Universidad de Buenos Aires

Facultad de Ciencias Económicas,
Facultad de Ciencias Exactas y Naturales,
Facultad de Ingeniería.

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Trabajo Final de Especialización

Carrera de Especialización en Seguridad Informática

Ciberseguridad en redes industriales identificadas como infraestructuras críticas.

Autor: Gabriel Martín Madariaga
Tutor/a: Mg. Patricia Prandini
Cohorte 2021
Argentina, 2023

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y 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

Gabriel Martín Madariaga

D.N.I.: 23.732.213

INDICE

ÍNDICE DE FIGURAS

RESUMEN

Los sistemas de control y automatización industrial (ICS o IACS, por sus iniciales en español) desempeñan un papel crucial en la gestión de procesos industriales en entornos productivos complejos, como ser fábricas, yacimientos, refinerías, plantas de energía, etc. Estos sistemas son soportados por redes denominadas tecnologías operativas (OT), las cuales se basan en paradigmas diferentes respecto de las tecnologías de Información (IT).

No hace mucho tiempo atrás, las tecnologías industriales se encontraban en redes totalmente aisladas, sin conexión al exterior, internet, proveedores e incluso a las mismas redes corporativas LAN de la empresa. Estas redes se consideraban “cajas negras”

La situación descripta generaba en los responsables de la operación, una falsa sensación de seguridad absoluta. Por tal motivo en muchos sistemas de control industrial no existe el concepto de ciberseguridad industrial.

Hoy en día, estas redes requieren vincularse con diferentes sistemas, tanto internos como externos de la organización. La integración con sistemas propios, con proveedores, el control y el manejo descentralizado, entre otros, hacen que sea necesario abrir las fronteras que antes delimitaban los accesos. Por consiguiente, las superficies de ataque de las redes industriales se han extendido enormemente, aumentando las probabilidades de ocurrencia de un incidente de ciberseguridad.

La pandemia COVID-19 (2021-2022) aceleró el proceso evolutivo de interacción y convergencia entre las redes IT y OT. Las empresas tuvieron que abrir controles y llevar parte de su operatoria y control a los hogares de sus empleados y proveedores. Esta situación generó una gran preocupación en las empresas y un gran desafío para los responsables de la seguridad.

Adicionalmente, la magnitud de los ciber ataques fue evolucionando, aumentando la complejidad y sofisticación, como así también sus consecuencias.

Los ciberdelincuentes encontraron en las redes industriales nuevas oportunidades, desafíos y motivaciones, hecho que queda demostrado por la gran cantidad de incidentes de ciberseguridad ocurridos en los últimos años. Actualmente nos encontramos frente a organizaciones delictivas organizadas, con fines económicos y/o políticos.

Las consecuencias no se limitan únicamente a pérdidas de la confidencialidad, integridad y disponibilidad de los datos, sino van más allá, como la posibilidad de poner en riesgo vidas humanas y causar daños ambientales significativos. Existe además el potencial de que un incidente se extienda fuera de los límites de la organización afectando gravemente a las infraestructuras nacionales o transfronterizas, generando consecuencias de magnitud mucho mayor.

OBJETIVO Y ALCANCE

En este trabajo se abordará el tema de infraestructuras críticas basadas en redes operativas de industrias energéticas (petróleo y gas). Se recopilará información, se definirán los conceptos y clasificaciones principales y se investigarán y presentarán los principales componentes de las redes industriales en infraestructuras críticas.

Se realizará un relevamiento sobre la regulación y las normativas nacionales en la República Argentina aplicables a este tipo de industria.

Se recopilarán incidentes de ciberseguridad que hayan afectado a infraestructuras críticas y sistemas de control industrial.

Desde el punto de vista de ciberseguridad, se estudiarán diferentes normativas y recomendaciones, profundizando en la norma ISA/IEC 62443, sus objetivos, conceptos y estructura. Se identificarán los desafíos en el desarrollo de un programa de ciberseguridad industrial y se definirán las

principales vulnerabilidades que sufren las infraestructuras críticas que se analizan en este trabajo.

En base a la problemática descripta, se realizará un estudio de las infraestructuras críticas en redes OT del sector de la energía, considerando como punto de partida para poder abordar esta problemática el estudio de la norma ISA/IEC 62443.

CAPÍTULO 1 Sistema de control y automatización industrial

Introducción

Un sistema de control y automatización industrial (IACS/ICS) es un conjunto de componentes de hardware y software que se utilizan para controlar y supervisar la ejecución automática y controlada de procesos en entornos industriales. Se los utiliza en plantas de fabricación y procesamiento, servicios públicos (electricidad, gas, agua), tuberías de extracción y distribución de petróleo, etc.

Un ICS permite controlar y ajustar en tiempo real variables tales como: temperatura, presión, caudal, nivel, etc., para procurar que los procesos industriales se mantengan dentro de los límites establecidos.

Diferencia entre redes IT y OT

En la actualidad, la interacción entre las áreas de ciberseguridad de tecnologías de la información (IT) y las áreas de ingeniería y operaciones de redes industriales de una organización es limitada. Sin embargo, es notable la tendencia creciente hacia una mayor integración y colaboración entre ambas áreas.

Para mayor detalle, puede observarse un bajo nivel de conciencia en materia de ciberseguridad por parte de los responsables de las redes industriales, al mismo tiempo que existe un desconocimiento técnico del personal de IT respecto a la protección de sistemas industriales.

En el mundo IT, el riesgo implica amenazas respecto a la tríada de seguridad de la información (CIA), es decir su confidencialidad, integridad y disponibilidad. En los sistemas de control industrial, el riesgo también implica amenazas a bienes y personas, impactos en la economía de la región, impactos ambientales y cortes de servicios esenciales entre otros. Sin embargo, a diferencia de los sistemas de IT, en los sistemas industriales se

prioriza la disponibilidad y continuidad sobre los otros dos factores. Los sistemas industriales en muchos cosos deben funcionar interrumpidamente (7 x 24), las paradas de plantas deben estar debidamente programadas y notificadas. Además, en estas redes existe un principio que se encuentra por encima de cualquier otro, que es preservar las vidas de las personas (en inglés, "*Safety*").

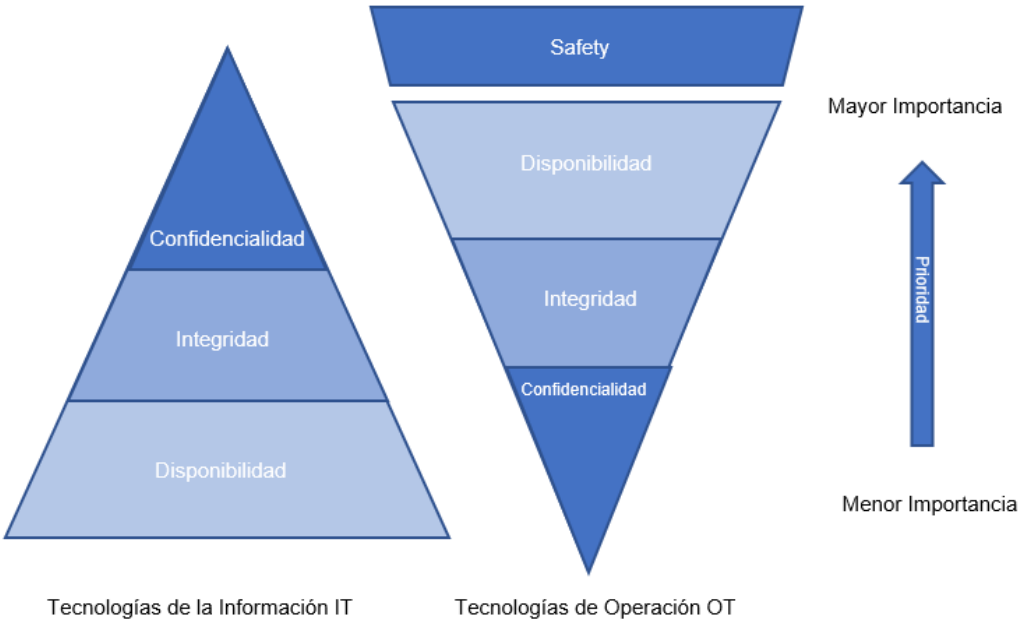

Figura 1 - Diferencias de prioridades de ciberseguridad IT y OT [1]

Debemos tener en cuenta que un incidente de ciberseguridad en las redes OT podría tener un impacto mucho mayor que un incidente de seguridad en un entorno tradicional de IT, más aún si consideramos los servicios críticos esenciales para la vida cotidiana, tales como la energía eléctrica, agua, petróleo, alimentos, salud, etc.

A continuación, se presenta una tabla que resume algunas diferencias principales entre sistemas IT y OT. [1]

Categoría	IT	OT
Procesamiento	No son en tiempo real.	Tiempo real.
Respuesta	La respuesta debe ser confiable y consistente. Se exige alto rendimiento. Pueden ser aceptados retrasos y fluctuaciones elevadas. La interacción de emergencia es menos critica. Se puede implementar un control de acceso estrictamente restringido.	La respuesta critica en cuanto al tiempo. No se aceptan retrasos ni fluctuaciones elevadas. La respuesta a la interacción humana y de emergencia es crítica. El acceso a OT debe estar estrictamente controlado, pero no debe obstaculizar ni interferir con la interacción hombre-máquina.
Disponibilidad	Los reinicios de sistemas son considerados aceptables. A menudo se pueden tolerar fallas o deficiencias de disponibilidad, según los requisitos operativos del sistema.	Los reinicios de sistemas pueden no ser aceptable debido a los requisitos de disponibilidad del proceso. Los requisitos de disponibilidad pueden requerir sistemas redundantes. Las interrupciones deben planificarse y programarse con días/semanas de anticipación. La alta disponibilidad requiere pruebas previas a la implementación exhaustivas.
Administración de riesgos	Administrar datos. La confidencialidad e integridad de los datos es primordial. La tolerancia a fallas es menos importante: el tiempo de inactividad momentáneo no es un riesgo importante. El principal impacto del riesgo es el retraso de las operaciones comerciales.	Controlar el mundo físico. La seguridad humana es primordial, seguida de la protección del proceso. La tolerancia a fallas es esencial; incluso el tiempo de inactividad momentáneo puede no ser aceptable. Los principales impactos de riesgo son el incumplimiento normativo, los impactos ambientales, la pérdida de vidas, equipos o producción.
Sistema operación	Los sistemas están diseñados para usarse con sistemas operativos típicos. Las actualizaciones son sencillas con la disponibilidad de herramientas de implementación automatizadas.	Los sistemas a menudo usan sistemas operativos diferentes y en algunos casos propietarios, a veces sin capacidades de seguridad integradas. Los cambios de software deben ser realizados con cuidado, generalmente por los proveedores de software.
Recursos	Los sistemas se especifican con suficientes recursos para admitir la adición de aplicaciones de terceros, como soluciones de seguridad.	Los sistemas están diseñados para admitir el proceso industrial previsto y es posible que no tengan suficiente memoria y recursos informáticos para admitir la adición de capacidades de seguridad.

Comunicaciones	Se utilizan protocolos de comunicaciones estándar. Principalmente redes cableadas con algunas capacidades inalámbricas localizadas. Prácticas típicas de redes de TI	Se utilizan protocolos de comunicación propietarios y también estándar. Se utilizan varios tipos de medios de comunicación, incluidos los dedicados alámbricos e inalámbricos (radio y satélite). Las redes son complejas.
Administración de cambios	Los cambios de software se aplican de manera oportuna en presencia de una buena política y procedimientos de seguridad. Los procedimientos suelen estar automatizados.	Los cambios de software deben probarse exhaustivamente e implementarse de forma incremental en todo el sistema para garantizar que se mantenga la integridad del sistema de control. Las interrupciones del ICS a menudo deben planificarse y programarse con días/semanas de anticipación. ICS puede usar sistemas operativos que ya no son compatibles
Soporte	Permitir estilos de soporte diversificados en cuanto a quien los provee.	El soporte de servicio suele ser a través de un solo proveedor.
Ciclo de vida	Vida útil del orden de 3 a 5 años.	Vida útil del orden de 10 a 15 años.
Ubicación de componentes	Los componentes suelen ser locales y de fácil acceso.	Los componentes pueden estar aislados, remotos y requieren un gran esfuerzo físico para acceder a ellos.

Figura 2 - Resumen diferencias IT / OT

(traducido por el autor)

Sistemas "*Safety*" en OT

En inglés existe una clara diferenciación entre los términos *"Security"* y "*Safety*", siendo que el primero aplica a la seguridad ante actos de naturaleza intencionada (robos, intrusiones) y el segundo suele aplicarse a la protección contra riesgos fortuitos (accidentes, desastres naturales, daños ambientales, etc.). Sin embargo, en español empleamos únicamente la palabra "seguridad", lo cual puede generar confusión. Por este motivo en el presente trabajo, se utilizará la palabra "*Safety*" para referirnos a la seguridad de personas e instalaciones.

Un sistema "*Safety*" se refiere a los componentes y medidas destinados a prevenir, detectar y responder a eventos que podrían causar situaciones peligrosas o a la pérdida de control sobre un proceso o instalación industrial. Son responsables de mantener bajo condiciones

seguras las instalaciones y personas en caso de producirse alguna anomalía o mal funcionamiento.

CAPÍTULO 2 Infraestructuras críticas

Definición

El Instituto Nacional de Estándares y Tecnología de los EE. UU. (NIST) y la Ley Patriótica (Patriot Act) de 2001 define a las infraestructuras críticas como: *“Sistemas y activos, ya sean físicos o virtuales, tan vitales para los EE. UU. que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de esos asuntos”* [1] [2]

En la República Argentina, de acuerdo con la Resolución N° 1523/2019 (anexo I) de la ex Secretaría de Gobierno de Modernización, aprobada en de septiembre de 2019, se define a las Infraestructuras críticas como:

“… aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.” [3]

Por otro lado, la resolución, establece que:

“Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.”

