CENTRO DE CIBERSEGURIDAD INDUSTRIAL

*Serie de cuadernos CCI. Número 1*

# ESTABLECIENDO ZONAS Y CONDUCTOS

## Según el estándar ISA99/IEC6443

## Consejos

Alt+flecha izquierda para volver a la vista anterior después de ir a un hipervínculo

Haz click en nuestro icono  y visita nuestra web

Haciendo click en la banderas de la portada podrás ver la actividad de CCI en cada uno de esos países

# Patrocinadores del CCI

## Platinum

Eleven Paths

Telefónica

iHackLabs

## Gold

Check Point Software Technologies Ltd.

Cisco

InnoTec System

Entelgy

Fortinet

paloalto Networks

## Silver

Accenture Security

Capsa Food

dimension data

CMC

Eulen Seguridad

Kaspersky Lab

S21sec

Siemens

Tecnicas Reunidas

Trend Micro

TSK Grupo

TÜViT TÜV Nord Group

## Bronze

axians

Atos

Getronics

everis

gmv

Intermark it

Logitek

minsait by Indra

Nozomi Networks

oylo Trust Engineering

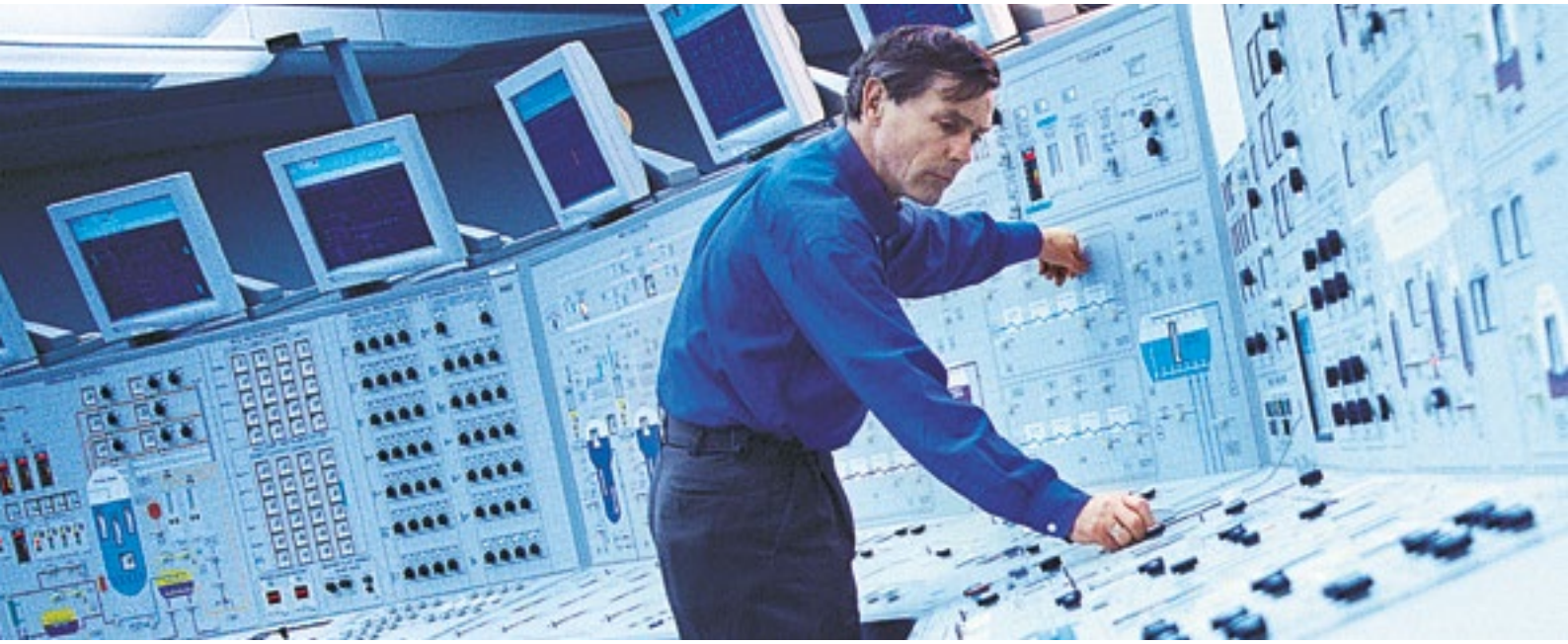
Phoenix Contact

S2 Grupo

sia

tecnalia Inspiring Business

Westcon Comstor Delivering Results Together



Edición: julio 2018
ISBN: El ISBN es 978-84-947727-4-0

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puntales del estado del bienestar.

El CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

Maiquez, 18 · 28009 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI

# Tabla de contenidos

Profesional experto en Ciberseguridad Industrial con experiencia de trabajo demostrable en la industria de Oil & Gas y Energía Eléctrica. Habilidades en Procesos de Negocio, Enterprise Risk Management, Auditoria Interna, Metodología ITIL, Normas y estándares ISO 27001, ISA99/IEC62443, NERC-CIP, AGA, TSA y NIST800-82 entre otras. Profesional de la ingeniería con múltiples certificaciones internacionales en redes industriales, ciberseguridad industrial y análisis de riesgos entre las que se destacan "Cisco Industrial Networking Specialist", "IoT Industry Expert Systems Engineer Representative", "ISA99/IEC 62443 Cybersecurity Fundamentals Specialist", "ISA99/IEC 62443 Cybersecurity Risk Assessment Specialist" y "CSSA Certified SCADA Security Architect" otorgada por el "Information Assurance Certification Review Board". Desde 2016 se encuentra como "Information Member of ISA99/IEC62443 Committee" dentro de los grupos de trabajo "WG2 - Focusing on the description of an effective cyber security management system in the ISA-62443-2-1 standard Security Management System)", "WG3 - Preparing of a second edition of the ISA-62443-1-1 standard (Models and Concepts)" y "WG4 TG3 - Working on the standard ISA-62443-3-2 (Security Risk Assessment and System Design)". Adicionalmente, desde 2018 participa como representante técnico dentro de ISA-Secure para una de las principales petroleras de la República Argentina.

Miembro activo del ecosistema del Centro de Ciberseguridad Industrial (CCI) de España desde 2015 participando como revisor y colaborador en la publicación de documentos realizados por este.

Autor
Ing.Javier F. Castillo

Ingeniero en Computación, Facultad de Ciencias Exactas y Tecnología,
Universidad Nacional de Tucumán, República Argentina.

# 1

# Prólogo

El análisis de los riesgos tecnológicos es una herramienta, como lo son las evaluaciones técnicas, las evaluciones de capacidad o el análisis de los incidentes, que nos ayudan a establecer o actualizar nuestro programa de ciberseguridad.

Es importante basarse en herramientas “ágiles” que permitan tomar mejores decisiones para proteger y dar respuesta a los incidentes en un entorno tan cambiante como el tecnológico, especialmente en los entornos industriales, donde la integración entre las tecnologías de información (IT) y las tecnologías de operación (OT), que es imprescindible para las actuales necesidades del negocio, provocan un mayor nivel de exposición, puntos de fallo y actores en la cadena de valor.

La aproximación basada en zonas, conductos y niveles de seguridad de IEC62443 permite establecer una base de protección de los sistemas operación e información del entorno industrial de una forma “ágil”, pero sobre todo proporciona un lenguaje común entre los propietarios, los integradores y fabricantes de tecnología a la hora de establecer los requisitos de protección en un entorno de automatización y control industrial.

En este excelente documento, escrito por el ingeniero Javier F. Castillo, podrá encontrar como deben establecerse las zonas y conductos para un alcance determinado, de forma ordenada, didáctica y práctica. También en el mismo se explica como establecer los niveles de seguridad, en la escala de 5 valores, que establece IEC62443, así como los requisitos de cada uno de los niveles agrupados en los siete requisitos fundamentales de ciberseguridad.

Este es el primer cuaderno, de esta nueva serie de cuadernos CCI, que tiene como objetivo cubrir aspectos específicos de la ciberseguridad industrial de forma didáctica y práctica, basándose en la experiencia de profesionales, como es en este caso, Javier F. Castillo, que ha decidido compartir este documento.

José Valiente

Director de CCI

# 2

# Introducción

La industria en general y, particularmente la comúnmente llamada industria 4.0, presenta múltiples desafíos entre los cuales la Ciberseguridad Industrial aparece como tópico principal a tener en cuenta para acompañar la evolución tecnología de los procesos industriales. Saber dónde y cuándo realizar inversiones en Ciberseguridad Industrial puede resultar en una ventaja competitiva para aquellas empresas que busquen obtener mayor disponibilidad, calidad y rendiemiento, pudiendo así mejorar la eficiencia en sus procesos de negocio o bien dar cumplimiento a regulaciones propias del mercado al que pertenecen.

¿Qué es industria 4.0? La industria 4.0 consiste en el aprovechamiento de la digitalización de los procesos industriales mediante la utilización cada vez más frecuente de sensores y actuadores que avanzan en la incorporación de tecnologías "digitalmente inteligentes" y sistemas de información complementarios que permiten transformar los procesos productivos y volverlos más eficientes.

El siguiente gráfico muestra de manera muy clara la evolución de la automatización industrial desde la incorporación de equipamiento mecánicos a los procesos industriales hasta la hoy conocida como cuarta revolución industrial donde los sistemas ciber-físicos cobran un rol protagonista y diferencial para mejorar la gestión y eficiencia en procesos industriales.

