COMISIÓN ELECTROTÉCNICA INTERNACIONAL

_____

REDES DE COMUNICACIÓN INDUSTRIAL - SEGURIDAD DE REDES Y SISTEMAS

Parte 1-1: Terminología, conceptos y modelos

PREFACIO

1. La Comisión Electrotécnica Internacional (IEC) es una organización mundial para la estandarización que comprende todos los comités electrotécnicos nacionales (comités nacionales de IEC). El objetivo de IEC es promover cooperación internacional en todas las cuestiones relativas a la normalización en los ámbitos eléctrico y electrónico. Con este fin y además de otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, especificaciones disponibles públicamente (PAS) y guías (en adelante, "IEC Publicación (es) "). Su preparación se confía a los comités técnicos; cualquier comité nacional de IEC interesado en el tema tratado pueden participar en este trabajo preparatorio. Las organizaciones internacionales, gubernamentales y no gubernamentales que se relacionan con la IEC también participan en esta preparación. IEC colabora estrechamente con la Organización Internacional de Normalización (ISO) de acuerdo con las condiciones determinadas por acuerdo entre las dos organizaciones.
2. Las decisiones o acuerdos formales de IEC sobre asuntos técnicos expresan, en la medida de lo posible, un acuerdo internacional, consenso de opinión sobre los temas relevantes ya que cada comité técnico tiene representación de todos los Comités Nacionales IEC interesados.
3. Las publicaciones IEC tienen la forma de recomendaciones para uso internacional y son aceptadas por IEC Comités Nacionales en ese sentido. Si bien se hacen todos los esfuerzos razonables para garantizar que el contenido técnico de IEC sean publicaciones precisas, IEC no se hace responsable de la forma en que se utilizan o de cualquier mala interpretación por parte de cualquier usuario final.
4. Para promover la uniformidad internacional, los Comités Nacionales de IEC se comprometen a aplicar las Publicaciones de IEC de forma transparente en la mayor medida posible en sus publicaciones nacionales y regionales. Cualquier divergencia entre cualquier publicación IEC y la publicación nacional o regional correspondiente se indicará claramente en esta última.
5. IEC no proporciona ningún procedimiento marcado para indicar su aprobación y no puede hacerse responsable de equipo declarado conforme a una publicación IEC.
6. Todos los usuarios deben asegurarse de tener la última edición de esta publicación.
7. No se responsabilizará a IEC o sus directores, empleados, servidores o agentes, incluidos expertos individuales y miembros de sus comités técnicos y comités nacionales de IEC por lesiones personales, daños a la propiedad u otros daños de cualquier naturaleza, ya sean directos o indirectos, o por costos (incluidos los honorarios legales) y gastos derivados de la publicación, uso o dependencia de esta publicación de IEC o cualquier otra IEC Publicaciones.
8. Se llama la atención a las referencias normativas citadas en esta publicación. El uso de las publicaciones referenciadas es indispensable para la correcta aplicación de esta publicación.
9. Se llama la atención sobre la posibilidad de que algunos de los elementos de esta publicación IEC puedan ser objeto de derechos de patente. IEC no será responsable de identificar ninguno o todos los derechos de patente.

La tarea principal de los comités técnicos de IEC es preparar normas internacionales. En circunstancias excepcionales, un comité técnico puede proponer la publicación de una especificación técnica cuando:

- No se puede obtener el soporte requerido para la publicación de una Norma Internacional, a pesar de los repetidos esfuerzos, o
- El tema aún se encuentra en desarrollo técnico o por cualquier otro motivo, no hay posibilidad en el futuro inmediato de un acuerdo sobre una Norma Internacional.

Las especificaciones técnicas están sujetas a revisión dentro de los tres años posteriores a la publicación para decidir si pueden transformarse en normas internacionales.

IEC 62443-1-1, que es una especificación técnica, ha sido preparada por IEC Comité Técnico 65: Medición, control y automatización de procesos industriales.

Esta especificación técnica se deriva del estándar estadounidense ANSI / S99.01.01 correspondiente.

El texto de esta especificación técnica se basa en los siguientes documentos:

Borrador de Consulta	Informe sobre votación
65/423 / DTS	65 / 432A / RVC

La información completa sobre la votación para la aprobación de esta especificación técnica se puede encontrar en el informe sobre votación indicado en la tabla anterior.

Esta publicación ha sido redactada de acuerdo con las Directivas ISO / IEC, Parte 2.