Identificación de Infraestructuras críticas

De acuerdo con la mencionada normativa nacional, se establecen las siguientes categorías para identificar una infraestructura como crítica:

- Impacto en la vida humana: Cuando la afectación de un sistema informático genere riesgos de vida o amenazas a la salud e integridad física de las personas.
- Impacto económico: Cuando la afectación de un sistema informático genere daños o amenazas graves a la estructura productiva y/o financiera del país.
- Impacto de medio ambiente: Cuando la afectación de un sistema informático afecte negativamente o dañe el espacio donde se desarrolla la vida de seres humanos.
- Derechos y libertades individuales: Existe impacto en ejercicio de derechos humanos o de las libertades individuales en aquellos casos en que, mediante cualquier acción desarrollada mediante un sistema informático, se restrinja o coarte indebidamente de manera colectiva, el pleno ejercicio de los derechos consagrados en los Tratados Internacionales, la Constitución Nacional o las leyes.
- Impacto público o social: Cuando la afectación de un sistema informático se produzcan acontecimientos susceptibles de provocar una grave conmoción en una parte significativa de la población.
- Impacto en el ejercicio de las funciones del estado: Cuando la afectación de un sistema informático afecte de manera sustancial el normal desempeño de los órganos de los poderes Ejecutivo, Legislativo o Judicial.
- Impacto en la soberanía Nacional: Cuando la afectación de un sistema informático se cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio de nacional.
- Impacto en la integridad territorial Nacional: Cando mediante la afectación de un sistema informático, se vulneren las fronteras territoriales, marítimas o espaciales de la nación.

Sectores identificados

La ENISA, en el libro verde sobre un programa europeo para la protección de infraestructuras críticas, describe una lista orientativa de once sectores: [4]

1. Energía
2. Tecnologías de la información y la comunicación (TIC)
3. Agua
4. Alimentos
5. Salud
6. Financiero
7. Orden público y seguridad
8. Administración Civil
9. Transporte
10. Industrias químicas y nucleares
11. Espacio

Esta lista no se utiliza como tal en todos los Estados miembros, algunos países han establecido su propia lista de sectores críticos.

De acuerdo con la Resolución argentina antes citada, en nuestro país se identificaron once sectores en los que se agrupan las infraestructuras críticas:

1. Energía
2. Tecnologías de información y comunicaciones
3. Transportes
4. Hídrico
5. Salud
6. Alimentación
7. Finanzas
8. Nuclear
9. Químico
10. Espacio

11. Estado

La norma ISA/IEC 62443 identifica las siguientes industrias de infraestructura crítica:

- Transmisión y distribución de electricidad
- Redes de distribución de gas y agua
- Operaciones de producción de petróleo y gas
- Tuberías de transmisión de gas y líquidos

A partir de la información relevada se confeccionó una tabla con los sectores identificados como críticos comparando algunos países, incluyendo el nuestro.

Sector / País	Argentina	EEUU	España	Reino Unido
Energía	X	X	X	X
Tecnologías de la Información y comunicación	X	X	X	X
Agua	X	X	X	X
Alimentos	X	X	X	X
Salud	X	X	X	X
Financiero	X	X	X	X
Orden Público/Seguridad	X	X		
Administración Civil		X	X	X
Transporte	X	X	X	X
Químicas	X	X	X	
Nuclear	X	X	X	
Espacio	X		X	
Otros	X	Comerciales Manufactura Represas Defensa Emergencias	X	

Figura 3 - Tabla de sectores críticos por país (autoría propia)

Cada rubro o industria presenta características únicas que requieren una evaluación especifica de medidas de seguridad. En este trabajo nos centraremos en las infraestructuras críticas del sector de energía, petróleo y gas (Oil & Gas). En el proceso intervienen varios subprocesos industriales, que incluyen extracción, separación, transformación, transporte, etc. y una diversificación de componentes extendidos en zonas geográficas extensas y desfavorables (sensores, actuadores, PLC, HMI, RTU, etc.).

Cualquier ciberataque o falla significativa en estas industrias podría tener un impacto importante, principalmente en la vida de las personas, el medio ambiente, la economía del país y la región, etc.

“En la industria de petróleo y gas, la seguridad es lo primero y no hay negociación posible al respecto. La tecnología moderna desempeña un papel importante en la supervisión y protección de estas instalaciones. Concretamente, la industria confía en las redundancias múltiples y la alimentación continua para garantizar que todos los componentes de los sistemas —cada sensor, cada válvula y cada PLC— estén funcionando en todo momento, incluso en una situación de apagado de emergencia.” [5]

Situación de América Latina [6]

A continuación, se detallan las iniciativas que están llevando a cabo algunos países de la región:

- **Argentina**: En 2019 aprueba su Estrategia Nacional de Ciberseguridad mediante Resolución N° 829 de la ex Secretaría de Gobierno de Modernización, y ese mismo año, la Resolución N° 1523, también de la ex Secretaría de Modernización del Estado, en la que como se mencionó, se definen y se enumeran los sectores considerados como infraestructuras críticas de información.

En el año 2021 se crea un centro de respuesta a incidentes informáticos, llamado (CERT.AR) Disposición 01/2021 de la Dirección Nacional de Ciberseguridad, que tiene entre sus objetivos la gestión de incidentes de seguridad informática que puedan afectar a las entidades del sector público y a las infraestructuras criticas nacionales definidas como tales.

Recientemente por Resolución N° 44/2023 de la Secretaría de Innovación Pública de Jefatura de Gabinete de Ministros, se aprueba la segunda versión de la Estrategia Nacional, dejando sin efecto la anterior.

- **Chile:** Presenta su Estrategia Nacional de Seguridad con objetivos definidos en el año 2022. Entre las acciones propuestas, se encuentran la de fortalecer un CSIRT e infraestructuras críticas.
- **Paraguay:** En 2017 aprueba su plan nacional de ciberseguridad que incluye ejes de acción para la protección de infraestructuras críticas y respuestas a incidentes. Tiene un CSIRT nacional.
- **Uruguay:** Según el reporte de ciberseguridad 2020 del BID y OEA, Uruguay ocupa el primer lugar en América Latina en materia de ciberseguridad. Tiene un CSIRT nacional y un centro de operaciones (SOC) que funciona 24 x 7.

También el gobierno de ese país publicó el Marco de Ciberseguridad para infraestructuras críticas (2020), que constituye un documento de referencia para mejorar la ciberseguridad en las infraestructuras críticas del país.

,

CAPÍTULO 3 Componentes de las redes industriales

Un sistema de control industrial involucra en su definición al conjunto de componentes (hardware y software) que trabajan en colaboración para monitorear y controlar las instalaciones en un entorno industrial.

Un ICS se divide en diferentes partes, según se encuentren en una red de producción o de supervisión. Estas partes se pueden clasificar de la siguiente manera:

Red de producción:

- Sensores
- Actuadores
- PLC
- RTU

Red de supervisión:

- SCADA
- DATA HISTORIAN

Sensores

Se trata de dispositivos capaces de realizar mediciones de variables del mundo real (físico o químicas) y transformarlas en señales eléctricas. Ejemplos: temperatura, presión, niveles de líquidos, humedad, radiación, etc.

Actuadores

Tienen la capacidad de modificar elementos del mundo físico en base a mediciones realizadas por los sensores. Ejemplos: abrir/cerrar válvulas, prender/apagar motores, etc.

PLC (Programmable Logic Controller)

Es un dispositivo lógico programable utilizado para automatizar las operaciones en un entorno industrial. Los PLC están diseñados para recibir

información de los sensores, ejecutar el programa lógico predefinido y enviar múltiples señales a los actuadores. Permiten generar acciones de salida para determinadas condiciones de entrada, ejemplos: pueden accionar motores, bombas, válvulas, etc. Constituyen el remplazo de los relés eléctricos.

Los PLC poseen un sistema operativo (SO) en tiempo real integrado, llamado firmware. Ejemplos de SO de PLC son: Microware OS-0, VxWorks, etc.

Figura 4 - PLC – https://www.rockwellautomation.com/

RTU (Remote Unit Terminal)

Es un dispositivo de campo que se conecta a sensores y convierte sus señales en datos digitales que pueden ser transmitidos a una unidad terminal de nivel superior (PLC o SCADA)

Figura 5 - imagen de un RTU – https://www.se.com/

SCADA (Supervisory Control and Data Acquisition)

Un sistema, es decir un software, que posee la funcionalidad de recolectar datos y presentarlos para controlar remotamente una instalación industrial. Pueden integrar datos recogidos desde distintos sensores, equipos y PLCs desde un lugar centralizado.

Pueden generar reportes y cálculos para la toma de decisiones y aumentar la eficiencia y seguridad. Además, pueden almacenar datos en tiempo real o históricos y ser utilizados por un operador humano o por otras aplicaciones.

Data Historian

Es una Base de Datos centralizada que permite registrar información histórica del proceso dentro de un entorno ICS. Los datos recopilados se utilizan para análisis de procesos, control estadístico y planificación.

HMI (Human Machine Interface)

Es una interfaz gráfica de usuario que permite la interacción entre el operador humano y el hardware. Permite configurar parámetros y puede mostrar información de estado y datos recopilados.

Protocolos de comunicación en un ICS

Existen varios protocolos de comunicación utilizados para garantizar la comunicación entre componentes en un entorno ICS. Algunos están diseñados para fines específicos como, por ejemplo, permitir la interoperabilidad entre diferentes fabricantes.

Ejemplos de estos protocolos: PROFUBUS, DNP3, MODBUS, OPC, CIP y Siemens S7.

Algunos de los protocolos se han adaptado para operar sobre redes Ethernet - TPC/IP. Esto permite que los datos del ICS se transmitan a través de una red LAN/WAN. Ejemplos de este tipo de protocolos son Modbus sobre TCP/IP y DNP3.

CAPÍTULO 4 Vulnerabilidades, Amenazas y Ataques

Definición

Según definición del NIST, una vulnerabilidad es una debilidad en un sistema de información, en los controles internos o implementación, que podría ser explotada o provocada por una fuente de amenaza. Las vulnerabilidades pueden ser:

- Públicas: vulnerabilidades conocidas y publicadas.
- Privadas: vulnerabilidades propias de una instalación en particular.
- De Día Zero: vulnerabilidades existentes, pero no conocidas ni publicadas.

En cambio, una amenaza es un evento con potencial de afectar negativamente las operaciones y activos de una organización, a través del acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio. Una amenaza es la posibilidad de que un sistema vulnerable sea afectado y sufra daños. Las amenazas pueden ser accidentales o intencionales. También se pueden clasificar según el agente de amenazas según su origen, que puede ser natural, técnico o humano.

Los ataques son el mecanismo por el que un agente de amenaza explota una vulnerabilidad para causar un impacto que afecte negativamente a un sistema.

A continuación, se detallan algunas de las principales fuentes de amenazas que pueden afectar a un ICS.:

- **Estados extranjeros:** Pueden ser entidades gubernamentales en sí mismas o grupos patrocinados por estos. Utilizan herramientas cibernéticas para realizar espionaje, generalmente para sustraer información estratégica o incluso, atacar a las infraestructuras críticas de un país enemigo.

- **Hacktivistas:** Generalmente motivados para desarrollar operaciones de protesta, su principal objetivo es llamar la atención de los medios y la población. Habitualmente, no persiguen ganancias económicas. Suelen realizar modificaciones de páginas web, divulgación de información confidencial, ataques de denegación de servicio, etc.
- **Ciberdelincuentes:** Los ciberdelincuentes buscan obtener ganancias económicas o afectar gravemente a un objetivo. En muchas oportunidades, son grupos organizados. Es uno de los agentes de amenaza más activos actualmente.
- **Terroristas:** Buscan impactar en infraestructuras críticas para debilitar y amenazar a sus objetivos, sembrando el terror en una determinada población o grupo.
- **Personal interno:** Se consideran empleados o proveedores. Puede ser causado por acciones intencionales o no. En el primer caso, se trata de personal disconforme y/o infiel. En el caso de acciones intencionales, puede ser causado por personal poco entrenado que pueden cometer errores involuntarios.
- **Cadenas de suministro:** Los atacantes utilizan a algún proveedor de confianza como origen para luego a través de técnicas de desplazamiento llegar al objetivo perseguido.

Ataques a sistemas de control industrial

En los ataques a las redes industriales, se utilizan técnicas muy parecida a los ataques en redes IT. Comienzan con el reconocimiento, la identificación de vulnerabilidades y su explotación para poder ingresar a los sistemas y luego usando diferentes técnicas, escalar privilegios y realizar desplazamientos laterales a toda la infraestructura. La mayoría de los ataques a redes industriales, los ciberdelincuentes comienzan en las redes IT y luego se propagan a las redes industriales.

Tipos de ciber ataques

A continuación, se enumeran algunos tipos de ciberataques que pueden afectar a un sistema OT. [7]

- **Suplantación de identidad:** Robo de usuario y contraseña de correo electrónico, accesos remotos ilegítimos, VPN no autorizadas, etc.
- **Malware:** Software malicioso (virus, troyanos, etc.), generalmente presente en archivos adjuntos o link de correo electrónico, en unidades extraíbles (USB) o tras consultar ciertas páginas web.
- **Denegación de servicio (DOS):** Ataques a sistemas para anular su disponibilidad, impidiendo a los usuarios legítimos acceder a la información o servicios y paralizando procesos.
- **Redes de bots:** El uso de estas redes permite a los cibercriminales acceder a sistemas de terceros que luego pueden usar para sus propios intereses delictivos, como cometer fraudes coordinados, distribuir phishing, denegar servicios, etc.
- **Ransomware:** Software malicioso que impide al usuario acceder al sistema y a los datos propios, ya que estos son encriptados hasta que el afectado pague un rescate. Algunos ataques logran dejar equipos inutilizados, comprometiendo el sistema operativo y la BIOS. Por lo general, se originan en ataques de phishing que ingresan a la red corporativa (IT) y luego por diferentes técnicas logran acceder a las redes OT. En algunos casos, existe una doble extorsión por parte de los delincuentes, que solicitan un pago para no divulgar la información robada, afectando a la confidencialidad. Estos ataques resultan muy sofisticados y las organizaciones de ciberdelincuentes son cada vez más grandes y profesionales. Además de la denegación del servicio a partir de los ataques,

las compañías suelen desconectar y apagar los sistemas y comunicaciones como método de contención, generando un escenario aún más problemático.