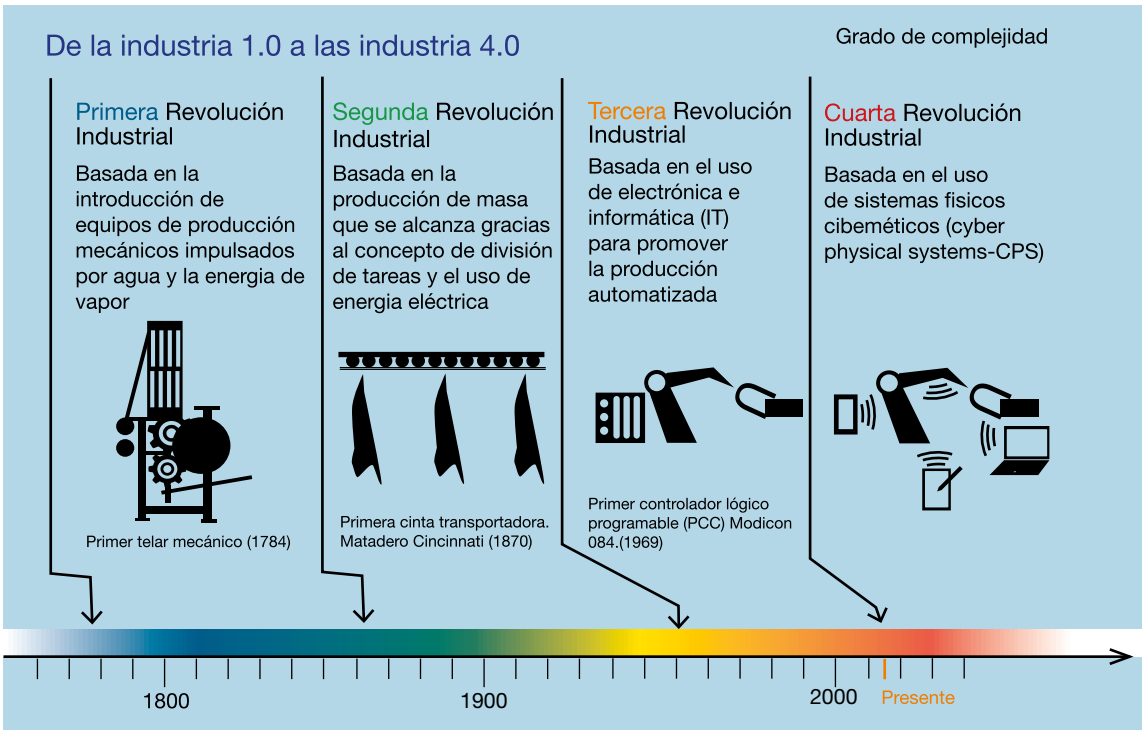



Figura 1. Evolución de la automatización industrial

Como todo programa de Ciberseguridad, el punto de partida para empezar a gestionar esta problemática consiste en llevar adelante un análisis de riesgos. Al plantearnos este objetivo surge la siguiente pregunta: ¿Qué es lo que vamos a analizar? Cada industria en particular presenta características propias que nos inclinan a evaluar diferentes elementos según el nivel de detalle que se busque obtener. Por ejemplo, en la industria de Oil & Gas, una refinería comprende múltiples procesos (separación, transformación, purificación etc.) mediante los cuales el petróleo crudo es convertido en diversos productos terminados. Dentro de cada uno de estos procesos intervienen más de un sistema industrial y, a su vez, estos están compuestos por una gran variedad de componentes (sensores, actuadores, PLCs, RTUs, HMIs etc.). Podemos entonces optar por analizar un proceso, un subproceso, un sistema industrial o bien cada uno de sus componentes. Todo un desafío…

El estándar ISA99/IEC62443 constituye el principal marco de referencia internacional de ciberseguridad en sistemas industriales donde la disponibilidad y la integridad son los factores más importantes para la adopción de medidas de protección contra ciberamenazas, pero también para reducir los incidentes tecnológicos no intencionados. El comité ISA99 que desarrollo inicialmente el esquema IEC62443 está compuesto por una serie de miembros donde se encuentran propietarios (owners), proveedores de equipamiento y servicios (fabricantes e integradores), gobiernos, instituciones educativas y diferentes grupos de investigación.

Como todo programa de Ciberseguridad, el punto de partida para empezar a gestionar esta problemática consiste es llevar adelante un análisis de riesgos. Al plantearnos este objetivo surge la siguiente pregunta: ¿Qué es lo que vamos a analizar? Cada industria en particular presenta características propias que nos inclinan a evaluar diferentes elementos según el nivel de detalle que se busque obtener. Por ejemplo, en la industria de Oil & Gas, una refinería comprende múltiples procesos (separación, transformación, purificación etc.) mediante los cuales el petróleo crudo es convertido en diversos productos terminados. Dentro de cada uno de estos procesos intervienen más de un sistema industrial y, a su vez, estos están compuestos por una gran variedad de componentes (sensores, actuadores, PLCs, RTUs, HMIs etc.). Podemos entonces optar por analizar un proceso, un subproceso, un sistema industrial o bien cada uno de sus componentes. Todo un desafío…

El estándar ISA99/IEC62443 constituye el principal marco de referencia internacional de ciberseguridad en sistemas industriales donde la disponibilidad y la integridad son los factores más importantes para la adopción de medidas de protección contra ciberamenazas, pero también para reducir los incidentes tecnológicos no intencionados. El comité ISA99 que desarrollo inicialmente el esquema IEC62443 está compuesto por una serie de miembros donde se encuentran propietarios (owners), proveedores de equipamiento y servicios (fabricantes e integradores), gobiernos, instituciones educativas y diferentes grupos de investigación.

Según este estándar, el ciclo de vida de Ciberseguridad Industrial consta de tres fases: Evaluación, Desarrollo & Implementación y Mantenimiento.

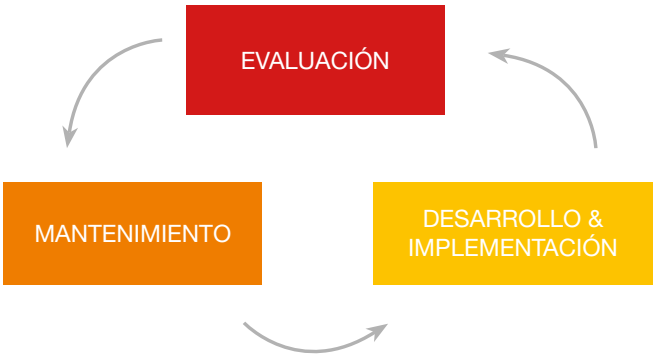



Figura 2. Ciclo de vidad de Ciberseguridad Industrial

Cada una de estas fases conforman la metodología propuesta por el estándar para la protección de los sistemas industriales contra incidentes intencionados o no. Al referirnos a este ciclo de vida en este rubro es indispensable comprender que en ciberseguridad no existe un estado de seguridad “garantizada” sino que cada una de estas fases se debe realizar de manera iterativa nutriéndose de la fase anterior y agregando valor a la siguiente. De esta manera, podremos mejorar las contramedidas implementadas hasta lograr alcanzar un nivel de riesgo tolerable.

Como punto de partida, el estándar propone identificar con claridad el “Sistema bajo Consideración” (SuC – “System under Consideration”) el cual consiste en la infraestructura completa que será objeto del análisis. Puede incluir redes de control, tele supervisión, infraestructura de comunicaciones y seguridad (Routers/Firewall) e incluso incorporar redes informáticas dependiendo de los servicios que estas brinden al proceso industrial y viceversa. Una vez identificado el SuC, se da inicio a la fase de “Evaluación” dentro de la cual se encuentra la etapa “Asignar activos a Zonas & Conductos” - (ver figura 6). En este documento nos concentraremos en dicha etapa dejando para posteriores publicaciones lo relacionado a análisis de riesgos.

La importancia de esta definición radica en la premisa de que cada escenario particular posee diferentes niveles de seguridad asociados al riesgo tolerable por cada Organización.

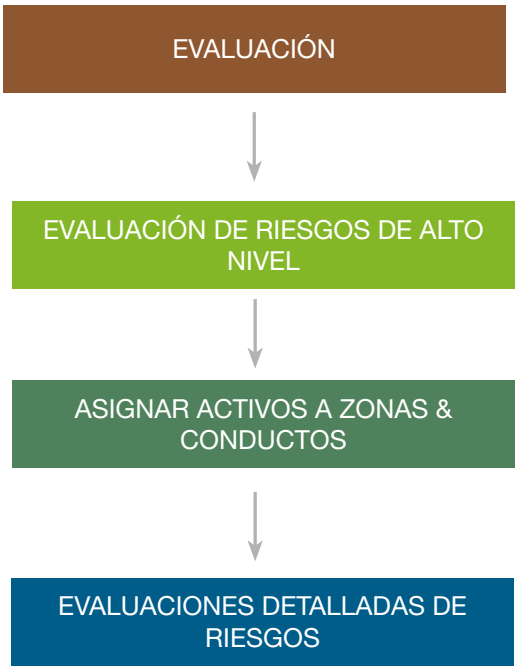



Figura 3. Fase de Evaluación.

Para sistemas industriales de gran envergadura o complejos quizás no sea recomendable o necesario aplicar el mismo nivel de seguridad a todos sus componentes. Es por ello que se crean los conceptos de Zona y Conducto los cuales deber ser identificados dentro del SuC.

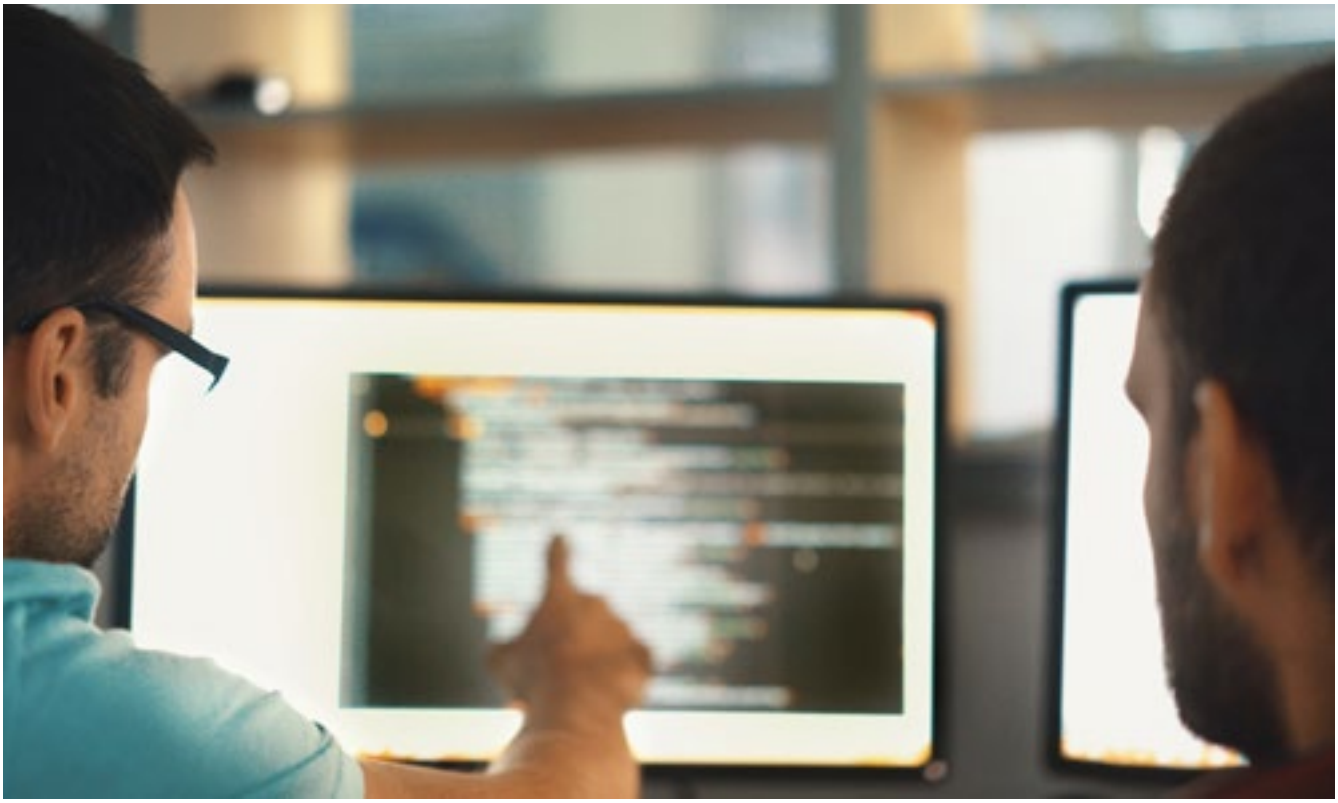
Una Zona se define como la agrupación lógica o física de activos industriales (dichos activos puedes ser físicos, aplicaciones o información) los cuales comparten los mismos requisitos de seguridad.