Una lista de todas las partes de la serie IEC 62433, publicada bajo el título general Redes de Comunicación Industrial: la seguridad de la red y del sistema se puede encontrar en el sitio web de IEC.

El comité ha decidido que el contenido de esta publicación permanecerá sin cambios hasta su mantenimiento en la fecha indicada en el sitio web de IEC en "http://webstore.iec.ch" en los datos relacionado con la publicación específica. En esta fecha, la publicación será:

- transformada en un estándar internacional,
- reconfirmada,
- retirada,
- reemplazada por una edición revisada, o
- modificada.

Se puede emitir una versión bilingüe de esta publicación en una fecha posterior.

NOTA: La revisión de esta especificación técnica se sincronizará con las otras partes de la serie IEC 62443.

IMPORTANTE: el logotipo de "color dentro" en la portada de esta publicación indica que contiene colores que se consideran útiles para la comprensión correcta de sus contenidos. Por lo tanto, los usuarios deben imprimir esta publicación con una impresora a color.

INTRODUCCIÓN

El objeto de esta especificación técnica es la seguridad de los sistemas de automatización y de control industrial. Para abordar una gama de aplicaciones (es decir, tipos de industria), cada uno de los términos en esta descripción ha sido interpretada de manera muy amplia.

El término "Sistemas de Automatización y Control Industrial" (IACS) incluye los sistemas de control utilizados en plantas e instalaciones de fabricación y procesamiento, construcción de sistemas de control ambiental, operaciones geográficamente dispersas como servicios públicos (es decir, electricidad, gas y agua), tuberías y las instalaciones de producción y distribución de petróleo, y otras industrias y aplicaciones como redes de transporte, que utilizan activos controlados o monitoreados de manera automatizada o remota.

El término "seguridad" se considera aquí para significar la prevención de actividades ilegales o no deseadas, penetración, interferencia intencional o no intencional con la operación adecuada y prevista, o acceso inapropiado a información confidencial en IACS. Esta especificación técnica, se enfoca en particular en la Ciberseguridad, incluye computadoras, redes, sistemas operativos, aplicaciones y otros componentes configurables o programables del sistema.

La audiencia para esta especificación técnica incluye a todos los usuarios de IACS (incluidas las instalaciones de operaciones, mantenimiento, ingeniería y componentes corporativos de organizaciones de usuarios), fabricantes, proveedores, organizaciones gubernamentales involucradas o afectadas por el sistema de control de ciberseguridad, profesionales del sistema de control y profesionales de la seguridad. La mutua comprensión y cooperación entre las tecnologías de la información (TI), operaciones, ingeniería y las organizaciones de fabricación, son importantes para el éxito general de cualquier iniciativa de seguridad, esta especificación técnica también son una referencia para los responsables de integración de IACS y redes empresariales.

Las preguntas típicas abordadas por esta especificación técnica incluyen:

a) ¿Cuál es el alcance general de la aplicación para la seguridad de IACS?
b) ¿Cómo se pueden definir las necesidades y requisitos de un sistema de seguridad usando terminologías consistentes?
c) ¿Cuáles son los conceptos básicos que forman la base para un mejor análisis de las actividades, los atributos del sistema y las acciones importantes para proporcionar un control electrónico seguro de los sistemas?
d) ¿Cómo se pueden agrupar o clasificar los componentes de un IACS con el fin de definir y gestionar la seguridad?
e) ¿Cuáles son los diferentes objetivos de ciberseguridad para las aplicaciones de sistemas de control?
f) ¿Cómo se pueden establecer y codificar estos objetivos?

Cada una de estas preguntas se aborda en detalle en las cláusulas posteriores de esta especificación técnica.

REDES DE COMUNICACIÓN INDUSTRIAL – SEGURIDAD DE REDES Y SISTEMAS

Parte 1-1: Terminología, conceptos y modelos.

1 Alcance

1.1 General

Esta parte de la serie IEC 62443 es una especificación técnica que define la terminología, conceptos y modelos para la seguridad de los Sistemas de Automatización y Control Industrial (IACS). Eso establece la base para los restantes estándares de la serie IEC 62443.

Para articular completamente los sistemas y componentes, la dirección de la serie IEC 62443, el rango de la cobertura se puede definir y comprender desde varias perspectivas, incluidas las siguientes:

a) rango de funcionalidad incluida;
b) sistemas e interfaces específicos;
c) criterios para seleccionar las actividades incluidas;
d) criterios para seleccionar los activos incluidos.