- **Phishing:** Técnicas que tienen como objetivo engañar a una víctima, ganándose su confianza al hacerse pasar por una entidad/persona de confianza. Por lo general, se utilizan correos electrónicos falsos o no deseados que pueden contener software malicioso o técnicas de ingeniería social que buscan engañar a la víctima y lograr que realice una acción que normalmente no realizaría.
- **Amenaza persistente avanzada (APT por sus siglas en inglés, Advanced Persistent Threat):** Consiste en el ataque de objetivos minuciosamente seleccionados y focalizados. Por lo general tienen un objetivo económico o político. Se integran sigilosamente en los sistemas durante largos periodos de tiempo para luego activarse y lograr el objetivo buscado.
- **Vectores de ataque en un contexto de criptografía:** Ataques de canal lateral basados en informaciones secundarias (como señales de energía, magnéticas, sonidos, etc.) obtenidas durante la implementación física de un criptosistema.

Vulnerabilidades en las infraestructuras críticas industriales

Una red industrial se encuentra expuesta a un sinnúmero de amenazas que pueden explotar distintas vulnerabilidades. A continuación, se listan algunas de ellas:

- **Gobierno de ciberseguridad:** No existe un responsable de ciberseguridad industrial, no están definidos roles, funciones y responsabilidades del personal involucrado en el proceso.
- **Actualización de software y parches de seguridad:** El proceso de implementación de parches de seguridad en aplicaciones y sistemas industriales es complejo, los sistemas operativos

industriales suelen ser obsoletos y encontrarse, por lo tanto, sin soporte. En muchos casos no pueden reiniciarse y no existen entornos de prueba. Los parches requieren la aprobación de los fabricantes de los sistemas.

- **Políticas de contraseñas:** Muchos ICS poseen mecanismos de autentificación pobres (por ejemplo, las contraseñas se almacenan en texto plano).
- **Usuarios por defecto:** En muchas instalaciones no se cambian las contraseñas por defecto.
- **Usuarios no nominados:** En los sistemas industriales existen usuarios genéricos que comparten las contraseñas para no detener la actividad.
- **Carencia de controles en los cambios:** No existen procesos de documentación, pruebas y aprobación de cambios.
- **Accesos de terceros (proveedores, fabricantes, etc.):** Es muy común que ciertas tareas de mantenimiento sean realizadas por personal externo ajeno a la entidad, ya sea de forma remota o presencial. La utilización de equipos portátiles propios complica los controles.
- **Falta de respaldos (Backups):** Los factores como obsolescencia de los sistemas y diversidad de soluciones y proveedores, dificultan los procesos de copias de seguridad.
- **Falta de gestión y recuperación de incidentes:** No existen planes de recuperación ante incidentes ni responsabilidades asignadas.
- **Ausencia de plan continuidad:** La complejidad dificulta los procesos de continuidad del proceso, que no se encuentran documentados.
- **Falta de concientización en temas de ciberseguridad:** No siempre los actores del área operativa están concientizados sobre

prácticas adecuadas de ciberseguridad. Los directivos muchas veces desconocen los riesgos relacionados con la ciberseguridad.

- **Falta de monitoreo y detección de intrusiones:** No existen procesos de detección y análisis de eventos de seguridad en tiempo real.
- **Falta de segmentación de redes:** Las redes OT no se encuentras debidamente segmentadas, de acuerdo con un modelo de capas (Purdue).

Tendencias actuales

Varias tendencias vinculadas a la actividad maliciosa contribuyen a darle mayor importancia a la ciberseguridad en ambientes industriales:

- Los intentos no autorizados (intencionales/no intencionales) de acceder a información de los sistemas se encuentran en aumento.
- Los sistemas industriales deben interactuar cada vez más con diferentes redes internas/externas a la empresa.
- Las alianzas, socios y servicios subcontratados, relaciones que aumentan en la actualidad, plantean situaciones más complejas desde la perspectiva de la protección de los activos de información.
- Los ciberdelincuentes se profesionalizaron en el campo de las redes industriales y existen múltiples alternativas de herramientas y recursos disponibles para este propósito.
- Los ciberdelincuentes comenzaron a captar empleados descontentos para realizar sus ataques. Se plantea el riesgo de los llamados “insiders”, que preocupa cada vez más a los directivos de las organizaciones.
- La estandarización de algunos protocolos industriales y la adopción de protocolos como por ejemplo TCP/IP, exponen los

sistemas de control industrial a las mismas vulnerabilidades de los sistemas IT.

Estas y otras tendencias se han combinado para aumentar significativamente los riesgos de las redes industriales.

Medidas aplicadas

Las contramedidas de seguridad aplicadas en entornos industriales no deberían tener el potencial de causar pérdidas o interrupciones en los servicios y funciones esenciales. Los objetivos de seguridad se centran en la disponibilidad del sistema de control, la protección de la planta, las operaciones y la respuesta ante incidentes.

Se mencionan a continuación algunos ejemplos de controles mencionados por la ISA/IEC 62443, que bajo ningún concepto deben impedir las operaciones de funciones esenciales:

- Las cuentas de usuarios utilizadas para funciones esenciales NO se bloquearán, ni siquiera temporalmente.
- La verificación y el registro de las acciones del operador no deberán agregar una demora significativa al tiempo de respuesta del sistema.
- Para los sistemas de control de alta disponibilidad, la falla de la autoridad de certificación no interrumpirá las funciones esenciales.
- La autentificación no impedirá la iniciación de los sistemas de seguridad, denominados “*Safety*”.
- Los registros de auditoria con marcas de tiempo incorrecta no deberían afectar negativamente a las funciones esenciales.
- Un evento de denegación de servicio (DoS) no impedirá la actuación de los sistemas “*Safety*”.

Se aclara que la ISA/IEC 62443 requiere la identificación de servicios y funciones esenciales para las operaciones.

CAPÍTULO 5 Ciberataques a infraestructuras críticas industriales

Se mencionan los ciberataques a infraestructuras críticas industriales más relevantes de los últimos años, que afectaron particularmente a la industria energética.

Irán (2010) Central nuclear de Natanz - STUXNET

Ciberataque con malware contra una planta de enriquecimiento de uranio que afectó a máquinas centrifugadoras. Se considera el primer malware que ataca a un sistema industrial con consecuencias en el mundo físico. Más de 1000 equipos industriales se autodestruyeron. El objetivo fue realizar un sabotaje al programa nuclear iraní.

Se comprometió el sistema utilizando varias vulnerabilidades de día cero, iniciado probablemente mediante una memoria USB. Una vez que la entidad atacante logró tomar control, utilizando técnicas de movimiento lateral logró acceder a los sistemas OT. Por medio de otras vulnerabilidades, los ciberdelincuentes lograron cambiar la programación de los dispositivos PLC de Siemens, encargados de los controladores de velocidad de las centrifugadoras. [8]

Arabia Saudita (2012) Petrolera Saudi Aramco - SHAMOON

Se trató de un ciberataque con malware Shamoon. Su principal objetivo fue destruir sistemas de datos, atacando al registro de arranque principal (MBR). Dejó más de 30.000 puestos de trabajo fuera de servicio, sobre escribiendo los datos y mostrando una imagen de una bandera estadounidense en llamas. [9]

En el mismo año, la empresa de gas natural de Qatar RaSGas sufrió un ataque con Shamoon que dejó a la red corporativa y al sitio web inutilizados. En 2016 volvió como Shamoon 2.0 a atacar otras empresas en diferentes países.

Alemania (2014) Planta de Acero

Una planta metalúrgica de Alemania fue víctima de un ataque. A través de técnicas de ingeniería social los atacantes consiguieron acceder al equipo de un empleado y desde allí, consiguieron acceso a la red interna del sistema de control, generando un daño masivo en las instalaciones. [10]

Ucrania (2015) Red eléctrica - BLACKENERGY

Fue un ciberataque con objetivo en el sector eléctrico, que dejó a 1,4 millones de habitantes sin servicio eléctrico por 6 hs. en invierno. Tres compañías fueron atacadas simultáneamente. Se calcula que los sistemas fueron comprometidos ocho meses antes del ataque. La intrusión fue mediante un malware en un email mediante un ataque de phishing con un archivo adjunto, ingresando por la red corporativa de IT. Luego se propagó a la red OT. En el momento del ataque tomó el control de los HMI, apagando los equipos de la red eléctrica. [11]

Israel (2016) Planta Eléctrica – BLACKENERGY 2.0

En este caso el ciberataque se realizó con el malware llamado BLACK ENERGY 2.0. Dejó inoperable varios sistemas operativos por dos días, lo cual afectó al suministro eléctrico del país. [12]

Inglaterra (2016) Planta de tratamiento de agua

Según un informe de la firma Verizon [8], un grupo de hacktivistas logró acceder a los sistemas de control de una planta de tratamiento de aguas. En el informe no se revela el nombre de la empresa.

Los hacktivistas accedieron a información de los consumidores y pudiendo realizar algunas acciones del sistema de control, alterando la concentración de químicos agregados al agua.

EE. UU y Europa (2017/2018) Industrias Energéticas – DRAGONFLY 2.0

El grupo de ciberdelincuentes llamado DRAGONFLY resurge en varias oportunidades y ataca a instalaciones de EE.UU. y Europa con la intención de interrumpir las operaciones de múltiples infraestructuras críticas. Por medio de emails con adjuntos maliciosos y técnicas de ingeniería social para conseguir credenciales, lograron acceder al control de los sistemas.

Europa del Este (2017) Operadoras de Gas y Petróleo - TRITON

Fue un ciberataque con malware, al igual que Stuxnet, que utilizó la propagación USB como principal vía de infección. Atacó los controladores Schneider Triconex SIS (Sistemas Safety) cambiando su configuración con el objetivo de detener la producción y causar daños mayores en la instalación física. Se cree que el malware fue infiltrado en el año 2014 y recién explotado en 2017.

EE.UU. (2021) Colonial Pipeline – Oleoducto de petróleo - DarkSide

Se trató de un ciberataque a través del ransomware DarkSide, que dejó varios días sin suministro a la costa este de EE. UU. Se pagó un rescate de 4,4 millones de dólares. [13]

Según investigaciones de CISA y del FBI [14] los ciberdelincuentes atacaron la red de tecnología de la información (IT), no existiendo indicios de que las redes (OT) hayan sido directamente afectadas. Cuando se descubrió el malware, los operadores se vieron obligados a apagar algunos sistemas OT para evitar que se propague, esto provocó que la operación del oleoducto quedara completamente bloqueada.

Según un informe de Bloomberg [15], los ciberdelincuentes pudieron obtener casi 100 gigabytes de datos en solo dos horas antes de que comenzara la fase del ataque.

Este incidente generó un impacto significativo en el gobierno de EE.UU., a consecuencia de lo cual se redactó una estrategia nacional de ciberseguridad para para fortalecer la resiliencia en infraestructuras críticas de ese país.

EE.UU. (2021) JBS – Proveedor de carne - REvil

Ciber ataque con ransomware que afectó la cadena de operaciones de EE.UU. y Australia. La compañía confirmó que pagó un rescate de 11 millones de dólares. [16]. El FBI culpó del ataque a ciberdelincuentes del grupo REvil.

Argentina (2022) TGS – Distribuidora de gas - LockBit

Ciber ataque del grupo de ciberdelincuentes LockBit que atacó al sistema SPAC de la distribuidora de gas, el sistema de procesamiento de solicitudes, asignación y programación de los volúmenes de gas que se cargan en la red de gasoductos. [17]

Este mismo grupo de ciberdelincuentes atacó a Ledesma, La Segunda, Accenture y OSDE entre otras empresas de Argentina.

Luxemburgo (2022) Encevo/Enovos - Gas y energía eléctrica - ALPHV-BLACKCAT

Ambas empresas fueron víctimas de un ataque de ransomware por el grupo de ciberdelincuentes ALPHV-BLACKCAT [18]. La empresa informa que sus sistemas industriales no fueron afectados.

Argentina (2023) Grupo Albanesi Gas y energía eléctrica - Lockbit

Fue un ciber ataque con ransomware. Los ciberdelincuentes extorsionaron a la empresa amenazando con publicar la información robada. La empresa no dio demasiada información y solo informó que el ataque no afectó sus sistemas de control industrial.

CAPÍTULO 6 Norma ISA/IEC 62443 [19]

La norma ISA/IEC 62443 consiste en una serie de estándares con un amplio alcance, utilizados a nivel mundial, que tiene como objetivo brindar lineamientos específicos para fortalecer la seguridad de sistemas de control y automatización industrial. Fueron desarrollados en conjunto por ANSI/ISA y IEC TC65WG10.

Está conformada por una serie de documentos con más de 800 páginas, que facilita un marco flexible que sirve de base y establece mejores prácticas para la ciberseguridad en sistemas de automatización y control industrial, cubriendo conceptos claves, sistemas, procesos, evaluación de riesgos, requisitos de seguridad, ciclo de vida, etc.

El comité redactor de esta norma contó con la participación de referentes de las siguientes organizaciones: Maverick Technologies, OIT Concepts LLC, Kenexis, DuPont, Conagra Foods, OPUS Consulting Group, Rockwell Automation, Siemens, Emerson Process Management, ABB, Consultant, Fluor, The George Washington University/NAVSEA, Honeywell y Barr-Thorp Electric Co. Inc.

Los estándares están dirigidos a propietarios de sistemas industriales (responsables de diseñar, implementar y/o administrar), integradores de sistemas, fabricantes de productos, proveedores de servicios, personal de cumplimento (auditoría), usuarios y gobiernos.