Un Conducto es un tipo particular de zona que agrupa las comunicaciones que permiten transmitir información entre diferentes zonas.

Por último, se agrega el concepto de Canal el cual se define como un determinado vínculo de comunicación establecido dentro de un conducto

El objetivo de la Ciberseguridad industrial es brindar al SuC dos conceptos claves: Robustez y Resiliencia.

El concepto de Robustez otorga la capacidad de operar frente a un determinado nivel de perturbaciones producidas por ciberamenazas y la Resiliencia es la capacidad de restablecer o restaurar el sistema luego de producido un evento no deseado, con el mínimo impacto posible acorde a los riesgos tolerables definidos por la Organización.



# 3

# Zonas y conductos

# 3.1. ZONAS

Durante la creación de un programa de Ciberseguridad, el concepto de "zonas" constituye uno de los recursos más importantes y su definición es uno de los aspectos fundamentales para el éxito de este proceso.

Las zonas pueden ser una agrupación de activos independientes, un grupo de subzonas o una combinación de ambos. A su vez, las zonas poseen atributos de herencia, lo cual significa que las zonas "hijas" (o subzonas) deben cumplir con todos los requisitos de seguridad de su zona "padre". Cuando nos referimos a activos, hacemos alusión a "activos necesarios para el proceso industrial" lo cual definiremos como "todo elemento perteneciente a un sistema industrial (PLCs, RTUs, estaciones de operación e ingeniería, equipamiento de comunicaciones etc.) que tiene valor o potencial valor para una organización". Las cotas en el valor a partir de cuándo un elemento es considerado activo varían dependiendo de las organizaciones y su magnitud.

Cada zona posee un conjunto de características y requisitos de seguridad que constituyen sus atributos:

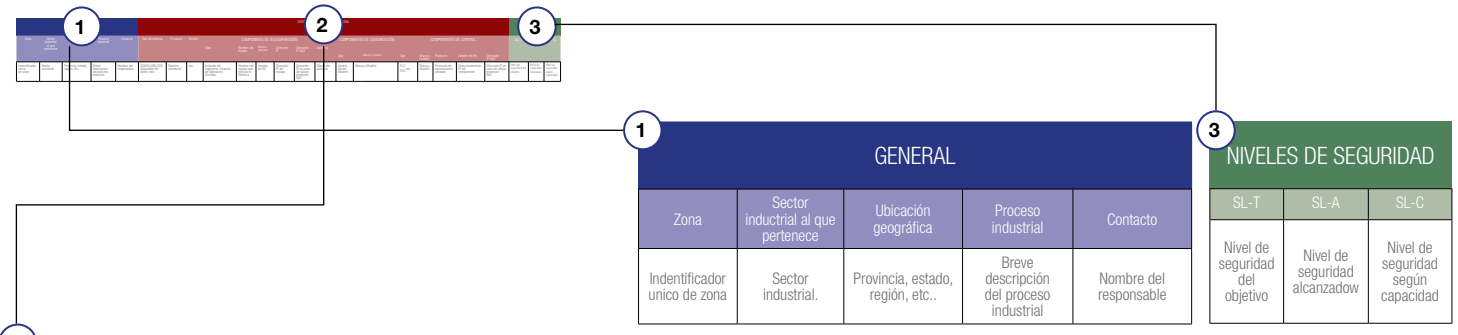
- Políticas de seguridad y niveles de seguridad
- Inventario de activos
- Requisitos de acceso y controles
- Amenazas y vulnerabilidades
- Consecuencias de una brecha de seguridad
- Tecnología autorizada
- Proceso de gestión de cambios.

Cada zona definida debe contener un documento que describa sus requisitos de seguridad y como asegurar que los niveles de riesgos tolerables son alcanzados. Este documento debe incluir, entre otros, el alcance de la zona, su nivel de seguridad, la estructura organizacional a la cual pertenece y sus responsabilidades, los riesgos asociados a la zona, la estrategia de seguridad adoptada, los tipos de actividades que son permitidas dentro de ella etc. Toda esta información debe estar documentada para cada zona ya que sirve como guía para la construcción y el mantenimiento de los activos contenidos en ella.

Con respecto al inventario de activos, este constituye un factor determinante para podes alcanzar los objetivos definidos en la política de seguridad. Se debe crear un documento que detalle todos aquellos activos, lógicos y físicos, que forman parte de la zona. Se incluye en este documento un ejemplo de matriz de activos (a modo de guía) que facilite la definición una zona así como también, con algunos cambios menores, cataloga los sistemas industriales asociados a un proceso industrial.

Si bien, la obtención de la información detallada en la "matriz guía" suele requerir un esfuerzo inicial significativo, debe realizarse con el mayor detalle posible, ya que como se ha mencionado anteriormente constituye un elemento fundamental a la hora de crear un programa de ciberseguridad industrial. Además, debido a la naturaleza de los sistemas industriales, es conocido que su ciclo de vida está en el rango de entre 15 y 20 años, con lo cual se espera una fuerte carga inicial, y escasas modificaciones durante periodos prolongados de tiempo. Como complemento mencionaremos que actualmente existen herramientas automáticas que, si bien no fueron

Tabla 1. Ejemplo de inventario de activos Zona



diseñadas para cumplir específicamente con este requisito, agilizan mucho su ejecución.

Al definir una zona, claramente estamos acotando un determinado segmento dentro del sistema y/o proceso industrial, y como consecuencia debería existir un número reducido de requisitos y medios para obtener acceso a la misma. Una política de acceso debe establecer con precisión el personal que está autorizado para acceder a cada zona, los medios a través de los cuales se realiza el acceso y los mecanismos de control sobre los mismos. Es aquí donde cobra importancia el concepto de conducto el cual desarrollaremos más adelante en este documento.

Una zona posee sus propias vulnerabilidades, y se encuentra expuesta a un determinado número de amenazas. Es por ello que realizar un análisis de vulnerabilidades periódicamente sobre ellas (o sobre el proceso industrial completo) resulta de vital importancia para identificar potenciales amenazas que provoquen que los activos industriales no cumplan con sus objetivos de negocio.

Los sistemas industriales, en general, deben acompañar los cambios en las necesidades y reglas de negocio a los que pertenecen. Estos cambios pueden impactar en las diferentes zonas identificadas a partir de la incorporación de nuevas tecnologías, necesidades extras de acceso, creación de nuevos conductos, entre otros. Resulta por ello imprescindible contar con mecanismos de control de cambios que permitan asegurar que cualquier modificación relacionada con una zona no altere los niveles de seguridad requeridos para ella.

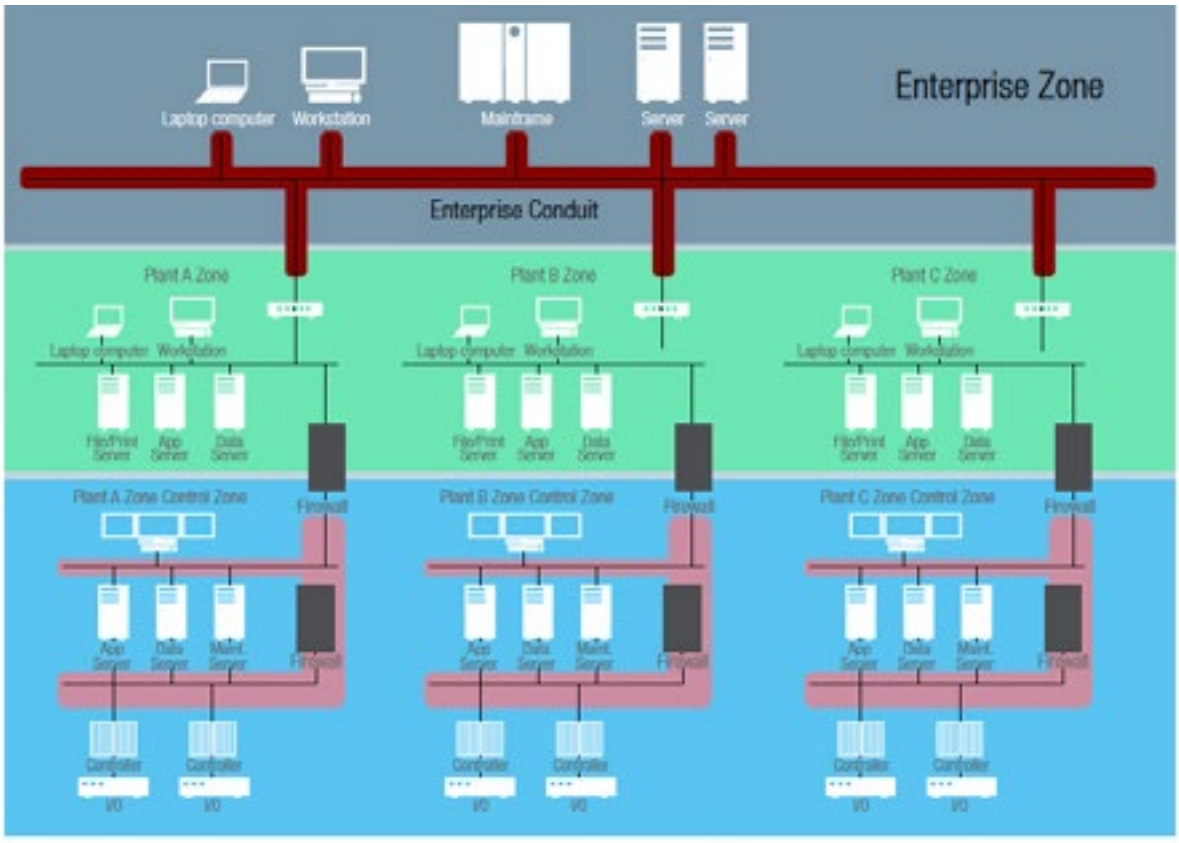



Figura 4 – Ejemplo de Zonas
Fuente: ISA99/IEC62443-1-1

# 3.2. CONDUCTOS

Los “conductos” son zonas particulares que se aplican a procesos de comunicación específicos proporcionando funciones de seguridad que permiten a dos zonas comunicarse de manera segura. Toda comunicación entre diferentes zonas ha de realizarse a través de un conducto.