Cada uno de estos se describe en las siguientes subcláusulas:

1.2 Funcionalidad incluida

El alcance de esta especificación técnica se puede describir en términos del rango de funcionalidad dentro de los sistemas de información y automatización de una organización. Esta funcionalidad es típicamente descrita en términos de uno o más modelos.

Esta especificación técnica se centra principalmente en la automatización y el control industrial, como se describe en un modelo de referencia (ver Cláusula 6). Los sistemas de planificación empresarial y logística no son explícitamente abordados dentro del alcance de esta especificación técnica, aunque la integridad de los datos se considera el intercambio entre sistemas comerciales e industriales.

La automatización y el control industrial incluyen los componentes de control de supervisión que se encuentran típicamente en industrias de procesos. También incluye sistemas SCADA (control supervisado y adquisición de datos) que son comúnmente utilizados por organizaciones que operan en industrias de infraestructura crítica. Estas incluyen las siguientes:

a) transmisión y distribución de electricidad;
b) redes de distribución de gas y agua;
c) operaciones de producción de petróleo y gas;
d) tuberías de transmisión de gas y líquido.

Esta no es una lista exclusiva. Los sistemas SCADA también se pueden encontrar en otros sistemas de infraestructuras industriales críticas y no críticas.

1.3 Sistemas e interfaces

Al abarcar todos los IACS, esta especificación técnica cubre los sistemas que pueden afectar o influir en la operación segura y confiable de los procesos industriales. Ella Incluye, pero no se limitada a:

a) Sistemas de control industrial y sus redes de comunicaciones asociadas[1], incluidos sistemas de control distribuido (DCS), controladores lógicos programables (PLC), unidades de terminal remoto (RTU), dispositivos electrónicos inteligentes, sistemas SCADA, detección electrónica en red y sistemas de control, medición y transferencia de custodia, y monitoreo y sistemas de diagnóstico. (En este contexto, los sistemas de control industrial incluyen sistemas básicos de control de procesos y funciones de Sistemas Instrumentados de Seguridad (SIS), ya sea físicamente separadas o integrado.)
b) Sistemas asociados en el nivel 3 o inferior del modelo de referencia descrito en la Cláusula 6. Los ejemplos incluyen control avanzado o multivariable, optimizadores en línea, monitoreo de equipos dedicados, interfaces gráficas, historiadores de procesos, sistemas de ejecución de fabricación, sistemas de detección de fugas en tuberías, gestión del trabajo, gestión de interrupciones y sistemas de gestión de energía eléctrica.
c) Interfaces internas, humanas, de red, software, máquinas o dispositivos asociados que se utilizan el control para proporcionar funcionalidad, seguridad, fabricación u operaciones remotas para procesos continuo, por lotes, discretos y de otro tipo.

1.4 Criterios basados en actividades

IEC 62443-2-1[2] proporciona criterios para definir actividades asociadas con las operaciones de fabricación. Se ha desarrollado una lista similar para determinar el alcance de esta especificación técnica. Se debe considerar que un sistema está dentro del rango de cobertura de las series IEC 62443 si la actividad que realiza es necesaria para cualquiera de los siguientes:

a) funcionamiento predecible de proceso;
b) seguridad de proceso o de personal;
c) fiabilidad o disponibilidad de proceso;
d) eficiencia de proceso;
e) operabilidad de proceso;
f) calidad de producto;
g) protección del medio ambiente;
h) cumplimiento normativo;
i) venta de productos o transferencia de custodia.

_____

1 El término "redes de comunicaciones" incluye todos los tipos de medios de comunicación, incluidos varios tipos de comunicaciones inalámbricas. Una descripción detallada del uso de las comunicaciones inalámbricas en la automatización industrial. sistemas está más allá del alcance de esta especificación técnica. Las técnicas de comunicación inalámbrica son específicamente mencionadas solo en situaciones donde su uso o aplicación puede cambiar la naturaleza de la seguridad aplicada o requerida.