La norma ISA/IEC 62443 busca mejorar la seguridad de los sistemas de control industrial, ayudando a identificar y tratar las vulnerabilidades y reducir el riesgo de los procesos bajo su control.

Se basa en estándares de sistemas tradicionales como los pertenecientes a la familia ISO/IEC 27000, identificando las principales diferencias en función de los distintos ambientes de tecnologías de operación y de Información.

Hace una gran diferenciación sobre los riesgos que enfrentan los sistemas industriales, principalmente vinculados a las implicancias para la salud, la seguridad del medio ambiente y el impacto en la seguridad nacional, aspectos que no son tan notorios en los ambientes de IT.

Estructura de la norma ISA/IEC 62443

En el siguiente gráfico se muestra la estructura y organización de la serie ISA/IEC 62443.

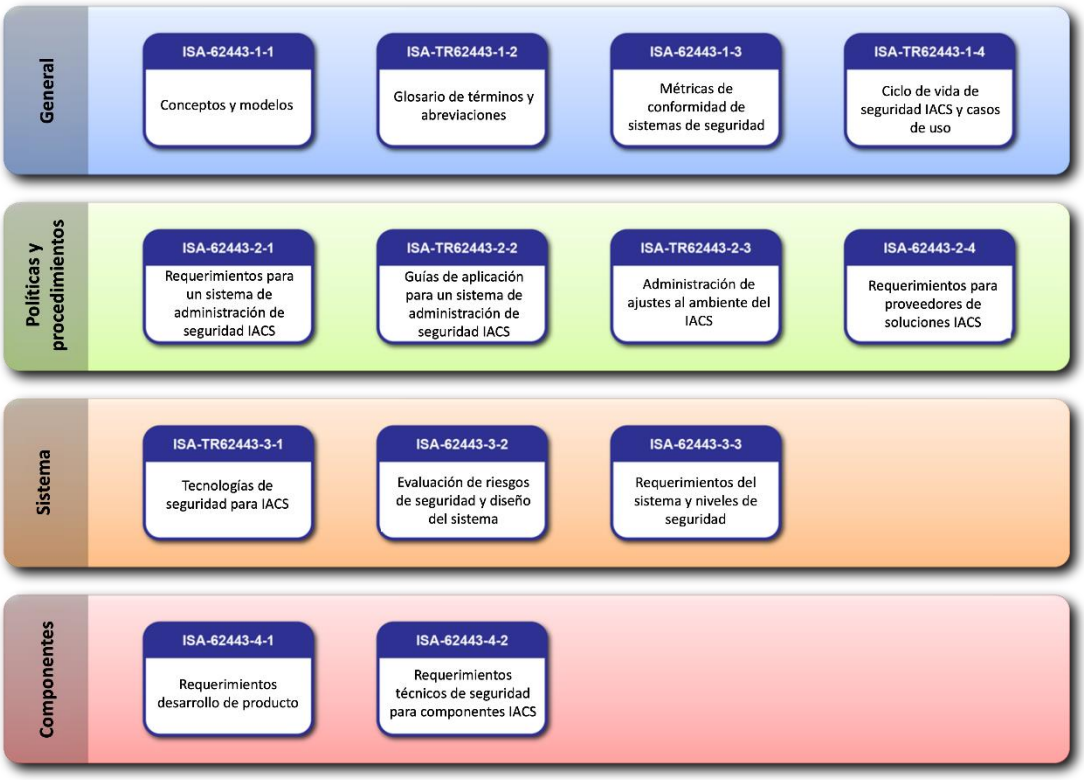

Figura 6 - Estructura ISA/IEC 62443 [20]

Como puede apreciarse en el gráfico anterior, el estándar está dividido en cuatro secciones principales.

- **General:** Se definen los conceptos básicos, métricas, ciclo de vida, casos de uso y los niveles de protección para los sistemas industriales. Se compone de cuatro documentos:

  ISA-62443-1-1: Terminología y conceptos básicos de la serie.
  ISA-TR62443-1-2: Glosario de términos y abreviaturas.

ISA-62443-1-3: Métricas cuantitativas.

ISA-TR62443-1-4: Ciclo de vida para IACS

- **Políticas y procedimientos:** Detalla un marco de referencia para la gestión de un gobierno de ciberseguridad en un entorno OT. Se compone por cuatro documentos:

  ISA-62443-2-1: Requerimientos para definir e implementar un sistema eficaz de gestión de ciberseguridad en un entorno IACS.

  ISA-62443-2-2: Requisitos para operar un sistema eficaz de gestión de ciberseguridad en un entorno IACS.

  ISA-TR62443-2-3: Gestión específica sobre la gestión de parches.

  ISA-62443-2-4: Requisitos para los proveedores.

- **Sistemas:** Se listan controles de seguridad que contribuyen a una protección de la información de los procesos. Se compone por tres documentos:

  ISA-TR62443-3-1: Aplicación de tecnologías de ciberseguridad a un entorno IACS.

  ISA-62443-3-2: Evaluación de riesgos de seguridad y el diseño de sistemas para IACS.

  ISA-62443-3-3: Requisitos básicos de seguridad del sistema y los niveles de garantía de seguridad SL.

- **Componentes:** Se enumeran los requisitos de ciberseguridad para el desarrollo seguro de productos, requerimientos que deben cumplir los fabricantes de dispositivos industriales.

  ISA-62443-4-1: Requisitos aplicables al desarrollo de productos.

  ISA-62443-4-2: Mapeo detallado de los requisitos del sistema a los subsistemas y componentes del IACS.

Los documentos de la norma se nombran con el formato “ISA-62443-xy” donde “x” hace referencia al grupo (1-4) e “y”, a un documento específico dentro del grupo. El prefijo TR en el nombre significa “Reporte técnico”.

Elementos del sistema de seguridad

La ISA agrupa los elementos de seguridad en tres amplias categorías. La seguridad integral solo se logra cuando se combinen estas tres áreas principales: personas, procesos y tecnología.

Figura 7 - Elementos de seguridad IEC 62443 [19]

Cada una de estas 3 categorías debe abordarse para responder los desafíos asociados con la ciberseguridad. [20]

Personas

Abarca a todos los miembros de la organización, incluyendo a la alta dirección, la gerencia, el personal, los contratistas y todo personal que desarrolla, controla, implementa o administra cualquier componente del programa de ciberseguridad de los sistemas industriales.

Estos componentes son:

- Relaciones: Se deberá promover las relaciones entre los diferentes equipos para lograr la integración entre los grupos de IT, OT y las áreas de negocio, como así también con proveedores e integradores de sistemas.
- Concientización: La organización debe asegurarse que todas las personas tengan la intención y la motivación para aplicar las

políticas de seguridad y garantizar la mejora continua. El personal debe estar concientizado respecto a las políticas.

- Recursos: Es necesario contar con el personal necesario y calificado para realizar las tareas asociadas con el sistema de gestión de seguridad.
- Roles y responsabilidades: Se debe definir el propietario del proceso y los diferentes grupos, así como sus responsabilidades sobre las tareas involucradas para operar y mantener los ICS. Es fundamental que todas las personas participantes tengan en claro sus funciones y responsabilidades. Para ello, se podrá usar una matriz de roles y responsabilidades (RACI).
- Capacidad y capacitación: El personal debe estar calificado y capacitarse para realizar las funciones asociadas con la ciberseguridad de los sistemas industriales.

Procesos

En esta categoría se incluyen las políticas, procedimientos, formularios, procesos y toda documentación asociada con el sistema de gestión de la seguridad. A continuación, se describen algunas de ellas:

- **Políticas:** declaración o plan formal, breve y de alto nivel que abarca las creencias, metas, objetivos y la enunciación de los procedimientos generales de una organización para un área temática específica.
- **Norma o Estándar:** Documento formal que establece requisitos obligatorios, criterios técnicos, métodos, etc. Están destinados a transmitir una acción o regla obligatoria y son complementarios a una política.
- **Procedimiento:** Describe detalladamente un conjunto de pasos y acciones establecidos y generalmente rutinarios para llevar adelante una acción o proceso.

- **Directriz:** no se requieren como parte de un marco de políticas, pero pueden desempeñar un papel importante en la transmisión de información sobre mejores prácticas para realizar alguna tarea. Las pautas están destinadas a "guiar" a los usuarios para que adopten comportamientos que aumenten la postura de ciberseguridad.

Tecnologia

Esta categoría incluye todas las capacidades técnicas de seguridad y los controles establecidos para preservar la disponibilidad/continuidad, integridad y confidencialidad del sistema industrial. Esto incluye soluciones para autenticación, control de acceso y encriptación, ya que estas medidas técnicas se aplican para reducir los riesgos de seguridad. El objetivo es lograr que los riesgos de seguridad se reduzcan.

Ejemplos de aplicación de la metodología

En la siguiente tabla se ilustra la manera en que se pueden aplicar estrategias y soluciones utilizando la metodología de personas, procesos y tecnología. [20]

Categoría	Aplicación
Personas	Se recomienda empezar por esta categoría para aumentar y asegurar tener éxito. › Obtener el compromiso de la Gerencia de que todos los cambios de dispositivos industriales deben estar autorizados y se requiere la adopción explicita de una evaluación de riesgos de ciberseguridad en el proceso de control de cambios › Identificar a las personas de la organización responsables en cada unidad de negocio, que puedan garantizar que la misma se adhiera al proceso de control de cambios › Identificar a los responsables dentro de la organización de apoyar el proceso de control de cambios y sus respectivos roles › Comunicar, promover y dispensar campañas de formación y concientización a todos los participantes del proceso de control de cambios.

Procesos	Esta categoría comienza una vez que la estrategia de "Personas" ya ha dado inicio. › Documentar un marco normativo (Política y Normas) apropiado dirigido a todo el personal y a los contratistas, quienes deberán seguir dichos estándares y procedimientos de control de cambios. › Identificar y actualizar todos los procesos de control de cambios tal que incluyan revisión de todos los dispositivos industriales existentes y la evaluación de sus ciber riesgos. › Desarrollar programas de entrenamiento y talleres de los nuevos procesos y procedimientos. › Monitorear y auditar el éxito de los nuevos programas y ajustarlos dinámicamente a las necesidades
Tecnología	La tecnología debe ser considerada para mejorar la productividad, eficiencia y la consistencia de los procesos industriales. › Desarrollar requerimientos técnicos para la presentación de solicitud de cambios, evaluación, aprobación y retención de pruebas › Migrar los procedimientos y formularios de control de cambios a la plataforma tecnológica. Verificar la consistencia de estos con los métodos basados en papel › Implementar tecnología para identificar y tener trazabilidad en los cambios de configuración de todos los dispositivos industriales y sus componentes, hardware y software.

Figura 8 - Estrategias y soluciones (personas-procesos-tecnología)

Requisitos relacionados con Personas – Procesos - Tecnología

Los requisitos para la seguridad definidos en la norma ISA/IEC 62443 están en concordancia con los definidos por la ISO/IEC 27000, en especial con la ISO/IEC 27002, con salvedades especiales de los sistemas industriales.

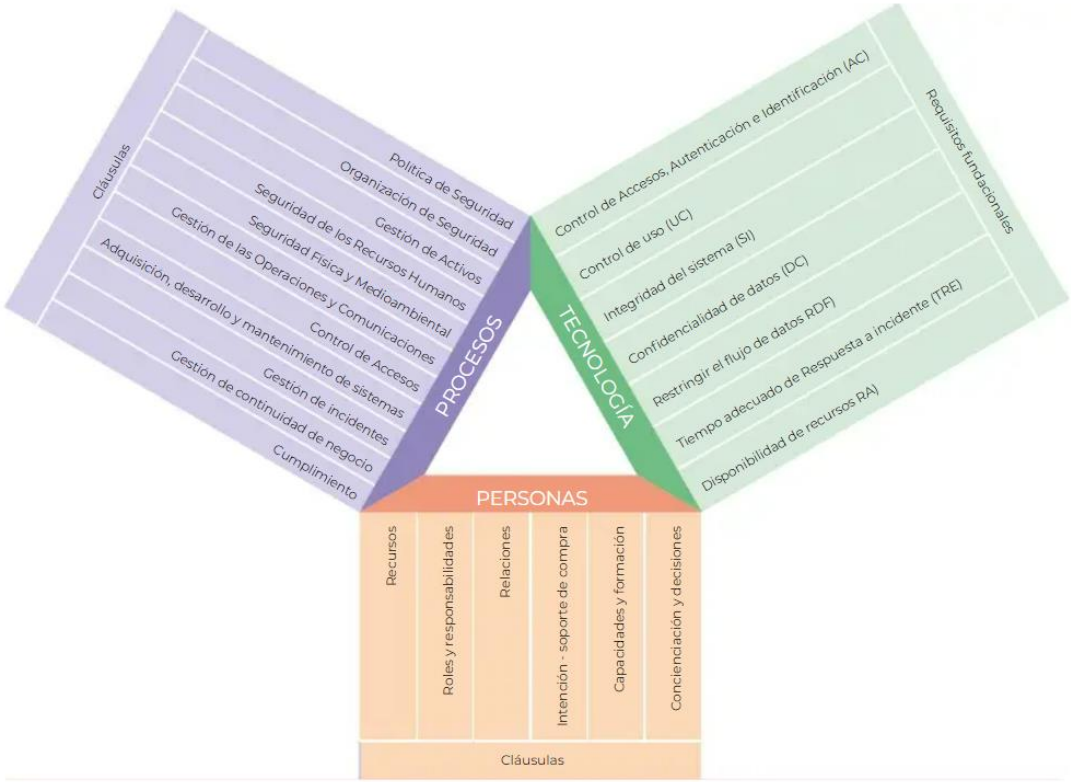

Figura 9 - implementación requisitos (personas-procesos-tecnología) [20]

Roles y Funciones

La norma ISA/IEC 62443 define los siguientes roles y funciones:

- **Propietario o dueño del activo:** Es la persona u organización que tiene la responsabilidad principal del funcionamiento del IACS y su seguridad. Las responsabilidades incluyen la identificación de riesgos asociados al ciclo de vida. También define el riesgo residual aceptable.
- **Operador de activos:** Es la persona u organización responsable de la operación del sistema.
- **Integrador de sistemas:** Es común que en un IACS sea diseñado y configurado por un integrador externo, bajo las especificaciones y requisitos proporcionados por el dueño del activo.