Al igual que una zona, los conductos constituyen una agrupación lógica y/o física de activos (activos de comunicación en este caso). Un “conducto de seguridad” protege la seguridad de los canales que éste contiene, de la misma manera que un conducto físico protege los cables de daños físicos.

Los conductos pueden ser pensados como los “tubos” que unen diferentes zonas o bien que son utilizados para unir componentes dentro de una misma zona. Ya sea internos (dentro de una zona) o externos (fuera de una zona) los conductos protegen los canales que proveen vínculos de comunicación entre activos industriales. Generalmente en los sistemas industriales, los conductos constituyen dispositivos de red (switches, routers, firewalls etc.) que forman parte de su arquitectura, pero en algunos casos también se pueden presentar como servidores o Gateway de comunicaciones utilizados para la conversión de diferentes protocolos.

Los conductos se utilizan como uno de los principales “inputs” para determinar las amenazas a las cuales se encuentra expuesta una zona. Identificando con claridad los conductos podremos conocer cuáles son los puntos de acceso que la zona posee, y analizar si pueden convertirse en un potencial vector de ataque. Un análisis de riesgos detallado debe incluir tanto las zonas, como sus conductos asociados para obtener mejores resultados.

Al ser un tipo particular de zona, de la misma manera que ellas cada conducto posee un conjunto de características y requisitos de seguridad que constituyen sus atributos.

- Políticas de seguridad y niveles de seguridad
- Inventario de activos
- Requisitos de acceso y controles
- Amenazas y vulnerabilidades
- Consecuencias de una brecha de seguridad
- Tecnología autorizada
- Proceso de gestión de cambios
- Zonas que interconecta

Protocolos de comunicaciones (muy heterogeneo por la naturaleza de cada industria y fabricante).A diferencia de las zonas, los conductos deben incluir el detalle de las diferentes zonas a las cuales interconectan, asegurando que la tecnología utilizada para la creación de canales de comunicación cumple con los requisitos fundamentales de seguridad especificados según el nivel de seguridad asociado. La definición de los diferentes niveles de seguridad y sus requisitos especificos se desarrolla con mayor profundidad en la “Sección 4 – Niveles de Seguridad”.

Al finalizar el análisis de Riesgos tecnológicos propuesto por la IEC-62443 se llegará a la agrupación de Zonas y Conductos óptima, de tal forma que se pueda asegurar el sistema por diseño, logrando los niveles de seguridad objetivo, y de riesgo tolerable para la organización; sin gastar de más, ni invertir de menos. Esta aproximación es valida para sistemas existentes normalmente llamados “base Instalada” o para sistemas nuevos que van cumpliendo con sus diferentes etapas de ingeniería (Ingeniería básica, ingeniería de detalle, diseño, compras, construcción, pruebas, puerta en marcha, operación, mantenimiento, hasta su retiro o decomisionado).

# 3.3. DEFINICIÓN DE REQUISITOS DE ZONAS Y CONDUCTOS

## 3.3.1.Sistema bajo Consideración (SuC)

Como primera medida, la organización deberá definir claramente el "Sistema bajo Consideración" (SuC) incluyendo una clara identificación de sus límites y todos los puntos de acceso a dicho SuC. Esta definición es fundamental ya que constituye la especificación del alcance sobre el cual se trabajará, fijando el nivel de granularidad que impactará directamente en los resultados obtenidos. No se obtendrá el mismo nivel de detalle seleccionando un proceso complejo donde intervienen múltiples sistemas, localizaciones y tecnologías, que segmentando dicho proceso en subprocesos y analizando cada uno de ellos por separado sin dejar de lado las interdependencias que pudieran existir entre los mismos.

Una vez determinado el SuC, se deben establecer las zonas y conductos que sean necesarias agrupando sus activos en base a su funcionalidad, ubicación, organización, responsables, resultados de análisis de riesgos etc. La agrupación de dichos activos debe reflejar claramente los requisitos comunes de seguridad para cada zona y conducto identificado.

## 3.3.2. Diagrama de Zonas y Conductos

Cada organización debe generar diagramas que ilustren la segmentación de zonas y conductos adoptada para el SuC donde se debe asegurar que todos los activos industriales del sistema en cuestión se encuentran asignados a una zona o bien a un conducto.

Para dar cumplimiento a este requisito, el estándar ISA99/IEC62443 propone utilizar como punto de partida el modelo de referencia propuesto dentro de "ANSI/ISA95.00.01-2000 Enterprise-Control System Integration Part 1: Models and Terminology" el cual consiste en un modelo de alto nivel que refleja la integración de sistemas corporativos e industriales.

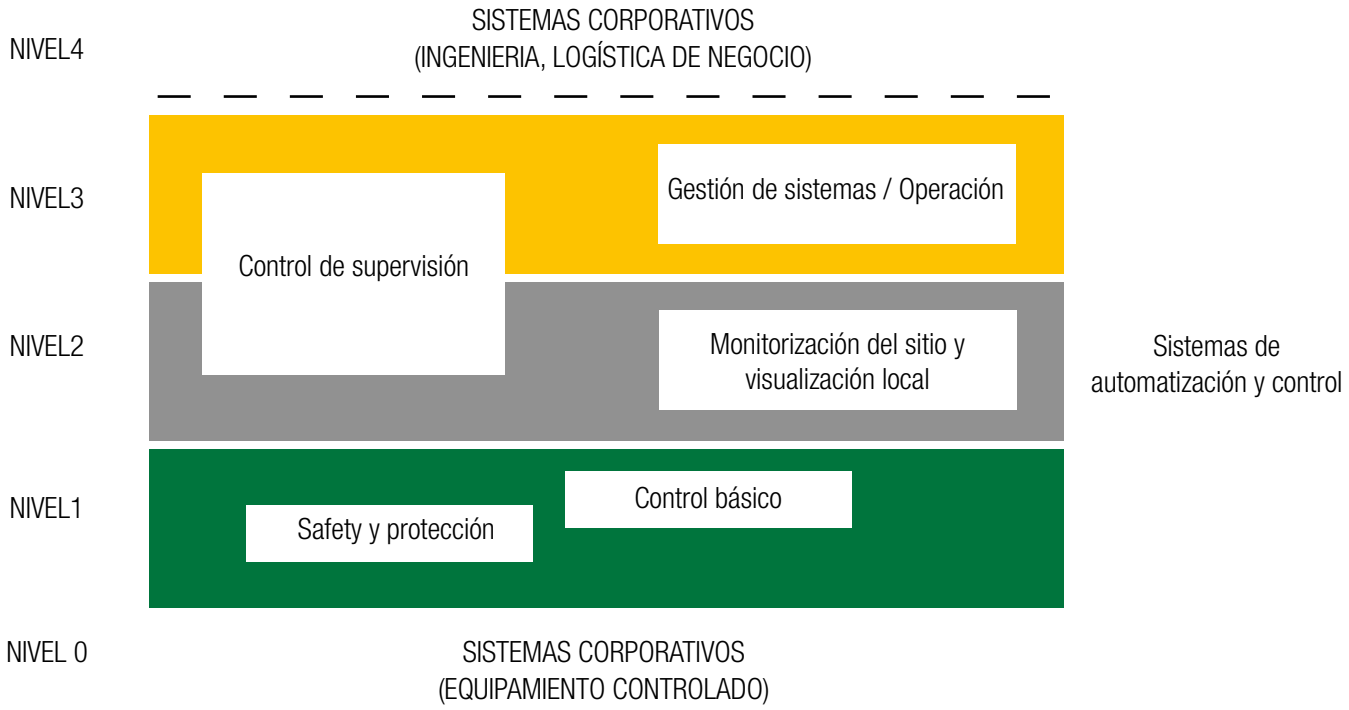



Figura 6. Modelo de alto nivel ISA999/IEC 62443-1-1

El modelo citado consta de cinco niveles los cuales se detallan a continuación;

- Nivel 4: abarca funcionalidades relacionadas a los sistemas corporativos que dan soporte a las necesidades de gestión de cada organización.
- Nivel 3: abarca funciones relacionadas a la gestión de flujos de trabajo destinados a la elaboración del producto final o resultado del proceso industrial.
- Nivel 2: abarca funciones relacionadas a la supervisión y operación de las diferentes áreas de producción involucradas en un proceso industrial.
- Nivel 1: abarca funciones relacionadas con la automatización y el control básico del proceso industrial. (Ej. Discreto, Batch, Continuo)
- Nivel 0: constituye el proceso en cuestión. Incluye los sensores y actuadores conectados directamente al proceso o su equipamiento asociado.

En el momento de comenzar con la tarea de documentar las zonas y conductos, se deberán ubicar todos los activos industriales que intervienen dentro del SuC según lo especificado en el modelo de referencia. Esta primera aproximación permite visualizar de una forma rápida y practica el flujo de datos e información desde los niveles más bajos (sensores y actuadores) hasta los servicios que comparten el ambiente de OT con TI. Una vez modelizado el SuC la agrupación de activos industriales en zonas y conductos debe ser una consecuencia de los criterios anteriormente citados (funcionalidad, ubicación, organización, responsables, resultados de análisis de riesgos etc.) sin perder de vista que el principal foco de este proceso es contribuir a la ejecución de un programa de ciberseguridad, por ello el resultado de la segmentación en zonas y conductos debe están fundamentado principalmente en la identificación de aquellos activos que poseen requisitos comunes de ciberseguridad.

Los siguientes atributos deber ser documentados para cada Zona y Conducto:

1. Nombre e Identificador Único.
2. Límites lógicos.
3. Límites físicos.
4. Listado de todos los puntos de acceso al sistema asociados a los límites y dispositivos.
5. Listado de los Flujos de datos en los puntos de acceso.
6. Zonas y Conductos conectados.
7. Listado de activos asociados y consecuencias (esto último si ya se cuenta con un análisis de riesgos previo).
8. Niveles de seguridad objetivo.
9. Políticas de Seguridad aplicables.
10. Hipótesis de dependencias externas.

## 3.3.3. Criterios iniciales para la separación de Zonas & Conductos

I. Los activos de sistemas de información de negocio (TI) y sistemas de control industrial (OT) deben ser agrupados en Zonas separadas.

