar riesgos y fortaleciendo la resiliencia cibernética en el sector industrial. Otra opción disponible es el marco de ciberseguridad que proporciona el NIST, el cual ayuda a identificar, proteger, detectar, responder y recuperarse de amenazas cibernéticas, proporcionando un enfoque integral para la gestión de riesgos de seguridad informática. Estos estándares abordan la seguridad de los dispositivos, redes y sistemas de control industrial, sistemas informáticos y se centra en las personas.

Finalmente, es importante realizar evaluaciones exhaustivas de seguridad cibernética y prácticas de gestión de riesgos de tus proveedores. Esto permitirá evaluar y mitigar posibles vulnerabilidades en la cadena de suministro. Además, es fundamental incluir cláusulas de seguridad cibernética en los contratos con proveedores para establecer expectativas claras en cuanto a la protección de datos y sistemas. De esta manera, se establecen las responsabilidades y requisitos mínimos en términos de acuerdos de seguridad.

## Conclusiones.

En la actualidad, la integración de la tecnología informática y operativa en las empresas industriales ha alcanzado un punto crítico. Tanto la tecnología como el factor humano y de los procesos bien documentados, son fundamentales para garantizar la continuidad del negocio. Esta convergencia en el contexto de la transformación digital ofrece oportunidades significativas para mejorar la eficiencia, visibilidad y la toma de decisiones en estas organizaciones.

En contraste, este proceso plantea desafíos culturales, de conocimientos técnicos, de experiencia en ejecución y como uno de los principales, el de seguridad de la información. Por lo tanto, resulta crucial implementar buenas prácticas de ciberseguridad, especialmente en procesos donde se genera información crítica y/o confidencial, que resulta esencial para el negocio. Para alcanzar este objetivo, es necesario contar con soluciones y servicios que refuercen la disponibilidad, integridad y confidencialidad de los datos, así como la continuidad de las operaciones.

Por ello, al seleccionar dispositivos para entornos industriales que integran redes de IT y OT, es crucial elegir componentes que cumplan con estándares y protocolos de seguridad, y que reciban actualizaciones regulares de firmware para abordar posibles vulnerabilidades. Asimismo, se deben aplicar medidas de seguridad en cada etapa del desarrollo de cada solución, tanto en el software como en el hardware, autenticación multifactor para el acceso a activos que respaldan servicios críticos, el cifrado de datos mediante algoritmos robustos y sin vulnerabilidades conocidas, y la capacidad de entrega de datos para monitoreo continuo, también son aspectos claves para garantizar la seguridad de la infraestructura tecnológica.

Al seleccionar las mejores prácticas, estándares y/o normas para asegurar la convergencia de redes de IT y OT en entornos industriales, es importante considerar la compatibilidad con las tecnologías existentes en la infraestructura de la empresa. Optar por soluciones que se integren sin problemas con los sistemas actuales no solo simplifica la implementación y reduce la interrupción en las operaciones, sino que también es crucial al momento de evaluar la escalabilidad de las soluciones propuestas. Efectivamente, se asegura que la infraestructura de IT y OT puedan expandirse con el tiempo e incorporar nuevos componentes.

Por otro lado, es importante identificar certificaciones reconocidas y estándares de la industria en ciberseguridad, que contribuyan a garantizar la integridad de la infraestructura y sean determinantes para la continuidad operativa. En este sentido, es recomendable adoptar la normativa IEC 62443, debido a que proporciona un marco integral para la ciberseguridad en sistemas de automatización y control industrial. Al ser el estándar más conocido a nivel global, respetado e implementado en el mercado de la tecnología operacional; establece directrices claras y prácticas para proteger las redes, sistemas y equipos en entornos industriales y resulta crucial para mitigar riesgos de ciberataques, ayudando así a identificar y gestionar proactivamente riesgos, implementar controles adecuados y establecer procesos para monitorear y mejorar la seguridad.