- **Proveedor de producto:** la responsabilidad es diseñar y fabricar los componentes de un IACS.
- **Proveedor de servicio:** se requieren para asistir en aspectos de seguridad durante todo el ciclo de vida. Ejemplo: instalaciones, mantenimientos, actualizaciones, etc.
- **Autoridad de cumplimiento:** Incluyen auditorías internas/externas y reglamentaciones gubernamentales para verificar el cumplimiento de las leyes y reglamentos vigentes.

CAPÍTULO 7 Conceptos de la Norma ISA/IEC 62443

Modelo de Zonas y Conductos de seguridad

La serie ISA/IEC 62443 establece un modelo de zonas que agrupa a los diferentes activos (hardware y software) que componen la arquitectura del proceso industrial (PCL, RTU, estaciones de operación, SCADA, etc.).

Las redes OT deben estar separadas de otras redes como la red LAN corporativa. Dentro de una red OT, la norma recomienda la separación de zonas con el objetivo de agrupar activos en función del contexto de amenazas y vulnerabilidades comunes, ya que puede que no sea necesario aplicar el mismo nivel de seguridad a todos los componentes del sistema.

Los sistemas ICS no deben conectarse directamente a internet, excepto en los casos necesarios, que debe hacerlo a través de un proxy.

Uno de los principales objetivos de la ISA/IEC 62443 es la defensa en profundidad, de tal forma que la seguridad no consista solo en una defensa perimetral basada en firewalls, sino una seguridad basada en diferentes niveles.

Zona

Una zona de seguridad es una agrupación lógica o física de activos (dispositivos, datos, aplicaciones) que comparten los mismos requisitos de seguridad. También puede haber subzonas dentro de zonas, que heredan los requisitos de seguridad de la zona madre y que brindan seguridad en capas, brindando defensa en profundidad.

Cada zona debe tener un documento que describa sus atributos y sus requisitos de seguridad:

- Políticas de seguridad y niveles de seguridad (SL)
- Inventario de activos
- Requisitos de acceso y controles
- Riesgos asociados a la zona

- Contramedidas implementadas
- Consecuencias de una brecha de seguridad
- Actividades/tecnologías permitidas
- Proceso de gestión de cambios
- Comunicación que permite el acceso a la zona

La separación de zonas puede lograrse usando diferentes tecnologías y métodos, como los que se detallan a continuación:

- Separación de red por medio de dispositivos
- Redes de área local virtual (VLANS)
- Redes privadas virtuales (VPN)
- Puertas de enlace unidireccionales
- Separación física
- Filtrado de tráfico de red
- Filtrado de capa de red (en función de la IP)
- Filtrado basado en el estado
- Filtrado de puerto y/o protocolo
- Filtrado de aplicaciones

Conducto de seguridad

Un conducto es un tipo particular de zona que agrupa los canales de comunicaciones que comparten los mismos requisitos de seguridad y permiten transmitir información entre diferentes zonas (switches, routers, firewalls, cables, repetidores, etc.). La información debe fluir hacía, desde y dentro de una zona de seguridad. Los conductos se utilizan para analizar las amenazas y vulnerabilidades de comunicación que pueden existir en las comunicaciones dentro y entre zonas.

Al igual que una zona, cada conducto tiene un documento que describe sus atributos y requisitos de seguridad:

- Políticas de seguridad y niveles de seguridad (SL)
- Inventario de activos

- Requisitos de acceso y controles
- Riesgos asociados al conducto
- Contramedidas implementadas
- Consecuencias de una brecha de seguridad
- Actividades/tecnologías permitidas
- Proceso de gestión de cambios
- Zonas que interconecta

Nivel de seguridad (SL)

La norma ISA/IEC 62443 establece que, para cada zona o conducto se debe establecer cuál es el nivel de protección deseado. Para ello define cuatro niveles diferentes de seguridad (SL – Security Levels), que van del 0 al 4. [21].

- **Nivel de Seguridad 0 (SL 0):** No requiere requisitos específicos ni protección de ciberseguridad.
- **Nivel de Seguridad (SL 1):** Requiere protección contra incidentes casuales no intencionados (errores o fallas).
- **Nivel de Seguridad (SL 2):** Requiere de protección contra incidentes intencionados, utilizando bajos recursos y/o habilidades, baja motivación o conocimiento.
- **Nivel de Seguridad (SL 3):** Requiere de protección contra incidentes intencionales, los cuales podrían ser ocasionados por atacantes con conocimientos y/o habilidades avanzadas, tales como hacktivistas y ciberterroristas, etc. con una motivación moderada.
- **Nivel de Seguridad (SL 4):** Requiere de protección contra incidentes intencionales, demanda recursos y conocimientos muy avanzados. Por parte de los ciberdelincuentes, la motivación es elevada y suelen constituirse como grandes organizaciones criminales, ejércitos con importantes capacidades cibernéticas, etc.

Tipos de niveles de seguridad (Objetivo Alcanzado Capacidad)

Según el estándar se identifican tres tipos diferentes de niveles de seguridad:

- **Nivel de seguridad Objetivo (SL-T):** Es el nivel de seguridad deseado por el propietario del sistema industrial para asegurar el buen funcionamiento de los activos. Se establece como resultado de una evaluación de riesgos.
- **Nivel de seguridad Alcanzado (SL-A):** Es el nivel de seguridad actual o alcanzado en el sistema industrial. Es conveniente realizar un seguimiento periódico, ya que dichos niveles suelen disminuir frente a crecientes ataques complejos y nuevas vulnerabilidades.
- **Nivel de seguridad según Capacidad (SL-C):** Es el nivel de seguridad que alcanza un activo cuando se configura correctamente, sin medidas de compensación adicionales. Se habla de medidas de compensación adicionales cuando es necesario agregar un elemento complementario a un producto para mejorar su seguridad.

Conocer los tres niveles de seguridad (SL-T, SL-A, SL-C) le permite a la compañía definir su plan de acción y definir controles para lograr su nivel de seguridad objetivo.

SL-A >= SL-T

El nivel de seguridad actual debería ser mayor o igual al nivel de seguridad objetivo.

Requerimientos Fundamentales de seguridad (FR)

Para determinar los niveles de seguridad asociados a cada zona de seguridad, en el documento ISA-62443-1-1 se definen siete requerimientos fundamentales (FR):

- **FR1 Control de Identificación y Autenticación (IAC):** Control de acceso a un activo (dispositivo, información) físico o lógico. Ejemplo: contraseñas, autentificación multi factor (MFA), etc.
- **FR2 Control del Uso (UC):** Control del uso que se le puede dar a un activo, proteger el uso no autorizado. Ejemplo: roles de usuarios y aplicación autorización (RBAC).
- **FR3 Integridad de los sistemas (SI):** Asegurar la integridad de los equipos y la información y protección contra cambios no autorizados y en los canales de comunicación. Ejemplo: manejo de sesiones y mecanismos para reconocer cambios.
- **FR4 Confidencialidad de Datos (DC):** Asegurar la confidencialidad de los datos, protección de los canales de comunicación. Ejemplo: encripción
- **FR5 Flujos de datos Restringidos (RDF):** Restringir las comunicaciones innecesarias. Ejemplo: segmentación de red en zonas y conductos.
- **FR6 Respuesta oportuna a Eventos (TRE):** Notificar, responder y reportar ante eventos de ciberseguridad. Ejemplo: registro de logs y monitoreo.
- **FR7 Disponibilidad de Recursos (RA):** Asegurar la disponibilidad de los recursos y evitar denegaciones de servicio. Ejemplo: Copia de seguridad backups y recuperación.

De cada requerimiento fundamental FR se desprenden requisitos de los sistemas (RS) para mejorar la seguridad y sus requisitos de mejoras (RE).

Para graficar lo mencionado anteriormente, se incluye a continuación un ejemplo de mapeo:

Mapeos de Requerimientos del sistema (Asociados a cada nivel de seguridad)						
SRs y REs			SL1	SL2	SL3	SL4
FR 1		**Identificacion y autenticacion**				
SR 1.1		Usuario humano autentificado e identificado	X	X	X	X
SR 1.1	RE 1	Identificación y autenticación única		X	X	X
SR 1.1	RE 2	Autenticación multifactor para redes no confiables			X	X
SR 1.1	RE 3	Autenticación multifactor para todas las redes				X
SR 1.2		Autenticación e identificación de Software procesos y dispositivos		X	X	X
SR 1.2	RE 1	Identificación y autenticación única			X	X
SR 1.3		Administración de cuentas	X	X	X	X
SR 1.3	RE 1	Administración de cuentas unificada			X	X
SR 1.4		Administración de identificaciones	X	X	X	X

Figura 10 - Mapeos de Requerimientos del sistema [23]

De esta manera, el nivel de seguridad deseado SL-T para una zona o conducto en particular se representa en forma de vector:

SL-T (Zona/Conducto) = {IAC UC SI DC RDF TRE RA}

Por ejemplo, para una zona desmilitarizada o DMZ, este podría ser el nivel de seguridad objetivo:

SL-T (Zona DMZ) = {3 3 2 1 3 1 2}

Modelo Purdue

El modelo Purdue es un modelo adoptado en la ISA-95 (1989) pero aún hoy sigue vigente como una arquitectura de referencia para el standard. Sin embargo, existen áreas en donde el modelo no es suficiente.

Esto se debe a que actualmente existen nuevas tecnologías, comunicaciones inalámbricas, servicios en la nube, accesos remotos, servicios subcontratados y por supuesto, un crecimiento de los ciberataques.

Por este motivo, el modelo no refleja exactamente la arquitectura de un ICS hoy, sino se constituye en una referencia que sirve como ayuda.

Básicamente establece una segmentación para lograr que los dispositivos de cada capa solo puedan comunicarse dentro de su misma capa. La implementación de firewalls en los puntos de comunicación entre capas regula y facilita el flujo de datos entre los dispositivos de diferentes capas. Como resultado, el tráfico se vuelve más predecible y controlado, lo que a su vez permite habilitar la capacidad de aislar los diferentes niveles en caso de que surja un incidente de ciberseguridad.

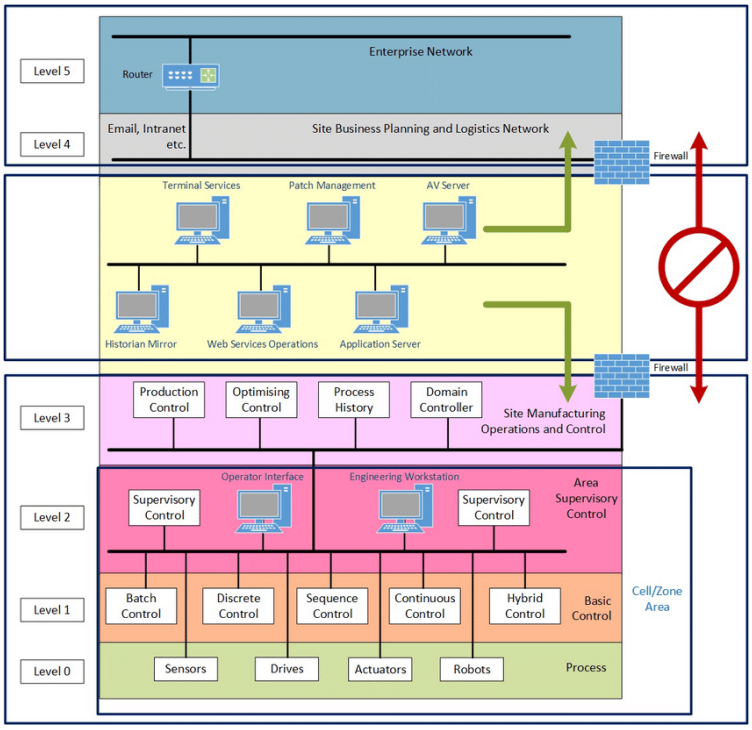

Figura 11 - Arquitectura de referencia Purdue [24]

Niveles del Modelo Purdue

- **Nivel 4/5 – Sistemas de Negocios:** En este nivel se encuentran los sistemas y aplicaciones que respaldan las funciones involucradas en las actividades relacionadas con el negocio. Esta capa está fuera de la red OT, pero necesita vincularse para

consumir datos. Incluyen sistemas de gestión ERP, gestión con clientes (CRM), financieros, de producción, etc.

- **Nivel 3.5 – DMZ OT:** Esta capa ofrece servicios para compartir servicios que deben ser accesibles desde el exterior a la red OT, sin exponer directamente la seguridad.
- **Nivel 3 – Gestión de operaciones:** En este nivel se engloban las funciones involucradas en la gestión de flujos de trabajo complementarios para poder llevar a cabo el proceso industrial. Aquí se encuentran los sistemas historiadores (Historian), estaciones de operadores, etc.
- **Nivel 2 – Supervisión:** Se centra en las funciones involucradas en la supervisión y control en tiempo real del proceso físico. Algunos elementos de este nivel son: SCADA, interfaces HMI, etc.
- **Nivel 1 – Control local:** En este nivel encontramos las funciones involucradas en la detección y manipulación del proceso físico. El sistema de control lee datos del Nivel 0 (sensores) y ejecutan un algoritmo de control, envía salidas a un dispositivo actuador (válvulas, compuertas, etc.). Este nivel comprende a los PLC, los RTU.
- **Nivel 0 – Proceso:** En este nivel se encuentra el proceso físico real. Incluye a los sensores y actuadores conectados directamente al proceso físico.

Modelos de referencia

Los diferentes modelos que muestra la ISA/IEC 62443 nos pueden servir de referencia para definir zonas en nuestra infraestructura. El tamaño de las zonas es arbitrario, ya que el diseño va a depender de las necesidades en cada organización.