Los sistemas de información y los sistemas de control industrial, en condiciones normales, deberán estar en distintas zonas, determinado esto por su funcionalidad, porque la responsabilidad de los mismos recae en diferentes áreas de las organizaciones, determinado por los resultados de análisis de riesgos previos, y habitualmente porque su ubicación es diferente. Resulta importante entender que la principal diferencia entre ambos entornos es que los sistemas de control industrial tienen impacto directo en la salud de las personas y el medio ambiente, además de que pueden afectar a la producción y a la imagen corporativa ente un incidente.

II. Los activos identificados como Sistemas Instrumentados de Seguridad (SIS) deben ser separados en Zonas distintas.

Los Sistemas Instrumentados de Seguridad (SIS) por su naturaleza poseen requisitos de seguridad diferentes a los demás componentes de un sistema de control industrial.

III. Los activos o dispositivos que se conectan temporalmente al SuC deben ser separados en Zonas distintas.

Los dispositivos que eventualmente se conectan al SuC, tales como Notebooks de personal de mantenimiento, dispositivos de análisis de ciberseguridad portátiles (herramientas de análisis de comportamiento en función de captura de trafico de red), dispositivos de almacenamiento USB, entre otros, suelen estar expuestos a un número mucho mayor de amenazas que aquellos que se encuentran permanentemente dentro de una zona. Es por ello que estos dispositivos deben ser modelados en una zona separada. La principal razón es que al ser dispositivos de conexión temporal es muy probable que también se conecten a otras redes fuera de la zona cuyos requisitos de ciberseguridad no alcancen los establecidos para ella.

IV. Las comunicaciones inalámbricas deben ubicarse en una o más zonas separadas de las comunicaciones cableadas.

Las comunicaciones inalámbricas no son controladas por vallados, muros o gabinetes y por lo tanto poseen un mayor nivel de exposición que las comunicaciones cableadas.

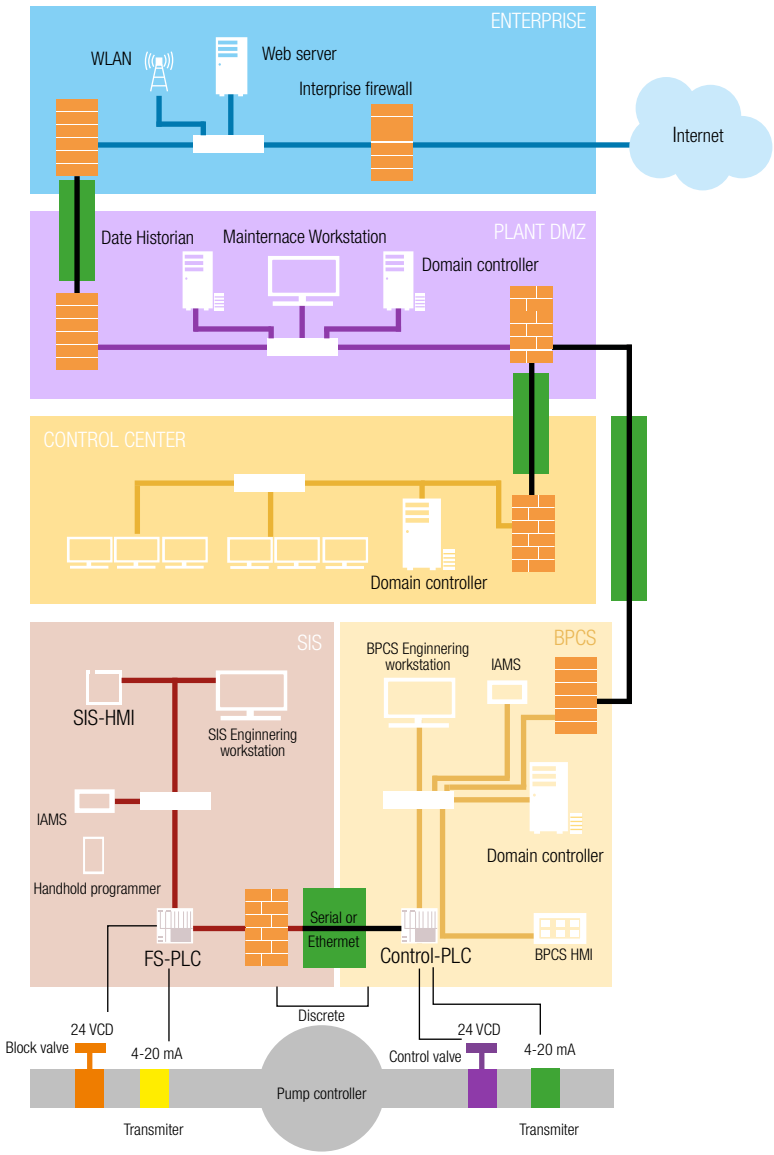



Figura 7 - Modelo de alto nivel para procesos industriales
Fuente: ISA99/IEC62443-1-1

# 3.4. MODELOS DE REFERENCIA

A continuación, se incluyen a modo de ejemplo, y para ayudar en una primera definición de zonas y conductos, los modelos de alto nivel de referencia propuestos por diferentes fuentes:

## 3.4.1. Arquitectura de Referencia de DuPont

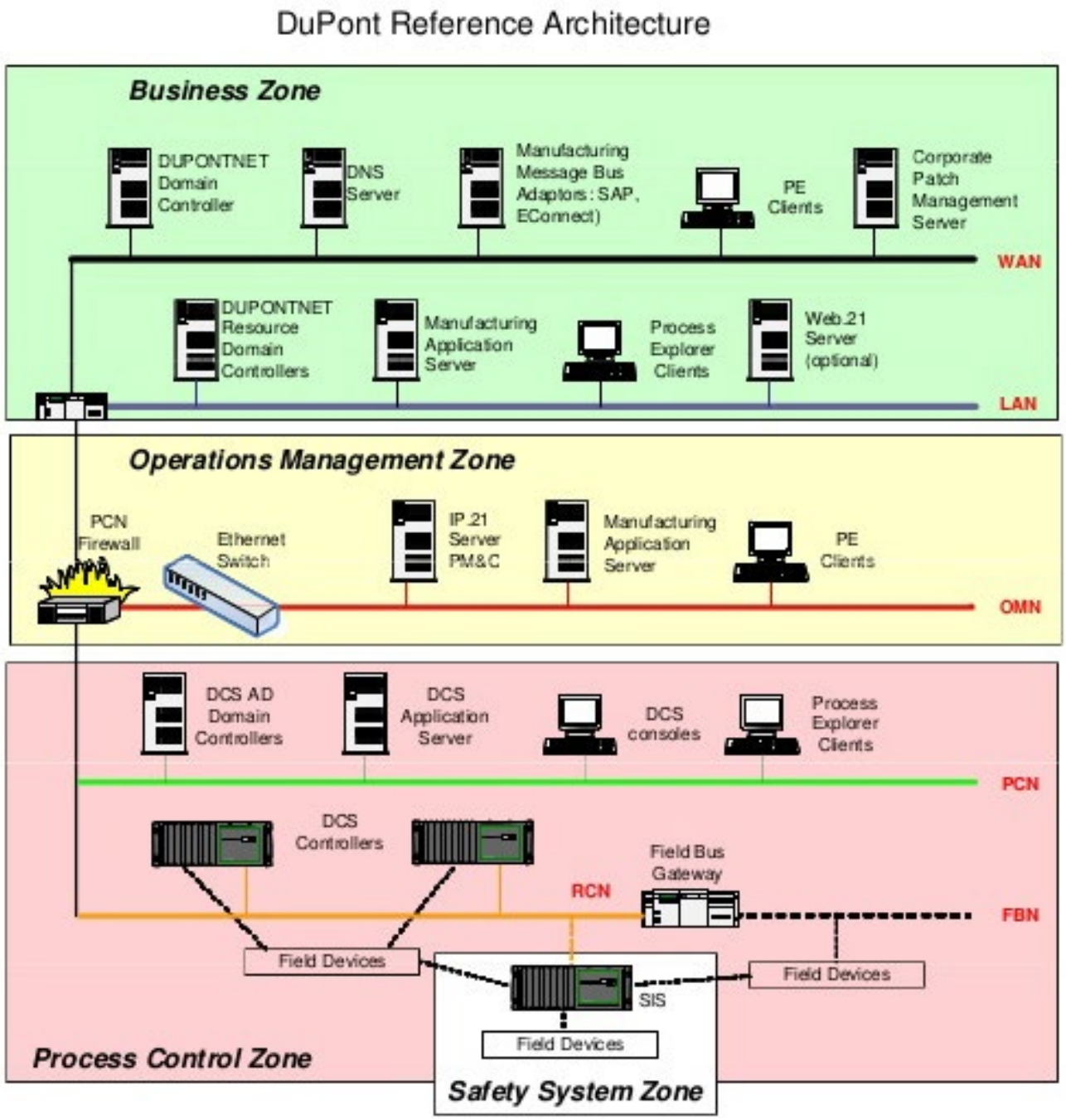



Figura 8. Modelo de alto nivel de Dupont

## 3.4.2. Ejemplo de una Refinería según Tofino Security (a Belden Company)

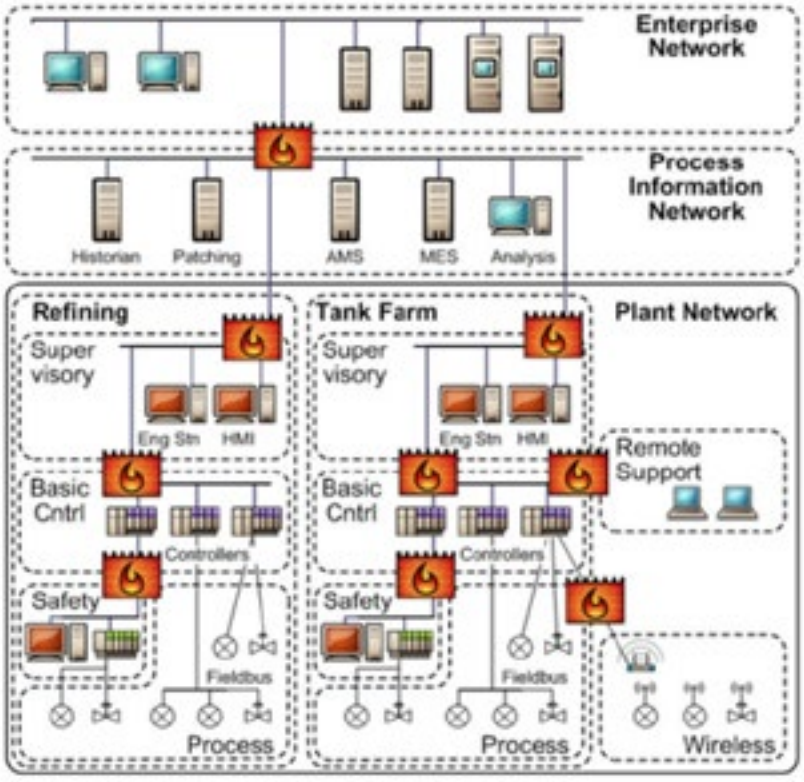



Figura 9. Modelo de alto nivel de Tofino Security

## 3.4.3. Arquitetura de Referencia de Honeywell

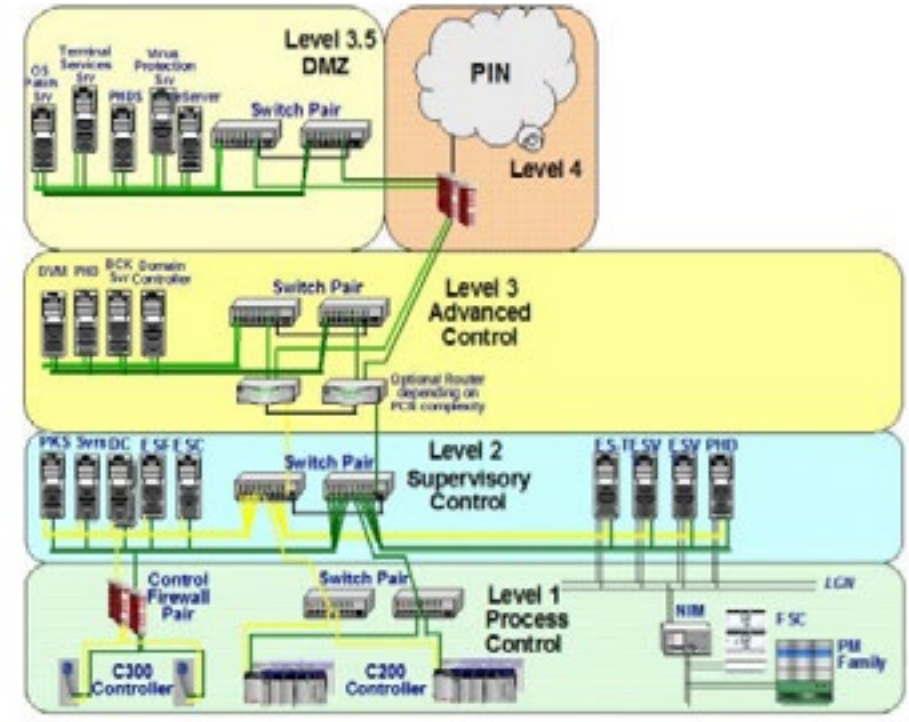



Figura 10. Modelo de alto nivel de Honeywell

## 3.4.4. Arquitectura de referencia de Rockwell

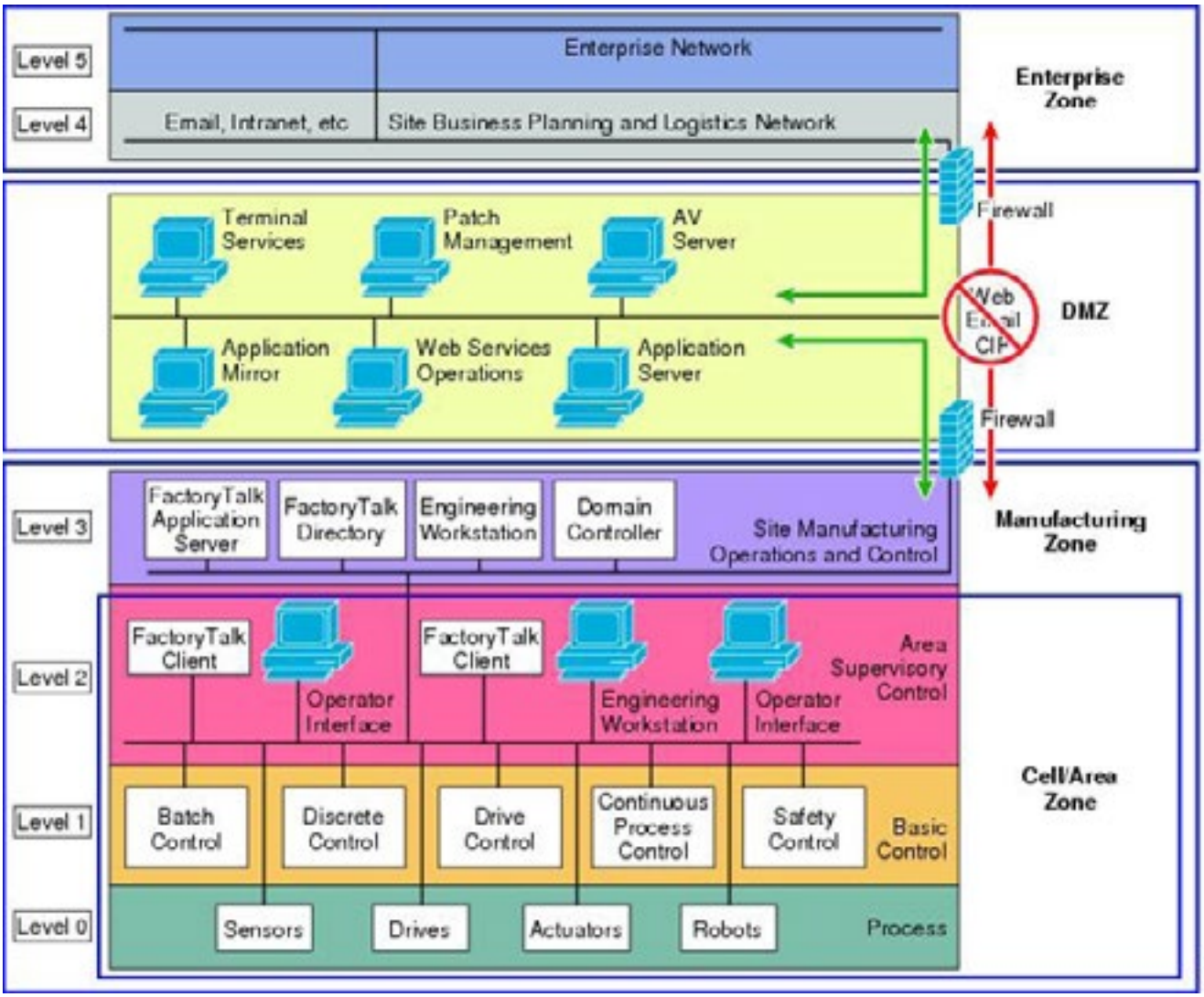



Figura 11. Modelo de alto nivel de Rockwell

## 3.4.5.Arquitetura de referencia de SIEMENS

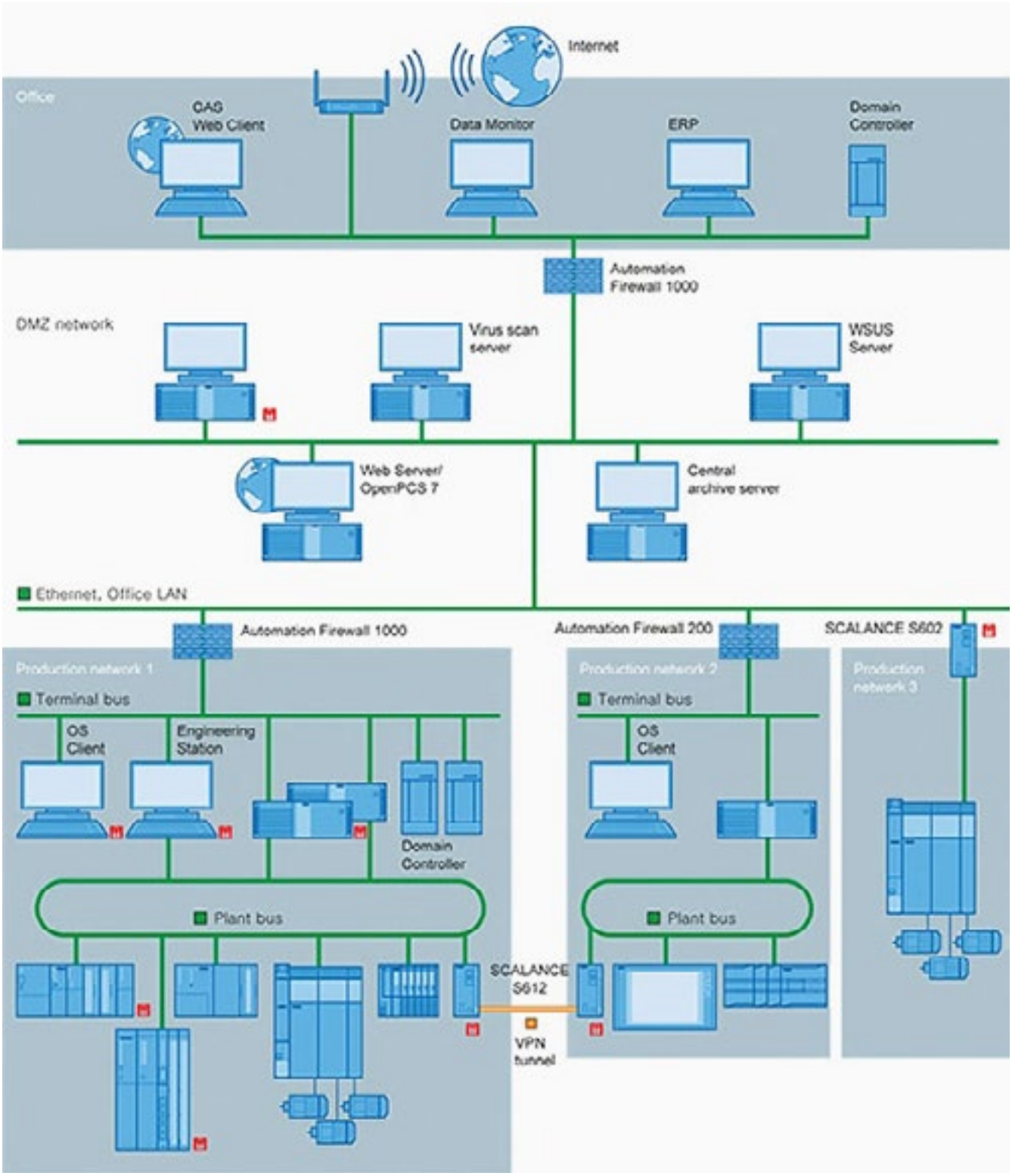



Figura 12. Modelo de alto nivel de SIEMENS

# 4

# Niveles de seguridad

# 4.1. ¿QUÉ SON LOS NIVELES DE SEGURIDAD?

El estándar ISA99/IEC62443 define los niveles de seguridad de la siguiente manera:

*"Los Niveles de Seguridad (SL, por sus siglas en idioma inglés) proveen una aproximación cualitativa para la Ciberseguridad de una determinada zona. Al ser un método cualitativo, la definición de niveles de seguridad sirve para comparar y gestionar la seguridad de diferentes zonas dentro de una organización."*

# 4.2. TIPOS DE NIVELES DE SEGURIDAD

Según el estándar es necesaria la identificación de tres tipos diferentes de niveles de seguridad:

- Nivel de Seguridad Objetivo (SL-T): Es el nivel de seguridad deseado para un sistema particular. Es determinado usualmente a través de la realización de evaluaciones de riesgos las cuales determinan un nivel de seguridad particular para asegurar la correcta operación.
- Nivel de Seguridad Alcanzado (SL-A): Es el nivel de seguridad actual para un sistema particular. Éste es medido una vez que el diseño del sistema está disponible o cuando un sistema ya se encuentra instalado. Se utilizan para establecer si la seguridad de un sistema alcanza los niveles definidos según el SL-T.
- Nivel de Seguridad según Capacidad (SL-C): Son los niveles de seguridad que los componentes o sistemas pueden otorgar cuando son configurados apropiadamente. Estos niveles permiten saber si un determinado sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) de forma nativa sin medidas compensatorias o contramedidas adicionales cuando es configurado e integrado apropiadamente.