2 Para ser publicado.

1.5 Criterios basados en activos

La cobertura de esta especificación técnica incluye aquellos sistemas en activos que cumplen con cualquiera de los siguientes criterios, o cuya seguridad es esencial para la protección de otros activos que cumplen estos criterios:

a) El activo tiene valor económico para un proceso de fabricación u operación.
b) El activo realiza una función necesaria para la operación de una manufactura u operación de proceso.
c) El activo representa la propiedad intelectual de un proceso de fabricación u operación.
d) El activo es necesario para operar y mantener la seguridad para una fabricación u operación de proceso.

e) El activo es necesario para proteger al personal, contratistas y visitantes involucrados en un proceso de fabricación u operación.
f) El activo es necesario para proteger el medio ambiente.
g) El activo es necesario para proteger al público de eventos causados por una fabricación o proceso operativo
h) El activo es un requisito legal, especialmente para fines de seguridad de una fábrica o proceso operativo
i) El activo es necesario para la recuperación ante desastres.
j) El activo es necesario para registrar eventos de seguridad.

Este rango de cobertura incluye sistemas cuyo compromiso podría resultar peligroso para la salud o seguridad pública o de los empleados, pérdida de confianza del público, violación de los requisitos normativos, pérdida o invalidación de información confidencial o de propiedad, contaminación ambiental y / o pérdida económica o impacto en una entidad o en la seguridad local o nacional.

2 Referencias normativas

Los siguientes documentos referenciados son indispensables para la aplicación de este documento. Por referencias fechadas, solo se aplica la edición citada. Para referencias sin fecha, se aplica la última edición de el documento de referencia (incluidas las enmiendas).

IEC 62264-1, Sistema Integral de control empresarial - Parte 1: Modelos y terminología

ISO / CEI 15408-1, Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad TI - Parte 1: Introducción y modelo general

3 Términos, definiciones y abreviaturas

3.1 General

Siempre que sea posible, las definiciones se han adaptado de las utilizadas en fuentes industriales establecidas. Algunas definiciones se han adaptado de definiciones más genéricas utilizadas en la industria de TI.

3.2 Términos y definiciones

A los fines de este documento, se aplican los siguientes términos y definiciones

3.2.1 Acceso

Capacidad y medios para comunicarse o interactuar con un sistema para usar recursos del sistema

NOTA: El acceso puede implicar acceso físico (autorización para ser permitido físicamente en un área, posesión física de la llave de la cerradura, código PIN o tarjeta de acceso o atributos biométricos que permitan el acceso) o acceso lógico (autorización para iniciar sesión en un sistema y aplicación, a través de una combinación de medios lógicos y físicos).

3.2.2 Control de acceso

Protección contra el acceso no autorizado de los recursos del sistema; un proceso por el cual el uso de los recursos del sistema está regulado de acuerdo con una política de seguridad y solo están autorizados por entidades (usuarios, programas, procesos u otros sistemas) de acuerdo con esa política [10][3] [RFC 2828, modificado]

3.2.3 Responsabilidad

Propiedad de un sistema (incluidos todos los recursos del sistema) que garantiza que las acciones en una entidad del sistema se puedan rastrear de forma exclusiva en esa entidad, que puede ser considerada responsable de sus acciones [10]

3.2.4 Solicitud

Programa de software que realiza funciones específicas iniciadas por un comando de usuario o evento de un proceso y que se puede ejecutar sin acceso al sistema de control, monitoreo o privilegios de administración.

3.2.5 Área

Subconjunto del grupo de activos físicos, geográficos o lógicos de un sitio

NOTA: Un área puede contener líneas de fabricación, celdas de proceso y unidades de producción. Las áreas pueden estar conectadas a entre sí por una red de área local del sitio y puede contener sistemas relacionados con las operaciones realizadas en esa área.

3.2.6 Activo

Objeto físico o lógico propiedad de o bajo los deberes de custodia de una organización, que tiene ya sea un valor percibido o real para la organización

3 Los números entre corchetes se refieren a la Bibliografía.

NOTA: En el caso de los sistemas de automatización y control industrial, los activos físicos que tienen el mayor valor medible directamente puede ser el equipo bajo control.

3.2.7 Asociación

Relación cooperativa entre entidades del sistema, generalmente con el propósito de transferir información entre ellos [10]

3.2.8 Garantía

Atributo de un sistema que proporciona motivos para confiar en que el sistema opera de tal manera que se aplique la política de seguridad del sistema

3.2.9 Ataque

Asalto a un sistema que se deriva de una amenaza inteligente, es decir, un acto inteligente que es un intento deliberado (especialmente en el sentido de un método o técnica) para evadir los servicios de seguridad y violar la política de seguridad de un sistema [10]

NOTA: Hay diferentes clases de ataque comúnmente reconocidas:

- Un "ataque activo" intenta alterar los recursos del sistema o afectar su funcionamiento.
- Un "ataque pasivo" intenta aprender o hacer uso de la información del sistema, pero no afecta los recursos del sistema.
- Un "ataque interno" es un ataque iniciado por una entidad dentro del perímetro de seguridad, es decir, una entidad que está autorizada para acceder a los recursos del sistema, pero los usa de una manera no aprobada por quienes otorgaron la autorización.
- Un "ataque externo" se inicia desde el exterior del perímetro, por un usuario no autorizado o ilegítimo del sistema. (incluido un atacante interno desde fuera del perímetro de seguridad). Los posibles atacantes externos van desde bromistas aficionados a delincuentes organizados, terroristas internacionales y gobiernos hostiles.