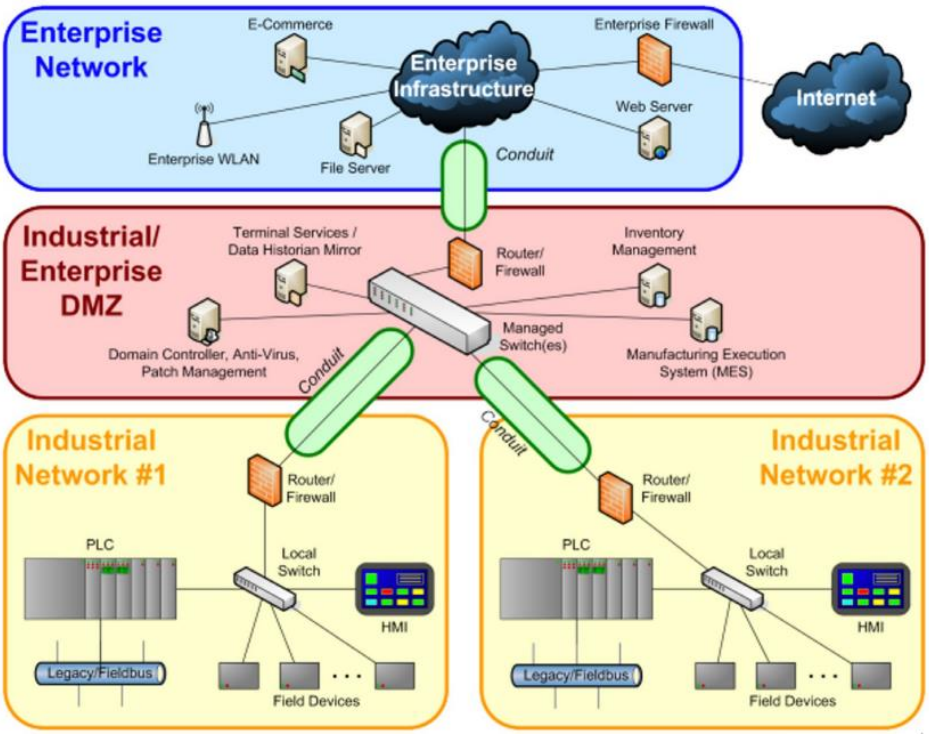

Figura 12 - Esquema referencia fabrica [25]

Ejemplo de referencia de fabrica:

Zonas:	Conductos:
Red Empresarial DMZ (Empresarial/Industrial) Red Industrial #1 Red Industrial #2	Red Empresarial – DMZ DMZ - Red Industrial #1 DMZ - Red Industrial #2

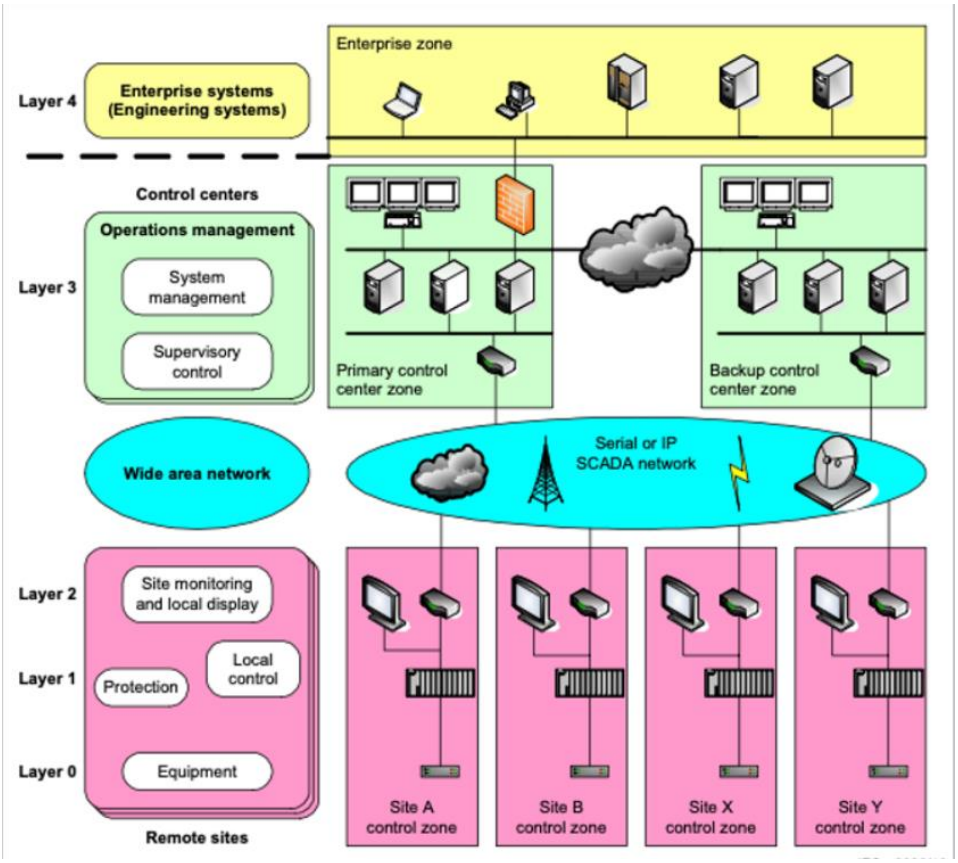

Figura 13 - Esquema referencia SCADA [25]

Ejemplo de referencia de SCADA

Zonas:	Conductos:
Red Empresarial	Centro primario – secundario
Centro de control primario	Centro primario – empresa
Centro de control secundario	Centros control – SCADA
Red supervisión y control	SCADA – Sitios remotos
Sitio remoto A / B / X / Y	

Criterios para la separación de zonas y conductos

A continuación, se enumeran algunos criterios iniciales para realizar una adecuada separación de zonas y conductos: [22]

- Los activos de las redes del negocio (IT) y los sistemas de control industrial (OT) deben estar agrupadas en zonas separadas.
- Los activos de seguridad "***safety***" (SIS) deben estar separados en zonas distintas, ya que por su criticidad y naturaleza poseen requisitos de seguridad diferentes.
- Los dispositivos que eventual o temporalmente se conectan deben estar en zonas diferentes. Ejemplo: Dispositivos móviles, notebook de proveedores, dispositivos de almacenamientos externos (USB), etc.
- Las comunicaciones inalámbricas deben ubicarse en una o más zonas separadas de las comunicaciones cableadas.

CAPÍTULO 8 Sistema de gestión de ciberseguridad industrial

Desarrollo del sistema (CSMS)

El sistema de gestión de ciberseguridad es un componente clave dentro de un sistema de control industrial.

La organización debe diseñar e implementar un programa de gestión de ciberseguridad OT para poder reducir y gestionar los riesgos creados por las amenazas que puedan afectar entornos industriales. Dicho programa debe ser integrado y consistente con el programa de ciberseguridad IT, contemplando los requisitos específicos de los entornos OT, según las diferencias analizadas anteriormente.

En la norma ISA-62443-2-1 se proporciona una base sobre cómo desarrollar un marco de gestión para los ICS, comenzando por el análisis de riesgos de nivel superior.

Los componentes del programa se presentan en las siguientes tres categorías:

1. Análisis de riesgos
2. Abordaje del riesgo (implementación)
3. Seguimiento y mejora continua (monitoreo y mantenimiento)

Cada una de estas tres categorías se divide a su vez en diferentes grupos de elementos. En la siguiente figura se muestra la relación entre las categorías, los grupos de elementos y los elementos en sí.

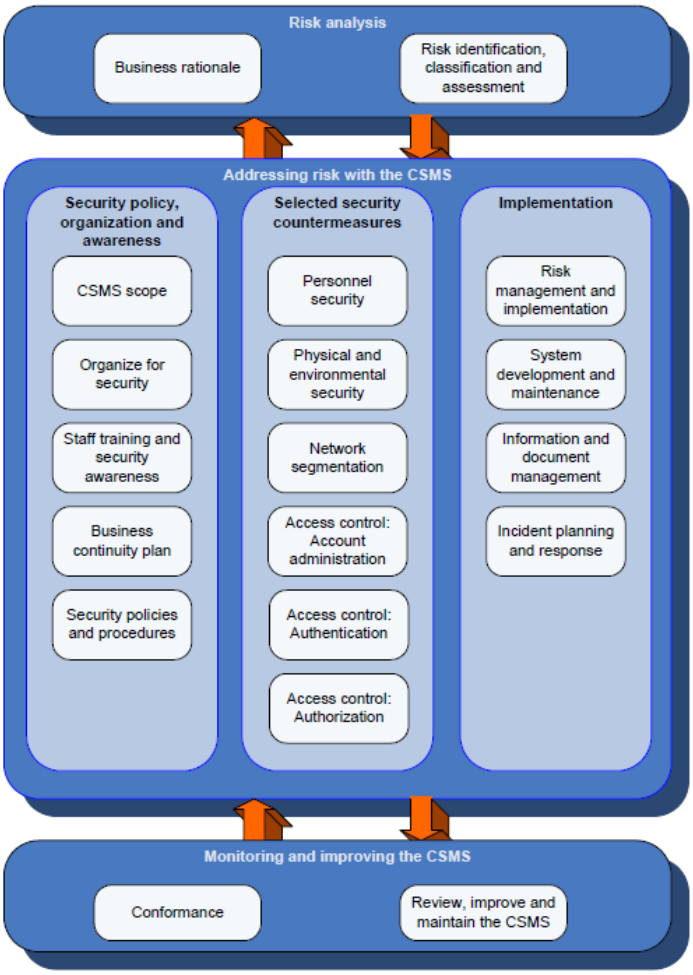

Figura 14 - Elementos de un sistema de gestión de ciberseguridad [19]

1. Análisis de riesgos

En el documento ISA-62443-3-2 se describen los requisitos para abordar la evaluación de riesgos en un IACS, incluyendo el uso de zonas, conductos y niveles de seguridad. No especifica la metodología en particular a ser utilizada, la cual debe ser establecida por el propietario del activo. Se recomienda que sea compatible con la metodología de la organización.

El negocio deberá identificar las necesidades para abordar el riesgo, basado en la naturaleza y magnitud de las posibles consecuencias financieras, de salud, de seguridad ambiental y de otro tipo, en caso de que ocurran incidentes de ciberseguridad. En base a estas razones, se determinará el nivel de riesgo aceptable.

El riesgo para la organización no es estático, puede cambiar como resultado de factores internos y externos en el tiempo. Por lo tanto, este proceso debe revisarse periódicamente.

2. **Abordar el riesgo**

Esta categoría contiene la mayor parte de los requisitos e información del programa de ciberseguridad, para la implementación de contramedidas para los riesgos identificados. Esta categoría a su vez se divide en tres grandes grupos:

- Política de seguridad, organización y concientización
- Contramedidas de seguridad
- Implementación

3. **Seguimiento y mejora continua**

Esta categoría proporciona procesos continuos del programa de gestión de la seguridad. El seguimiento de los (KPI) definidos para cada contramedida, así como el desarrollo continuo del programa, son requisitos fundamentales para la eficiencia del mismo.

Políticas y procedimientos

Las políticas de seguridad permiten que una organización siga un programa coherente para alcanzar un nivel aceptable de seguridad. Se definen en diferentes niveles de la organización, desde las políticas de gobierno o gestión, establecidas a nivel superior hasta las de operación que definen los detalles de la administración de la seguridad.

Una política de seguridad es una declaración o plan formal, breve y de alto nivel que abarca las creencias, metas, objetivos y procedimientos de una organización. Regula cómo ésta protege los recursos pertenecientes a

sistemas críticos y su cumplimiento es obligatorio. Permiten medir el desempeño y son útiles en las auditorias.

Políticas y procedimientos de Arquitectura

Describen configuraciones seguras para sistemas de control, e incluyen:

- Diseño de redes recomendado
- Configuración de firewall recomendada
- Autentificación y autorización de usuarios
- Interconexión de diferentes redes
- Uso de comunicaciones inalámbricas
- Dominios y relaciones de confianza
- Administración de actualizaciones y parches de seguridad
- Herramientas antivirus
- Acceso a redes externas
- Uso adecuado de correo electrónico
- Dispositivos portátiles
- Accesos remotos
- Política de proveedores o subcontratistas

Inventario de activos físicos y lógicos

Para poder garantizar la seguridad dentro de una zona, es imprescindible que la organización cuente con un inventario de activos físicos y lógicos actualizado. El inventario es fundamental para evaluar el riesgo y las vulnerabilidades y así poder desarrollar las medidas de seguridad de acuerdo con el nivel de riesgo aceptable por el negocio.

Los activos lógicos incluyen el software y los datos utilizados en la zona.

Las herramientas no intrusivas tipo IDS basados en comportamientos pueden ser de gran utilidad para descubrir dispositivos existentes en las diferentes zonas.