# 4.3. ¿CÓMO USAR LOS NIVELES DE SEGURIDAD?

Cuando se diseña un nuevo sistema o se analiza la ciberseguridad de uno existente, el primer paso es segmentar dicho sistema en diferentes zonas y definir los conductos que las vinculan.

Una vez establecido el modelo de zonas y conductos, se debe asignar a cada zona y conducto un SL-T (nivel de seguridad objetivo). Una vez determinado el SL-T el sistema puede ser diseñado o rediseñado para alcanzar dicho nivel.

Durante el proceso de diseño o adecuación, es necesario evaluar las capacidades de seguridad de cada componente o subsistema. Los proveedores o integradores del producto deberán proveer dicha información como parte de sus tareas. Esta información es de suma utilidad ya que permite determinar si un componente o sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) deseado. Es probable que en un diseño particular haya algunos componentes o sistemas que no pueden alcanzar el SL-T. En aquellos casos en que el nivel de seguridad según capacidad (SL-C) de estos es menor al deseado como SL-T, se deberán considerar medidas compensatorias o contramedidas para reducir esa brecha. Dichas contramedidas pueden requerir cambios en los diseños e incluso la selección de componentes adicionales. Cada vez que se realice una modificación en los sistemas industriales, su nivel de seguridad debe ser evaluado obteniéndose así el nivel de seguridad alcanzado (SL-A) y comparar el mismo con el SL-T).

La siguiente figura muestra este proceso:


Figura 13 – ¿Cómo utilizar los Niveles de seguridad?
Fuente: ISA99/IEC62443-3-3

# 4.4. VECTOR DE NIVELES DE SEGURIDAD

## 4.4.1. Requisitos fundamentales de ciberseguridad.

Los Niveles de Seguridad se encuentran basados en los siete requisitos fundamentales definidos en el documento ISA-62443-1-1.

Dichos requisitos son:

1. *Controles de Identificación y Autenticación (IAC)*
2. *Control de Uso (UC)*
3. *Integridad del Sistema (SI)*
4. *Confidencialidad de los Datos (DC)*
5. *Flujo de Datos Restringido (RDF)*
6. *Tiempo de Respuesta a Eventos (TRE)*
7. *Disponibilidad de Recursos (RA)*

En lugar de representar el nivel de seguridad asignado con un único valor, es posible utilizar un vector de niveles de seguridad el cual representa los niveles de seguridad definidos para cada uno de los siete requisitos fundamentales.

## 4.4.2. Definición de Niveles de Seguridad.

El estándar ISA99/IEC62443 define los niveles de seguridad dentro de una escala de cinco valores (0, 1, 2, 3 y 4), cada uno de los cuales representa un nivel incremental en cuanto a medidas de ciberseguridad.

Los niveles de seguridad definidos son los siguientes:

- SL 0: *No fija requisitos específicos o no precisa protecciones de ciberseguridad.W*
- SL 1: *Requiere protección contra violaciones casuales.*
- SL 2: *Requiere protección contra violaciones intencionales con bajos recursos, conocimientos generales y baja motivación.*
- SL 3: *Requiere protección contra violaciones intencionales con recursos sofisticados, conocimientos específicos de los Sistemas de Automatización y Control y una moderada motivación.*
- SL 4: *Requiere protección contra violaciones intencionales con recursos sofisticados, conocimientos avanzados de los Sistemas de Automatización y Control y una elevada motivación.*

## 4.4.3. Formato del Vector de Niveles de Seguridad.

Un vector puede ser utilizado para representar los requisitos de ciberseguridad para una zona, conducto o sistema de forma más representativa que un único valor. Dicho vector contiene un valor específico para los niveles de seguridad definidos para cada uno de los requisitos fundamentales. (ver 3.4.1)

El formato utilizado es el siguiente:

SL-?([FR,]dominio) = { IAC UC SI DC RDF TRE RA }

Donde:

SL-? = (Requerido) Representa el tipo de SLs (ver 3.2). Los posibles valores son:

- SL-T = Nivel de Seguridad Objetivo
- SL-A = Nivel de Seguridad Alcanzado
- SL-C = Nivel de Seguridad según Capacidad

[FR,] = (Opcional) Campo que indica los requisitos fundamentales (FRs) que cada SL representa. Los FRs son representados de manera abreviada según las siglas mencionadas en el punto 3.4.1 para facilitar su interpretación.

dominio = (Requerido) Representa el dominio al cual los SLs son aplicados. Un dominio puede ser una determinada zona, un conducto, sistema de control o un determinado componente. Algunos ejemplos de diferentes dominios de la “Figura 5 - Modelo de alto nivel para procesos industriales” pueden ser: “SIS zone”, “BPCS zone”, “BPCS HMI”, “Plant DMZ” etc.

- Ejemplo 1 — SL-T(BPCS Zone) = { 2 2 0 1 3 1 3 }
- Ejemplo 2 — SL-C(SIS Zone) = { 3 3 2 3 0 0 1 }
- Ejemplo 3 — SL-C(RA, BPCS HMI) = 4

*Nota: el ejemplo 3 define solamente un nivel de seguridad 4 para el requisito fundamenta RA (Disponibilidad de Recursos) en el BPCS HMI.*

# 5

# Guía para la definición de niveles de seguridad

El estándar ISA99/IEC62443 establece una guía práctica de cómo implementar medidas de protección contra incidentes de ciberseguridad fundamentada en los niveles de seguridad previamente definidos para cada zona y/o conducto agrupados en siete requisitos "técnicos" fundamentales de ciberseguridad que como ya se ha mencionado son:

1. Controles de Identificación y Autenticación (IAC)
2. Control de Uso (UC)
3. Integridad del Sistema (SI)
4. Confidencialidad de los Datos (DC)
5. Flujo de Datos Restringido (RDF)
6. Tiempo de Respuesta a Eventos (TRE)
7. Disponibilidad de Recursos (DR)

Las siguientes siete tablas muestran los controles propuestos por el estándar para cada uno de los siete requisitos fundamentales de ciberseguridad. Las tablas están compuestas por *"Requisitos del Sistema (SR)"* y *"Aumento de Requisitos (RE)":*

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| **FR 1 - CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN (IAC)** | | | | |
| SR 1.1 -Identificación y autenticación de usuarios humanos | ✓ | ✓ | ✓ | ✓ |
| RE (1) Identificación y autenticación única | | ✓ | ✓ | ✓ |
| RE (2) Múltiple factor de autenticación para redes no confiables | | | ✓ | ✓ |
| RE (3) Múltiple factor de autenticación para todas las redes | | | | ✓ |
| SR 1.2 - Identificación y autenticación de procesos de software y dispositivos | | ✓ | ✓ | ✓ |
| RE (1) identificación y autenticación única | | | ✓ | ✓ |
| SR 1.3 - Gestión de cuentas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Gestión de cuentas unificada | | | ✓ | ✓ |
| SR 1.4 - identificación de gestión | ✓ | ✓ | ✓ | ✓ |
| SR 1.5 - Gestión de autenticación | ✓ | ✓ | ✓ | ✓ |
| RE (1) Hardware de seguridad para identificar credenciales mediante procesos de software | | | ✓ | ✓ |
| SR 1.6 - Gestión de acceso inalámbrico | ✓ | ✓ | ✓ | ✓ |

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| RE (1) Identificador y autenticador único | | ✓ | ✓ | ✓ |
| SR 1.7 - Fortaleza de autenticación basada en contraseñas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Generación de contraseñas y restricciones en tiempo de vida para usuarios humanos | | | ✓ | ✓ |
| RE (2) Restricciones en el tiempo de vida de contraseñas para todos los usuarios | | | | ✓ |
| SR 1.8 - Certificados de infraestructura de clave publica | | ✓ | ✓ | ✓ |
| SR 1.9 - Fuerte autenticación basada en clave publica | | ✓ | ✓ | ✓ |
| RE (1) Hardware de seguridad para autenticar claves publicas | | | ✓ | ✓ |
| SR 1.10 - Feedback de autenticador | ✓ | ✓ | ✓ | ✓ |
| SR 1.11 - Intentos de login fallidos | ✓ | ✓ | ✓ | ✓ |
| SR 1.12 - Notificaciones de uso de sistema | ✓ | ✓ | ✓ | ✓ |
| SR 1.13 - Acceso a través de redes no seguras | ✓ | ✓ | ✓ | ✓ |
| RE (1) Solicitud de aprobación de acceso explicita | | ✓ | ✓ | ✓ |
| **FR 2 - CONTROL DE USO (UC)** | | | | |
| SR 2.1 - Aplicación de autorización | ✓ | ✓ | ✓ | ✓ |
| RE (1) Aplicación de autorización para todos los usuarios | | ✓ | ✓ | ✓ |
| RE (2) Mapeo de permisos a roles | | ✓ | ✓ | ✓ |
| RE (3) Anular supervisor | | | ✓ | ✓ |
| RE (4) Doble Aprobación | | | | ✓ |
| SR 2.2 - Control de uso inalámbrico | ✓ | ✓ | ✓ | ✓ |
| RE (1) Identificar y reportar dispositivos inalámbricos no autorizados | | | ✓ | ✓ |
| SR 2.3 - Control de uso para dispositivos portátiles y mobile | ✓ | ✓ | ✓ | ✓ |
| RE (1) Aplicación del estado de seguridad de dispositivos portátiles y mobile | | | ✓ | ✓ |
| SR 2.4 - Código mobile | ✓ | ✓ | ✓ | ✓ |