Otro marco de trabajo recomendado para implementar en entornos industriales es el del NIST, debido a su capacidad para ofrecer directrices detalladas y prácticas que mejoran la ciberseguridad, lo cual es fundamental para proteger sistemas críticos. Con un enfoque integral, el NIST abarca la identificación, protección, detección, respuesta y recuperación frente a incidentes de ciberseguridad, siendo aplicable en entornos industriales donde la interrupción de operaciones puede tener un impacto significativo.

Por su parte en el rubro de IT, la familia de normas ISO 27000 asiste a las organizaciones en la protección de su información, garantizando su manejo seguro en entornos de redes informáticas corporativas. Estas normas ofrecen un conjunto de controles y procesos que posibilitan la identificación, evaluación y gestión de los riesgos asociados con la seguridad de la información. Con su implementación, se ayuda a establecer controles y procesos para identificar y gestionar los riesgos de seguridad, proteger los activos de información y cumplir con requisitos legales y regulatorios. Además, se demuestra un compromiso con la seguridad de la información, lo que aumenta el grado de confianza de clientes y socios comerciales. En entornos donde convergen redes de IT y de OT, estos estándares favorecen la integración e interacción segura de dispositivos, información y personas.

Para mejorar la ciberseguridad en la cadena de suministro, es crucial establecer una estrecha colaboración con proveedores y socios comerciales, promoviendo la transparencia y el cumplimiento de estándares de seguridad. Esto incluye realizar evaluaciones de riesgos, auditorías de seguridad y la inclusión de

cláusulas contractuales en los contratos, que exijan el cumplimiento de estándares de ciberseguridad. Asimismo, es fundamental supervisar y monitorear dispositivos y sistemas, llevando a cabo revisiones periódicas para detectar y abordar posibles brechas de seguridad de manera proactiva. En consecuencia, se recomienda implementar diversas tecnologías de monitoreo y detección de amenazas en toda la cadena de suministro, así como adoptar soluciones avanzadas de seguridad cibernética.

Del mismo modo, se debe capacitar a empleados y proveedores en buenas prácticas de seguridad cibernética. Es fundamental que todos los socios de la cadena de suministro intercambien información y adopten buenas prácticas en ciberseguridad, estando preparados para actuar rápidamente ante incidentes mediante planes de respuesta coordinados. Asimismo, resulta esencial implementar programas continuos de formación en seguridad y concienciación, y mantener actualizada la documentación de procesos en la planta. Además, se deben realizar actualizaciones periódicas de hardware y software, emplear herramientas de seguridad como firewalls y antivirus, y establecer una segmentación de red adecuada con conexiones controladas entre dispositivos.

En resumen, al combinar esfuerzos de colaboración, coordinación y capacitación, los entornos de IT y OT pueden mejorar significativamente la ciberseguridad de sus plataformas tecnológicas, proteger sus datos y recursos, fortalecer la protección de sus activos críticos y garantizar la necesaria continuidad operativa para seguir generando valor en sus respectivos negocios.

## GLOSARIO

Amenaza: probabilidad latente de que ocurra un hecho de peligro.

Big Data: conjunto de datos masivos en alto volumen.

Confidencialidad: la información solo debe ser accedida por personal autorizado.

Convergencia: lugar donde se genera una unión.

Criptografía: técnicas de cifrado y encriptado de la información para hacerla inteligible a personas no autorizados a la misma.

Disponibilidad: disponer y acceder a la información en el momento que se requiera, desde los lugares destinados para tal fin.

ERP: sistema de planificación de recursos empresariales.

HMI: Interfaz usuario máquina.

ISO 27001: norma para los sistemas de gestión de seguridad de la información en las organizaciones.

ICS: Sistemas de Control Industrial.

Integridad: preservar el contenido de información generada.

IoT: Internet de las cosas.

IT: Tecnología de la Información, buenas prácticas y procedimientos enfocados en el servicio con infraestructura tecnológica para el manejo de los servicios de información, el procesamiento, almacenamiento y transporte de información.