Se debe crear un documento o apoyarse en algún software con tal fin, que detalle todos los activos lógicos y físicos que forman parte de la zona. A modo de guía, se comparte una matriz que contiene a modo de ejemplo los campos que podrían incluirse en ese detalle. [22]

1

GENERAL				
Zona	Sector inductrial al que pertenece	Ubicación geográfica	Proceso industrial	Contacto
Indentificador unico de zona	Sector industrial.	Provincia, estado, región, etc..	Breve descripción del proceso industrial	Nombre del responsable

3

NIVELES DE SEGURIDAD		
SL-T	SL-A	SL-C
Nivel de seguridad del objetivo	Nivel de seguridad alcanzadow	Nivel de seguridad según capacidad

2

SISTEMA DE SUPERVISIÓN Y CONTROL															
Tipo de sistema	Producto	Versión	COMPONENTE DE TELESUPERVISIÓN						COMPONENTES DE COMUNICACIÓN		COMPONENTES DE CONTROL				
			Tipo	Nombre del equipo	Sistema operativo	Dirección IP	Dirección IP-NAT	Antivirus	Tipo	Marca y modelo	Tipo	Marca y modelo	Protocolo	Detalle del IPs	Dirección IP-NAT
SCADA,HMI,DCS, Adquisidor de datos, otro	Nombre comercial	xxx	Estación de Ingeniería, Estación de Operación, Servidor.	Nombre del equipo que ejecuta el Sistema.	Versión de SO	Dirección IP del equipo	Dirección IP en caso de utilizar protocolo NAT	Marca del antivirus	Switch, Router, Modem,	Marca y Modelo	PLC, RTU etc.	Marca y Modelo	Protocolo de comunicación utilizado	Direccionamiento IP del componente	Dirección IP en caso de utilizar protocolo NAT

Gobierno de Ciberseguridad

Una de las principales medidas recomendada por la normativa ISA/IEC respecto a la ciberseguridad, es el desarrollo de un sistema de gobierno que defina los lineamientos generales para proteger los sistemas industriales. Este sistema incluye los siguientes aspectos:

- Análisis de Riesgo
- Entendimiento del negocio
- Clasificación de riesgos.
- Implementación de un Gobierno de Ciberseguridad Industrial
- Políticas de seguridad
- Medidas de seguridad

- Implementación
- Cumplimiento del programa de Ciberseguridad Industrial
- Métricas de seguridad
- Conformidad y plan de mejora

Establecimiento de un estatuto para el programa de ciberseguridad OT.

La alta dirección puede demostrar su compromiso con la ciberseguridad a través de un documento de alto nivel y escrito en un lenguaje sencillo, que establezca un mandato para la persona de mayor rango responsable de establecer y mantener el programa de seguridad. Según el informe de estado para 2023 en tecnologías operativas de Fortinet [23], la mayoría de las organizaciones han puesto la responsabilidad de la ciberseguridad OT bajo un director de seguridad de la información o CISO.

Es fundamental que el programa defina claramente los roles y las responsabilidades de las personas involucradas.

Conformación del equipo de ciberseguridad industrial

Según la recomendación de la guía NIST 800-82 para abordar adecuadamente la seguridad en un sistema industrial (OT) es fundamental contar con un equipo interdisciplinario que debería estar formado por un miembro de IT, un ingeniero de control industrial, un operador del sistema de control, un experto en seguridad de redes y sistemas, un miembro de administración y un miembro de seguridad física como mínimo. También hace referencia a la importancia de integrarse con los proveedores del sistema de control y el integrador del sistema.

Definir un programa de concientización sobre ciberseguridad industrial

La inclusión de una capacitación y concientización adecuada del factor humano puede ser una diferencia entre una fortaleza o una gran vulnerabilidad. Los equipos que operan, administran y tienen acceso al

sistema de control deberán tener una formación adecuada en materia de ciberseguridad industrial. Es responsabilidad de la organización diseñar e implementar un programa de capacitación en ciberseguridad.

Las políticas de seguridad deben ser comunicadas y conocidas por todo el personal. Cada empleado debe comprender su rol y responsabilidad.

La capacitación y concientización puede reducir significativamente los riesgos de ciberseguridad y deben ser validadas de manera continua.

Nivel de madurez

Para el bucle en el ciclo de vida de mejora continua, la norma ISA/IEC 62443 se basa en un modelo de madurez derivado del CMMI (Capability Maturity Model Integration). Describe diferentes niveles de madurez para procesos.

Para cumplir con un determinado nivel de madurez, todos los requisitos del nivel deben cumplirse para todo el proceso.

- **Nivel 1 (Inicial):** Los procesos no están definidos y las tareas se realizan básicamente por el esfuerzo individual de las personas (ad hoc). No existe estandarización y documentación, ni un responsable ni un programa de ciberseguridad formal.
- **Nivel 2 (Gestionado):** Existen procesos parcialmente definidos, pero no son adoptados por todo el ecosistema. Las mejores prácticas no están en el ADN de los usuarios. Puede existir un gobierno informal de ciberseguridad.
- **Nivel 3 (Definido):** Existen procesos bien definidos e integrados en toda la organización. Se enfocan en la gestión de riesgos. Existe un gobierno formal de ciberseguridad con interacciones con los niveles ejecutivos.
- **Nivel 4 (Optimizado):** Existen controles documentados, se realizan mediciones y auditorias periódicamente para gestionar y controlar los procesos. Se recopilan datos y se utilizan para la

toma de decisiones. Se busca una mejora continua. Los niveles ejecutivos interaccionan de forma continua con ciberseguridad.

La ISA/IEC 62443 se ha limitado a cuatro niveles de madurez, agrupando los niveles 4 y 5 del modelo CMMI en un solo nivel (4-Optmizado).

Existen otras herramientas para medir el nivel de madurez. Por ejemplo, el departamento de energía de los EE.UU. (DOE), colaboradores de la industria y otras agencias gubernamentales diseñaron el modelo C2M2 o CMMC para ayudar a las organizaciones de infraestructura critica a evaluar y mejorar sus prácticas de ciberseguridad.

Desarrollar la capacidad de respuesta a incidentes

A pesar de las medidas preventivas, los incidentes de seguridad son inevitables y es muy importante desarrollar capacidades de detección y respuesta para minimizar los impactos y tiempos de recuperación.

El proceso de gestión y respuesta a incidentes está compuesto por diferentes actividades, que son la planificación, respuesta y recuperación. Ante un incidente se deberá analizar el alcance y riesgo, contener y responder al incidente, comunicar a los interesados y tomar medidas para reducir el impacto futuro. El plan debe incluir funciones y responsabilidades, el flujo de trabajo, la clasificación de gravedad del incidente, los contactos de los involucrados internos y externos y tipo de comunicación.

Es muy importante que las organizaciones desarrollen capacidades de recuperación y restauración.

Fase de planificación: Debe establecerse un programa para reconocer y responder a un incidente. Este programa deberá incluir los tipos de incidentes que se tratarán y las respuestas para cada uno de ellos, las personas que intervendrán, así como las comunicaciones dentro y fuera de la organización.

Fase de respuesta: Agrupa las acciones necesarias para eliminar o minimizar los impactos del incidente. La respuesta tomada ante un incidente depende del tipo del incidente y su efecto.

Fase de recuperación: Consiste en llevar a cabo las acciones para que el sistema vuelva a operar normalmente de la manera más rápida y segura posible. Incluye tareas de restauración de los sistemas de respaldo (backups).

CAPÍTULO 9 Centro de Seguridad para Internet (CIS)

El Centro de Seguridad para Internet (CIS) es un organismo sin fines de lucro creado en el año 2000 con el objetivo de compartir mejores prácticas de ciberseguridad, reconocidas a nivel mundial, con el fin de proteger los sistemas y datos. [24]

El (CIS) en su versión 7, establece en términos generales 20 controles relacionados con las redes industriales. A continuación se realiza un resumen de los controles:

CIS Control 1: Inventario y control de activos de hardware

El primer paso consiste en identificar los sistemas y dispositivos que deben protegerse. Los desafíos comunes para llevar a cabo el inventario son la falta de documentación, la segmentación de la red, la presencia de dispositivos antiguos y nuevos de múltiples proveedores, los protocolos específicos, la sensibilidad de equipos para realizar escaneos, etc.

CIS Control 2: Inventario y control de activos de software

Consiste en identificar, rastrear y contabilizar el software en la red. Al igual que el hardware, los componentes de software suelen ser sensibles al uso de herramientas automatizadas tradicionales de inventario de IT.

CIS Control 3: Gestión de vulnerabilidades

Este control aborda la necesidad de una gestión continua de vulnerabilidades. Algunos desafíos son: las ventanas de mantenimiento son limitadas, el ciclo de vida de los componentes es más extenso.

CIS Control 4: Uso controlado de privilegios administrativos

Aborda la necesidad de limitar y administrar el acceso del administrador. Se recomienda el uso de privilegios elevados y la utilización de cuentas de administración solo cuando sean necesarias.

CIS Control 5: Configuraciones seguras

Este control proporciona orientación para proteger el hardware y el software. Es importante definir y aplicar recomendaciones de aseguramiento tanto a los sistemas operativos como a los softwares originales de los proveedores del ICS y deshabilitar protocolos y funcionalidades que no se utilicen de manera de reducir la superficie de ataque.

CIS Control 6: Mantenimiento, seguimiento y análisis de registros de auditoria

Este control ofrece orientación para el mantenimiento y seguimiento de los registros de auditoría. Es un gran desafío ya que muchos dispositivos del entorno ICS no admiten registros nativos de seguridad o compatibilidad con elementos externos para su gestión.

CIS Control 7: protección de correo electrónico y navegador web

Este control se centra en la seguridad de los clientes de correo electrónico y de los navegadores web, ya que son vectores de ataques muy importantes. En los entornos ICS no se requieren accesos a web de internet ni clientes de correo electrónico ya que están separadas de las redes de IT, pero muchos sistemas ICS interactúan con correos salientes, por lo general de alertas y consolas web con servidores internos.

CIS Control 8: Defensa contra malware

Este control aborda los pasos necesarios para garantizar una defensa contra intrusiones de malware. Si bien la segmentación adecuada de la red y las estrategias de defensa en profundidad ayudan a mitigar este riesgo, es necesario contemplar una herramienta para tal fin.

La sensibilidad de los equipos, la obsolescencia y compatibilidad son los desafíos para las herramientas antivirus. Las soluciones deben estar validadas por los proveedores de los sistemas ICS y las pruebas y configuraciones deben ser mucho más cuidadosas.

CIS Control 9: Limitaciones y control de puertos, protocolos y servicios de red

Este Control CIS se enfoca en la necesidad de controlar los puntos de acceso a la red, los puertos y los servicios.

Al contabilizar puertos, protocolos y servicios, a menudo es útil comenzar con la documentación del proveedor, ya que muchos ICS comprenden sistemas propietarios. Muchos proveedores tienen documentación básica que puede proporcionar un punto de partida o detalles específicos de sus soluciones.

CIS Control 10: Capacidad de recuperación de datos

Este control CIS hace referencia a la necesidad de realizar copias de seguridad del sistema para contribuir a la capacidad de recuperación de datos.

Al igual que los controles anteriores el desafío es encontrar en cada sistema ICS, la forma de realizar las copias completas. Se aclara que muchos sistemas no admiten copias de seguridad automáticas.

CIS Control 11: Configuraciones seguras de red Firewall, enrutadores y conmutadores

Este control CIS aborda la relevancia de gestionar la configuración de todos los dispositivos de red mediante un proceso de control de cambios. La infraestructura de una red ICS normalmente conlleva requisitos adicionales en comparación con los sistemas de TI tradicionales.

Por lo general, estas redes se enfocan en la disponibilidad y están diseñadas con requisitos de rendimiento y redundancia en tiempo real.

Los firewalls deben estar configurados para denegar en forma predeterminada.

CIS Control 12: Defensa de límites

Este Control CIS se centra en la importancia de gestionar y controlar el flujo de información entre redes de diferentes zonas, es decir el alineamiento con el modelo de referencia de Purdue.

Los sistemas ICS no deben conectarse directamente a internet, excepto en los casos necesarios, que debe hacerlo a través de un proxy.

CIS Control 13: Protección de datos

El enfoque de este control CIS está en la protección de datos y la relevancia varía mucho según el entorno ICS. Estos entornos a menudo no contienen prácticamente datos confidenciales en el sentido tradicional. En muchas redes ICS, los datos de control consisten en mediciones físicas como flujo, temperatura, presión o lecturas de válvulas y comandos específicos emitidos por dispositivos de control lógico que controlan un proceso general.

A veces, esta información no se considera especialmente sensible o patentada por sí misma y en algunos casos, carece de protecciones particulares en la forma en que se recopila, transfiere, almacena y analiza. Sin embargo, algunas organizaciones consideran que esta misma información es confidencial, ya que de hecho puede proporcionar indicios sobre el diseño de un ICS, los productos conectados, el proceso patentado, los datos de producción, las variables del proceso, los cronogramas del sistema, los cambios de configuración y una gran cantidad de otros datos que pueden proporcionar inteligencia significativa para ciberdelincuentes.

En algunos entornos de ICS puede haber cierta información que esté muy protegida y la capacidad de mantenerla confidencial es clave para el éxito empresarial. Esto se ve a menudo en el espacio de fabricación donde se utilizan recetas o fórmulas para fabricar alimentos o productos químicos. Es una preocupación creciente para la infraestructura crítica ICS porque se

reconoce que dicha fuga de datos puede ayudar a un atacante a desarrollar una estrategia.

CIS Control 14: Acceso controlado basado en la necesidad

Controlar el acceso a los sistemas en función de la necesidad es de vital importancia. Al lograr una estratificación de red adecuada (modelo de referencia de Purdue), se implementará cierto grado de segmentación física y lógica. Los dispositivos que miden o controlan directamente los procesos físicos suelen estar separados de las estaciones de trabajo de propósito general.

Sin embargo, también se debe considerar la segmentación dentro de las capas.

La segmentación por subredes suele ser un enfoque aceptable. Se pueden usar VLAN o conmutadores dedicados según los requisitos de disponibilidad y costo.

CIS Control 15: Control de acceso inalámbrico

Algunos equipos de OT usan tecnología inalámbrica donde los dispositivos deben ser móviles o cuando se encuentran dispersos.

Son varias las consideraciones para tener en cuenta, entre las que se encuentran la utilización en comunicaciones críticas, los sistemas de redundancia ya que son más probables a fallas, la utilización de infraestructura de claves (encriptado) o la limitación cuando sea posible, de la intensidad y el alcance de la señal con el fin de reducir el acceso remoto desde fuera del perímetro de seguridad.

CIS Control 16: supervisión y control de cuentas

Este control CIS enfatiza la importancia de controlar el acceso de los usuarios a los sistemas en un entorno de red típico y garantizar una gestión de cuentas eficaz. Puede surgir una vulnerabilidad común si las cuentas de los empleados no se deshabilitan cuando dejan de pertenecer a la

organización o cambian de rol. En los ICS funcionan sistemas de diferentes proveedores, cada uno con sus propios directorios de cuentas de usuarios. Además, los contratistas a menudo solicitan o requieren acceso remoto. Estos factores pueden dificultar la administración de cuentas de usuario para muchos equipos de OT.