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| RE (1) Chequeo de integridad de código mobile | | | ✓ | ✓ |
| SR 2.5 - Bloqueo de sesión | ✓ | ✓ | ✓ | ✓ |
| SR 2.6 - Terminación de sesiones remotas | | ✓ | ✓ | ✓ |
| SR 2.7 - Control de sesiones concurrentes | | | ✓ | ✓ |
| SR 2.8 - Eventos auditables | ✓ | ✓ | ✓ | ✓ |
| RE (1) Pistas de auditoria de sistemas con gestión centralizada | | | ✓ | ✓ |
| SR 2.9 - Auditar capacidad de almacenamiento | ✓ | ✓ | ✓ | ✓ |
| RE (1) Advertir cuando se haya alcanzado el umbral de capacidad en los registros de auditoria | | | ✓ | ✓ |
| SR 2.10 - Responder a fallas en el proceso de auditoria | ✓ | ✓ | ✓ | ✓ |
| SR 2.11 - Marcas de tiempo | | ✓ | ✓ | ✓ |
| RE (1) Sincronización interna de tiempo | | | ✓ | ✓ |
| RE (2) Protección en la integridad de la fuente de tiempo | | | | ✓ |
| SR 2.12 - No repudio | | | ✓ | ✓ |
| RE (1) No repudio para todos los usuarios | | | | ✓ |
| **FR 3 - INTEGRIDAD DEL SISTEMA (SI)** | | | | |
| SR 3.1 - Integridad en las comunicaciones | ✓ | ✓ | ✓ | ✓ |
| RE (1) Usar criptografía para proteger la integridad | | | ✓ | ✓ |
| SR 3.2 - Protección contra código malicioso | ✓ | ✓ | ✓ | ✓ |
| RE (1) Protección contra código malicioso en los puntos de entrada y salida | | ✓ | ✓ | ✓ |
| RE (2) Gestión centralizada para protección contra código malicioso | | | ✓ | ✓ |
| SR 3.3 - Verificación de funcionalidades de seguridad | ✓ | ✓ | ✓ | ✓ |
| RE (1) Mecanismos automáticos para verificar funcionalidades de seguridad | | | ✓ | ✓ |
| RE (2) Verificaciones de funcionalidades de seguridad durante la normal operación | | | | ✓ |

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| SR 3.4 - Integridad del software e información | | ✓ | ✓ | ✓ |
| RE (1) Notificaciones automáticas sobre violaciones de integridad | | | ✓ | ✓ |
| SR 3.5 - Validación de entradas | ✓ | ✓ | ✓ | ✓ |
| SR 3.6 - Salidas Determinísticas | ✓ | ✓ | ✓ | ✓ |
| SR 3.7 - Manejo de errores | | ✓ | ✓ | ✓ |
| SR 3.8 - Integridad de sesiones | | ✓ | ✓ | ✓ |
| RE (1) Invalidar IDs de sesión una vez que la sesión fue terminada | | | ✓ | ✓ |
| RE (2) Generación de IDs únicos de sesión | | | ✓ | ✓ |
| RE (3) Aleatoriedad de IDs de sesión | | | | ✓ |
| **FR 4 - CONFIDENCIALIDAD DE LOS DATOS (DC)** | | | | |
| SR 4.1 - Confidencialidad de la información | ✓ | ✓ | ✓ | ✓ |
| RE (1) Protección de la confidencialidad de la información alojada o en tránsito por redes no confiables | | ✓ | ✓ | ✓ |
| RE (2) Protección de la confidencialidad a través de los límites de las zonas | | | | ✓ |
| SR 4.2 - Persistencia de la información | | ✓ | ✓ | ✓ |
| RE (1) Purga de recursos de memoria compartida | | | ✓ | ✓ |
| SR 4.3 - Uso de criptografía | ✓ | ✓ | ✓ | ✓ |
| **FR 5 - FLUJO DE DATOS RESTRINGIDO (RDF)** | | | | |
| SR 5.1 - Segmentación de redes | ✓ | ✓ | ✓ | ✓ |
| RE (1) Segmentación física de redes | | ✓ | ✓ | ✓ |
| RE (2) Independencia de redes sin sistemas de control | | | ✓ | ✓ |
| RE (3) Aislamiento lógico y físico de redes criticas | | | | ✓ |
| SR 5.2 - Protección de limites de zonas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Denegar por defecto, permitir por excepción | | ✓ | ✓ | ✓ |
| RE (2) Modo isla | | | ✓ | ✓ |

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| RE (3) Cierre ante falla | | | ✓ | ✓ |
| SR 5.3 - Restricción en comunicaciones persona a persona de propósitos generales | ✓ | ✓ | ✓ | ✓ |
| RE (1) Prohibir todas las comunicaciones persona a persona de propósitos generales | | | ✓ | ✓ |
| SR 5.4 - Particionamiento de aplicaciones | ✓ | ✓ | ✓ | ✓ |
| **FR 6 - TIEMPO DE RESPUESTA A EVENTOS (TRE)** | | | | |
| SR 6.1 - Auditar accesibilidad a logs | ✓ | ✓ | ✓ | ✓ |
| RE (1) Acceso programado a logs de auditoria | | | ✓ | ✓ |
| SR 6.2 - Monitoreo continuo | | ✓ | ✓ | ✓ |
| **FR 7 - DISPONIBILIDAD DE RECURSOS (RA)** | | | | |
| SR 7.1 - Protección contra denegación de servicio | ✓ | ✓ | ✓ | ✓ |
| RE (1) Gestionar la carga en las comunicaciones | | ✓ | ✓ | ✓ |
| RE (1) Limitar los efectos de una denegación de servicio a otros sistemas o redes | | | ✓ | ✓ |
| SR 7.2 - Gestión de recursos | ✓ | ✓ | ✓ | ✓ |
| SR 7.3 - Control de backup del sistema | ✓ | ✓ | ✓ | ✓ |
| RE (1) Verificación de backup | | ✓ | ✓ | ✓ |
| RE (2) Automatización de backup | | | ✓ | ✓ |
| SR 7.4 - Restauración y reconstitución del sistema de control | ✓ | ✓ | ✓ | ✓ |
| SR 7.5 - Energía de emergencia | ✓ | ✓ | ✓ | ✓ |
| SR 7.6 - Ajustes de redes y configuraciones de seguridad | | | ✓ | ✓ |
| RE (1) Reportes de ajustes de seguridad actuales legibles desde una maquina | | | ✓ | ✓ |
| SR 7.7 - Menos funcionalidades | ✓ | ✓ | ✓ | ✓ |
| SR 7.8 - Inventario de componentes de sistemas de control | | ✓ | ✓ | ✓ |

# 6

# Comentario final y conclusión


Zonas y conductos, si bien parecen conceptos triviales o básicos, constituyen un componente fundamental para iniciar el proceso de creación de un programa de ciberseguridad basado en el estándar IEC 62443. Una correcta segmentación en zonas y conductos permitirá analizar los sistemas industriales de manera ordenada y sistemática desde el punto de vista de la ciberseguridad. En lugar de analizar procesos, subprocesos, sistemas y/o subsistemas y sus correspondientes componentes, podemos centrar nuestros esfuerzos de implementar medidas de protección focalizando los mismos en cada una de las zonas y(o conductos identificados. El estándar es muy claro en este sentido definiendo siete requisitos fundamentales de ciberseguridad los cuales se vuelven más rigurosos a medida que avanzamos a través de los cuatro niveles seguridad propuestos.

Resulta de gran valor incorporar los conceptos de Zonas y Conductos desde la concepción de los sistemas industriales. Los diseños de sistemas de control industrial deberían estar basados en dichos conceptos y los fabricantes deberían especificar los niveles de seguridad según su capacidad (SL-C) para cada componente y/o sistema de la solución propuesta. Actualmente existen organismos especializados (como es el caso de ISA Secure) que colaboran en este tipo de especificaciones certificando que determinados productos instalados correctamente según las especificaciones del fabricante satisfacen los requisitos fundamentales para un determinado SL-C.

A partir de ello, los propietarios de infraestructuras industriales podrán exigir a sus fabricantes y/o integradores que adecuen sus propuestas, o bien implementen medidas de protección adicionales para cumplir con los requisitos necesarios para alcanzar el nivel de seguridad definido como objetivo (SL-T).

El estándar IEC 62443 brinda un lenguaje y/o punto de referencia común a partir del cual tanto propietarios, fabricantes como integradores pueden trabajar conjuntamente, y de manera ordenada en mejorar la ciberseguridad en entornos industriales.

Este documento permite identificar claramente un punto de partida para iniciar el proceso continuo de protección de sistemas industriales contra ciberamenazas.

# 7

# Glosario de términos y acrónimos

- Zona: Conjunto de activos lógicos o físicos agrupados por requisitos comunes de seguridad. Los límites de cada zona deben estar claramente establecidos. Las zonas pueden estar organizadas jerárquicamente, es decir una zona puede ser el resultado de una agrupación de sub zonas
- Conducto: Es un canal de comunicación entre dos zonas de seguridad. Proporciona las funciones de seguridad que permiten a dos zonas comunicarse de forma segura. Toda comunicación entre diferentes zonas ha de realizarse a través de un conducto.
- Canal: Vínculo de comunicación establecido dentro de un conducto.
- SuC: Sistema bajo Consideración.
- SL: Nivel de Seguridad (Security Level)
- SL-T: Nivel de Seguridad Objetivo
- SL-A: Nivel de Seguridad Alcanzado
- SL-C: Nivel de Seguridad según Capacidad
- IAC: Controles de Identificación y Autentificación
- UC: Control de Uso
- SI: Integridad del Sistema
- DC: Confidencialidad de los Datos
- RDF: Flujo de Datos Restringido
- TRE: Tiempo de Respuesta a Eventos
- RA: Disponibilidad de Recursos
- FR: Requisitos Fundamentales de Ciberseguridad
- SR: Requisitos de Seguridad
- RE: Niveles de Exigencia
- SIS: Sistema Instrumentado de Seguridad
- BPCS: Business Planning and Control System
- HMI: Human Machine Interface
- DMZ: Zona desmilitarizada

# 8

# Bibliografía

*[1] ANSI/ISA-62443-1-1-2007, Security for industrial automation and control systems: Terminology, concepts and models*

*[2] ANSI/ISA-TR62443-1-2, Security for industrial automation and control systems: Master glossary of terms and abbreviations*

*[3] ANSI/ISA-62443-3-2, Security for industrial automation and control systems: Target security levels for zones and conduits*

*[4] ANSI/ISA-62443-3-3, Security for industrial automation and control systems: System security requirements and security levels*