3.2.10 Árbol de ataque

Forma y metódica de encontrar formas de atacar la seguridad de un sistema

3.2.11 Auditoría

Revisión independiente y examen de registros y actividades para evaluar la idoneidad del sistema de controles, para garantizar el cumplimiento de las políticas establecidas y los procedimientos operativos, y recomendar los cambios necesarios en los controles, políticas o procedimientos (ver 3.2.100).

NOTA: Hay tres formas de auditoría.

- Las auditorías externas son realizadas por partes que no son empleados o contratistas de la organización.
- La auditoría interna son realizada por una unidad organizativa separada dedicada a la auditoría interna.
- Las autoevaluaciones son realizadas por par de miembros de la función de automatización de procesos.

3.2.12 Autenticar

Verificar la identidad de un usuario, dispositivo de usuario, u otra entidad, o la integridad de los datos almacenados, transmitido o expuesto a modificaciones no autorizadas en un sistema de información, o establecer la validez de una transmisión.

3.2.13 Autenticación

Medida de seguridad diseñada para establecer la validez de una transmisión, mensaje u origen, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información.

3.2.14 Autorización

Derecho o permiso otorgado a una entidad del sistema para acceder a un recurso del sistema [10].

3.2.15 Vehículo automatizado

Dispositivo móvil que incluye un sistema de control que le permite operar de forma autónoma o bajo control remoto.

3.2.16 Disponibilidad (rendimiento)

Capacidad de un elemento para estar en un estado para realizar una función requerida en determinadas condiciones en un instante dado o durante un intervalo de tiempo dado, suponiendo que los recursos externos necesarios son previstos.

NOTA 1: Esta capacidad depende de los aspectos combinados del rendimiento de la confiabilidad, el rendimiento la mantenibilidad y el rendimiento de soporte de mantenimiento.

NOTA 2: Los recursos externos necesarios, que no sean recursos de mantenimiento, no afectan el rendimiento de disponibilidad del artículo.

NOTA 3: En francés, el término "disponibilidad" también se utiliza en el sentido de "disponibilidad instantánea".

3.2.17 Frontera

Borde o límite de una zona de seguridad física o lógica.

3.2.18 Botnet

Colección de robots de software, o bots, que se ejecutan de forma autónoma.
NOTA: El creador de un botnet puede controlar el grupo de forma remota, posiblemente con fines nefastos.

3.2.19 Perímetro
Software, hardware u otra barrera física que limita el acceso a un sistema o parte de un sistema.

3.2.20 Canal

Enlace de comunicación específico establecido dentro de un conducto de comunicación (ver 3.2.27).

3.2.21 Texto cifrado

Datos que se han transformado mediante cifrado para que su contenido de información semántica (es decir, su significado) no sea inteligible o directamente disponible.

3.2.22 Cliente

Dispositivo o aplicación que recibe o solicita servicios o información de una aplicación de servidor [11].

3.2.23 Camino de comunicación

Conexión lógica entre una fuente y uno o más destinos, que podrían ser dispositivos, procesos físicos, elementos de datos, comandos o interfaces programáticas.

NOTA: La ruta de comunicación no se limita a redes cableadas o inalámbricas, sino que incluye otros medios de comunicación como memoria, llamadas a procedimientos, estado de físico de la planta, medios portátiles e interacciones humanas.

3.2.24 Seguridad de comunicación

a) medidas que implementan y garantizan servicios de seguridad en un sistema de comunicación, particularmente aquellos que brindan confidencialidad e integridad de datos y que autentican entidades comunicantes,
b) el estado alcanzado mediante la aplicación de servicios de seguridad, en particular, el estado de confidencialidad de los datos, integridad y entidades de comunicaciones autenticadas con éxito [10].