Se debe tener cuidado de no cancelar o impedir que un usuario legítimo tenga el acceso adecuado sin darse cuenta, ya que esto podría causar la interrupción o el retraso del proceso. Además, se debe considerar y administrar cuidadosamente un equilibrio entre los privilegios de cuenta solo de administrador y los privilegios de nivel de grupo. Dada la operación ininterrumpida 24x7 de muchos sistemas ICS, los incidentes pueden ocurrir en cualquier momento, incluso cuando no hay personas con privilegios administrativos disponibles para responder, remediar y recuperar.

Los subcontroles relacionados con el vencimiento de la cuenta, los bloqueos por inactividad y la autenticación multifactor no se aplican a los sistemas ICS.

CIS Control 17: Implementar un programa de capacitación y concientización sobre seguridad

Este Control CIS se centra en un programa de concientización de ciberseguridad para el personal. Es esencial que los equipos de OT estén completamente familiarizados con las mejores prácticas de seguridad. Estas habilidades deben fomentarse y expandirse en forma continua y evolutiva.

Muchos equipos de OT dependen de contratistas o proveedores que necesitan acceso a partes críticas de la red para dar servicio a equipos especializados, estos equipos deben ser incluidos en el programa de concientización de la empresa. En consiguiente, es necesario implementar un programa de concientización sobre seguridad para todos los visitantes (incluidos terceros: contratistas, subcontratistas, proveedores, etc.) antes de otorgar acceso remoto o local al sitio.

CIS Control 18: Seguridad del software de aplicación

Este control se centra en la seguridad de las aplicaciones utilizadas en el entorno industrial. El objetivo principal es proteger los ICS contra riesgos asociados a las vulnerabilidades con el software. El control establece que es fundamental llevar a cabo una gestión adecuada del ciclo de vida de las aplicaciones.

CIS Control 19: Respuesta y gestión de incidentes

Este Control CIS aborda los procesos y pasos necesarios para prepararse para un incidente. Los planes de respuesta a incidentes bien definidos e implementados pueden permitir que una empresa identifique, contenga, reduzca los impactos y se recupere más rápidamente de un ciber incidente. Esto es especialmente importante para las organizaciones donde el tiempo de inactividad del ICS puede generar impactos en la seguridad, la salud o la rentabilidad de la empresa, los empleados, los clientes, los socios de la cadena de suministro, la comunidad y otros integrantes, para permitir la operación segura y confiable.

La mayoría de los equipos de OT están acostumbrados a realizar copias de seguridad de los sistemas críticos para mitigar los riesgos de componentes defectuosos, pérdida de servicios, acciones accidentales de los empleados o incluso, aspectos de desastres naturales. Sin embargo, a menudo hay una brecha en las otras áreas de respuesta a incidentes, como la coordinación eficiente, la cadena de mando, la autoridad para tomar decisiones, el aislamiento de impactos, los informes, la recopilación de datos, la responsabilidad de gestión, los protocolos legales y la estrategia de comunicaciones. Además, no es inusual que dichos procesos se prueben de manera adecuada o periódica, y mucho menos, que evolucionen con el tiempo a medida que surgen nuevas variables, se identifican los riesgos y evolucionan las amenazas.

Para este Control CIS considerar los siguientes pasos adicionales:

- Si se extiende un plan de respuesta a incidentes de TI, se debe asegurar que el liderazgo operativo de ICS haya revisado y aprobado el plan de respuesta a incidentes.
- Los equipos de respuesta deben estar completamente familiarizados con los riesgos inherentes al entorno ICS y las mitigaciones para evitar daños secundarios que puedan afectar la seguridad operativa y la protección del personal, el equipo, la información y una variedad de otros factores dependientes e interdependientes.

CIS Control 20: Pruebas de penetración y ejercicios del equipo rojo

Este control de CIS se centra en el diseño y la realización de pruebas de penetración controladas en un entorno de tecnología operativa, incluidos los dispositivos y sistemas conectados que normalmente no se pueden ver como un componente, servicio o sistema constituyente de un ICS. El objetivo es probar tanto la capacidad de respuesta de los empleados como la resistencia de los controles internos. Se refiere a la realización de pruebas en productos, sistemas y otros productos y sistemas interconectados en tiempo real para identificar, aislar, y demostrar la capacidad de explotación de una debilidad o vulnerabilidad en la postura de seguridad del ICS.

Los procesos controlados por entornos ICS se interrumpen fácilmente con pruebas de penetración, ejercicios de equipo rojo u otras actividades similares. La realización de estas actividades en los sistemas de producción, incluso durante las interrupciones programadas, puede provocar tiempo de inactividad, destrucción, lesiones o introducir artefactos persistentes que reducen la seguridad, la eficiencia o el rendimiento del sistema probado.

Por estas razones, se recomienda realizar únicamente pruebas de penetración y ejercicios de equipo rojo en sistemas que no sean de producción, como los de laboratorio, durante el tiempo de inactividad programado o durante las pruebas de aceptación de fábrica cuando se tomen las precauciones y los descuidos adecuados antes de instalar un

sistema. Sin embargo, dichas pruebas deben realizarse periódicamente, ya que las configuraciones del sistema cambian, se descubren nuevas vulnerabilidades, surgen nuevas amenazas y evolucionan las herramientas y las metodologías de prueba.

Al analizar los sistemas de producción, se recomienda utilizar evaluaciones de seguridad que no sean intrusivas.

Estas evaluaciones pueden realizarse en papel, utilizar la enumeración pasiva de los detalles del sistema y la red, o cualquier otra actividad que no afecte la seguridad, la disponibilidad y el rendimiento del entorno ICS.

CAPÍTULO 10 Conclusiones

La ausencia de un marco normativo reconocido que contemple controles efectivos sobre los sistemas de control industrial, sumado a las vulnerabilidades y amenazas expuestas en este trabajo, así como la creciente necesidad de integrar la tecnología a todos los procesos industriales, plantean un escenario de alto riesgo para las organizaciones y los Estados.

Efectivamente, muchos de estos sistemas conforman infraestructuras críticas que deben ser protegidas tanto a nivel organizacional como nacional. Esto es así ya que estas situaciones no solo afectan a los intereses propios de las organizaciones, sino también pueden tener efectos en cascada y comprometer negativamente a una parte importante de la población de un país o región.

Es fundamental que tanto el sector público como el privado, trabajen coordinadamente y comprendan la necesidad de crear un marco que regule estas infraestructuras. Para abordar esta problemática de manera proactiva, se requiere establecer regulaciones y controles que contribuyan a mejorar la seguridad y requerir una mayor responsabilidad en materia de ciberseguridad por parte de las organizaciones.

Afrontar la ciberseguridad industrial implica enfrentar un gran desafío que requiere conocimiento especializado y multidisciplinario. Si bien como se mencionó, existen diferencias de enfoque y características entre IT y OT, es importante destacar que existe una tendencia de integración entre estos dos entornos.

Es de vital importancia llevar a cabo una campaña de concientización que llegue a todo el personal de la organización, comenzando por los niveles directivos que deben comprender los riesgos para luego tomar las medidas necesarias.

De acuerdo con los distintos estándares y normas estudiados en este trabajo, se hace hincapié a continuación en algunos puntos en común que resultan importantes para hacer foco en la protección de los entornos industriales.

- Crear un marco adecuado para el gobierno de ciberseguridad
- Definir políticas y procedimientos de ciberseguridad para entornos industriales
- Establecer roles y responsabilidades
- Priorizar y gestionar el ciberriesgo
- Concientizar y capacitar al personal técnico y no técnico
- Realizar inventarios de activos
- Gestionar backups, verificando que sea posible una adecuada restauración
- Gestionar usuarios y privilegios, con base al establecimiento de privilegios mínimos
- Realizar configuraciones de seguridad en dispositivos (hardening)
- Segmentar las redes, en base a niveles de seguridad
- Recolectar y analizar logs para detectar anomalías en tiempo real
- Actualizar parches de seguridad
- Asegurar la seguridad en la cadena de suministros
- Ser ciberresiliente, gestionar y responder a incidentes

Los sistemas son cada vez más complejos, la tecnología atraviesa a todos los procesos de una organización y todos los días se descubren vulnerabilidades nuevas. La seguridad no es un objetivo que se pueda lograr al 100% y en términos absolutos, es imposible de alcanzar.

Por lo tanto, debe ser vista como un proceso vivo y continuo que requiere de un gran esfuerzo y compromiso de todos los involucrados, con el fin de contener los daños y lograr una rápida recuperación. El objetivo será

entonces lograr sistemas OT resilientes, que permitan continuar las operaciones en el menor tiempo posible y con la menor afectación de los procesos considerados críticos.

Abreviaturas y acrónimos

CIA	Confidencialidad, Integridad y Disponibilidad
DCS	Sistema de control distribuido
CMMI	Capability Maturity Model Integration
CSIRT	Equipo de Respuesta a Incidentes de Seguridad
CSMS	Sistema de gestión de ciberseguridad
DMZ	Zona desmilitarizada
FR	Requisito fundamental
IACS	Sistema de Automatización y Control Industrial
ICS	Sistema de Control Industrial
IDS	Sistema de Detección de Intrusos
IT	Tecnologia de la información
KPI	Indicadores claves de rendimiento
OT	Tecnologia operativa
RACI:	Matriz de asignación de responsabilidades
RBAC:	Control de acceso basado en roles
RS:	Requisitos del sistema
RE:	Requisitos de mejora
SCADA	Supervisión control adquisición de datos
SL	Nivel de seguridad
SL-A	Nivel de seguridad alcanzado
SL-C	Nivel de seguridad nativo de la capacidad
SL-T	Nivel de seguridad objetivo

Organismos

ANSI (Instituto Americano de Estándares Nacionales)

APEC (Asia-Pacific Economic Cooperation)

ARPEL: Asociación de empresas de petróleo, Gas y Energia Renovable de América Latina y el Caribe

CISA: Cibersecurity & Infrastructure Security Agency

ENISA (European Network and Information Security Agency)

IAPG: Instituto Argentino del petróleo y del Gas

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

IEC (International Electrotechnical Commission)

ISA (Sociedad Internacional de automatización)

LACNIC (Latin America & Caribbean Network Information Centre)

NIST (National Institute of Standards and Technology)

NERC: (North American Electric Reliabiulity Corporation)

OEA (Organización de Estados Americanos)

UIT (Unión Internacional de Telecomunicaciones)

Normas – Publicaciones

- CIS Critical Security Controls. Guía de implementación de sistemas de control industrial Ver. 7
- ISA/IEC 62443 - Standard specifies security capabilities for control system components
- ISO/IEC 27000
- NIST 800-82r3. Guide to operational Technology (OT) Security

Bibliografía

[1] NIST, «NIST 800-82 Guía de Control Industrial,» [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf. [Último acceso: 20 08 2022].

[2] NIST V1.1, «Framework for Improving Critical Infrastructure Cybersecurity,» 2018.

[3] SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, «Resolución 1523/2019,» de DEFINICION DE INFRAESTRUCTURAS CRITICAS, 2019, pp. http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/norma.htm.

[4] Comision de las comunidades Europeas, «Libro Verde sobre un programa Europeo para la proteccion de infraestructuras criticas,» Bruselas, 2005.

[5] VERTIV - JEAN-BAPTISTE TROLLÉ, «Investigacion de las industrias mas criticas del miundo».

[6] BID - OEA, «Reporte Ciberseguridad 2020 America Latina y el Caribe».

[7] Agencia Federal para la Seguridad Digital – BSI), «The State of IT Security in Germany in 2019».

[8] K. Hemsley y R. Fisher, A History of Cyber Incidents and Threats Involving Industrial Control Systems, 2018.

[9] ITS, «Sistemas de Control Industrial (ICS),» 2018. [En línea]. Available: www.its-security.es.

[10] Panda Security, «Infraestructuras Criticas,» [En línea]. Available: https://www.pandasecurity.com/es/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf. [Último acceso: 27 08 2022].

[11] ISA, «Ukrainian power grids cyberattack,» 2017. [En línea]. Available: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack. [Último acceso: 27 08 2022].

[12] The Times of Israel, «Autoridad Eléctrica de Israel golpeada por ciberataque 'grave',» 26 01 2016.

[13] M. Egan, «El ciberataque a un oleoducto de Estados Unidos es un 'llamado de atención' para el país,» cnn espanol, Mayo 2021.

[14] «CISA Cybersecurity & Infrastructure Security Agency,» 08 07 202. [En línea]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a. [Último acceso: 03 07 2023].

[15] J. R. a. W. Turton, «Bloomberg,» 08 05 2021. [En línea]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown#xj4y7vzkg. [Último acceso: 03 07 2023].

[16] L. Tung, «Ransomware: Meat firm JBS says it paid out $11m after attack,» zdnet, June 10, 2021.

[17] «TGS logra controlar un ciberataque contra el sistema de gestión virtual de su red de gasoductos,» Econo Journal, abril 2022.

[18] Kaspersky ICS CERT, «H2 2022 - brief overview of main incidents in industrial cybersecurity,» 2023.

[19] ISA/IEC, «62443 - Standard specifies security capabilities for control system components».

[20] J. Ing. Castillo y G. Ing. Gonzalez, «Evaluacion de Ciberriesgos segun IEC 62443,» 2023.

[21] M. García, «Dreamlab Technologies,» 08 06 2022. [En línea]. Available: https://dreamlab.net/es/blog/entrada/la-norma-iec-62443-para-la-ciberseguridad-industria/. [Último acceso: 06 06 2023].

[22] Ing.Javier F. Castillo, «Estableciendo zonas y conductos ISA99/IEC62443,» 2018.

[23] Fortinet, «Informe del estado de la tecnología 2023,» 2023.

[24] C. C. f. I. Security, «CIS Controls Guia de implementacion de sistemas de control industrial Ver. 7,» 2018.