LAN: redes de área local.

MAC: Médium Access Control, se encuentra ubicado en la capa dos del modelo OSI.

OT: Tecnología Operacional, infraestructura de los procesos industrializados, compuesta por elementos componentes lógicos que controlan sensores e integran múltiples plataformas de control a través de protocolos como el SCADA.

PLC: controlador lógico programable.

Riesgo: probabilidad que se materialice una amenaza.

SCADA: software en ordenadores que permite supervisar y controlar procesos

Industriales.

Tecnología: ciencia aplicada a la resolución de problemas concretos.

Seguridad: ausencia del riesgo, estado de tranquilidad.

Vulnerabilidad: debilidad o falló en un sistema de información.

WAN: redes de área amplia.

**Bibliografía.**

[1] Mora Isaza, José Luis. (2023). Ciberseguridad: Ransomware en entornos OT (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1866_PazminoSosaES.pdf

[2] Pérez, Luis. (2018) Semana AADECA ´18 “Evolucionando en la era digital: Las tecnologías del cambio IT-OT”, Recuperado de: https://www.editores-srl.com.ar/sites/default/files/aa9_perez_tecnologias.pdf

[3] Cornwell, Kimberly. (2023) La colaboración entre OT y IT es fundamental para la industria 4.0. Recuperado de https://assets.new.siemens.com/siemens/assets/api/uuid:a6d987f8-115c-43b2-a8ed-d0b0dd9cf591/articulo-it-ot.pdf

[4] Rizzo, Dario Osvaldo. (2020). Marco de referencia de ciberseguridad para infraestructuras críticas. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1603_RizzoDO.pdf

[5] Ministerio del Interior y Seguridad Publica de Chile. Bendel, Matias. Equipo de Respuesta ante Incidentes de Seguridad Informática. IBM. (2021). Ciberamenazas en redes industriales. Recuperado de https://www.csirt.gob.cl/reportes/ciberamenazas-en-redes-industriales-amenazas-ciberneticas-no-28/.

[6] ALCARAZ, Cristian et al. Gestión segura de redes SCADA. Nuevas tendencias en gestión de redes, Novática. En: NICS Lab. Publications, 2008. p. 20-25. Recuperado de https://www.nics.uma.es/pub/papers/Alcaraz2008a.pdf

[7] GUERRERO, Manuel. Necesitamos el entendimiento IT & OT. En: Kaizen, Mejora Continua [blog empresarial], 2018. Recuperado de https://manuelguerrerocano.com/it_ot_convergencia/

[8] USMP, «Administración USMP,» 05 01 2024. [En línea].

[9] USMP, «Administracion USMP,» [En línea]. Available: https://www.administracion.usmp.edu.pe/revista-digital/numero-1/que-es-la-transformacion-digital-en-las-empresas/ [Último acceso: 05 01 2024].

[10] Salesforce, «¿Qué es la Cuarta Revolución Industrial?,» [En línea]. Available: https://www.salesforce.com/mx/blog/cuarta-revolucion-

industrial/?gclid=CjwKCAiA44OtBhAOEiwAj4gpOS_qPstvu_hR6xMlf-Pzl7AFmEyCivdsdzGfR7RC9-M7v-lTuryMWRoCZFcQAvD_BwE&d=7013y000002EkCcAAK&nc=7013y000002EkKgAAK&utm_source=google&utm_medium=paid_search&utm_camp. [Último acceso: 20 12 2023].

[11] Makaia, «La ciberseguridad como uno de los desafios más importantes en la transformación digital.,» [En línea]. Available: https://makaia.org/ciberseguridad-en-la-transformacion-digital/. [Último acceso: 2023 12 12].

[12] U. d. Linkedin, «Principales desafíos de la transformación digital y el papel crucial de la gestión del cambio para superarlos.,» [En línea]. Available: https://www.linkedin.com/pulse/principales-desaf%C3%ADos-de-la-transformaci%C3%B3n-digital-y-el-papel-crucial/?originalSubdomain=es. [Último acceso: 06 01 2024].

[13] M. Stanley, «A report by Morgan Stanley cites Cybersecurity as the single biggest challenge to IIoT adoption. » 2020.

[14] D. Garrido, «¿Qué es la convergencia IT/OT?,» [En línea]. Available: https://www.linkedin.com/pulse/qu%C3%A9-es-la-convergencia-itot-daniel-garrido/?originalSubdomain=es. [Último acceso: 13 12 2023].

[15] Mheducation, «Introducción a los sistemas digitales.,» [En línea]. Available: https://www.mheducation.es/bcv/guide/capitulo/844817156X.pdf. [Último acceso: 11 01 2024].

[16] DynSolutions, «Surgimiento de los sistemas de información y gestión empresarial.,» [En línea]. Available: https://dyncsolutions.com/general/evolucion-de-los-sistemas-de-gestion-empresarial-erp/#:~:text=Origen%20de%20los%20sistemas%20de,materiales%20que%20demandaba%20el%20ej%C3%A9rcito. [Último acceso: 11 01 2024].

[17] NVTecnologias, «¿Qué es SCADA?,» [En línea]. Available: https://www.nvtecnologias.com/blog/blog-1/que-es-scada-10. [Último acceso: 01 11 2024].

[18] C. d. C. I. -. C. España, «Guía de bolsillo: Ciberseguridad en la Pirámide de Automatización Industrial.,» CCI, 2023.

[19] S. Electric, «CXM Tofino Firewall Inspeccion E/IP,» de CXM Tofino Firewall Inspeccion E/IP, Paris, 2023.

[20] INCIBE, «Soluciones IDS en entornos industriales.,» [En línea]. Available: Tomado de: https://www.incibe.es/incibe-cert/blog/soluciones-ids-en-entornos-industriales. [Último acceso: 16 01 2024].

[21] Lab Wallarm, «XDR vs SIEM,» [En línea]. Available: https://lab.wallarm.com/what/xdr-vs-siem-unveiling-the-next-generation-of-threat-detection-and-response/. [Último acceso: 16 01 2024].

[22] Claroty, «Secure Remote Access by Claroty.,» [En línea]. Available: https://claroty.com/ndustrial-cybersecurity/sra. [Último acceso: 02 01 2024].

[23] Siemens, «Sistema RFID de control de acceso de Siemens.,» [En línea]. Available: https://www.digitalsecuritymagazine.com/2017/02/09/siemens-simplifica-el-control-de-acceso-en-entornos-industriales-con-un-sistema-rfid/. [Último acceso: 16 01 2024].

[24] «Guía de protocolos de conectividad industrial.,» [En línea]. Available: https://www.arrow.com/es-mx/research-and-events/articles/industrial-connectivity-protocols. [Último acceso: 17 01 2024].

[25] Scheneider Electric, «EcoStruxure™ Power SCADA Operation.,» [En línea]. Available: https://www.se.com/mx/es/product-range/63067-ecostruxure-power-scada-operation/. [Último acceso: 17 01 2024].

[26] CEIINC, «¿Qué es un SCADA?,» [En línea]. Available: https://ceiinc.co/que-es-un-scada/. [Último acceso: 17 01 2024].

[27] Manage Engine, «5 hechos fundamentales que debe conocer acerca de la gestión de identidades y acceso.,» [En línea]. Available: https://blogs.manageengine.co.m/espanol/2017/12/03/cinco-aspectos-sobre-control-de-acceso-identidades-iam.html. [Último acceso: 17 01 2024].

[28] Siemens, «ISA 95 y Gestión de Operaciones de Fabricación.,» [En línea]. Available: https://www.plm.automation.siemens.com/global/en/our-story/glossary/isa-95-framework-and-layers/53244. [Último acceso: 17 01 2024]