NOTA: Por lo general, se entiende que esta frase incluye algoritmos criptográficos y métodos de administración de claves y procesos, dispositivos que los implementan, y la gestión del ciclo de vida de materiales y dispositivos de claves. Sin embargo, Los algoritmos criptográficos y los métodos y procesos de administración de claves pueden no ser aplicables a algunas aplicaciones del sistema de control.

3.2.25 Sistema de comunicación

Disposición de hardware, software y medios de propagación para permitir la transferencia de mensajes de una aplicación a otra [9].

3.2.26 Compromiso

Divulgación no autorizada, modificación, sustitución o uso de información (incluido texto sin formato claves criptográficas y otros parámetros críticos de seguridad) [12].

3.2.27 Conducto

Agrupación lógica de activos de comunicación que protege la seguridad de los canales que contiene.
NOTA: Esto es análogo a la forma en que un conducto físico protege los cables del daño físico.

3.2.28 Confidencialidad

Aseguramiento de que la información no se divulgue a personas, procesos o dispositivos no autorizados.

3.2.29 Centro de control

Ubicación central utilizada para operar un conjunto de activos.

NOTA 1: Las industrias de infraestructura generalmente usan uno o más centros de control para supervisar o coordinar sus operaciones. Si hay varios centros de control (por ejemplo, un centro de respaldo en un sitio separado), generalmente son conectados entre sí a través de una red de área amplia. El centro de control contiene el sistema SCADA, las computadoras host y dispositivos de visualización del operador asociados más sistemas de información auxiliar como un historiador.

NOTA 2: En algunas industrias, el término "sala de control" puede usarse más comúnmente.

3.2.30 Equipo de control

Clase que incluye sistemas de control distribuido, controladores lógicos programables, sistemas SCADA, consolas de interfaz de operador asociadas y dispositivos de detección y control de campo utilizados para gestionar y controlar el proceso.

NOTA: El término también incluye redes de bus de campo donde la lógica de control y los algoritmos se ejecutan en dispositivos inteligentes, dispositivos electrónicos que coordinan acciones entre sí, así como sistemas utilizados para monitorear el proceso y los sistemas utilizados para mantener el proceso.

3.2.31 Red de control

Red de tiempo crítico que normalmente está conectada a equipos que controlan procesos físicos (ver 3.2.97).

NOTA: La red de control se puede subdividir en zonas y puede haber múltiples redes de control separadas dentro de una empresa o sitio.

3.2.32 Costo

Valor del impacto para una organización o persona que se puede medir.

3.2.33 Contramedida

Acción, dispositivo, procedimiento o técnica que reduce una amenaza, una vulnerabilidad o un ataque eliminándolo o previniéndolo, minimizando el daño que puede causar, o descubriendo e informarlo para que se puedan tomar medidas correctivas [10].

NOTA: El término "control" también se utiliza para describir este concepto en algunos contextos. El término contramedida es elegido para este documento para evitar confusiones con el término "control" en el contexto del control del proceso.

3.2.34 Algoritmo criptográfico

Algoritmo basado en la ciencia de la criptografía, incluidos los algoritmos de cifrado, algoritmos criptográficos hash, algoritmos de firma digital y algoritmos de acuerdo de llaves.

3.2.35 Clave criptográfica

Parámetro de entrada que varía la transformación a realizar por un algoritmo criptográfico [10]

NOTA: Generalmente abreviado a "clave"

3.2.36 Ciberseguridad

Acciones requeridas para impedir el uso no autorizado de, denegación de servicio a, modificaciones a, divulgación de, pérdida de ingresos desde, o destrucción de sistemas críticos o activos informativos.

NOTA: El objetivo es reducir el riesgo de causar lesiones personales o poner en peligro la salud pública, la pérdida de confianza del consumidor, divulgación de activos confidenciales, incumplimiento de la protección de los activos comerciales o incumplimiento de regulaciones Estos conceptos se aplican a cualquier sistema en el proceso de producción e incluyen tanto independientes como componentes en red. Las comunicaciones entre sistemas pueden ser a través de mensajes internos o por cualquier interfaz humana o de máquinas que autentican, operan,

controlan o intercambian datos con cualquiera de estos sistemas de control. La ciberseguridad incluye los conceptos de identificación, autenticación, responsabilidad, autorización, disponibilidad y privacidad.

3.2.37 Confidencialidad de datos

Propiedad de que la información no está disponible o divulgada a ninguna entidad del sistema no autorizada, incluidos individuos, entidades o procesos no autorizados [8].

3.2.38 Integridad de los datos

Propiedad de que los datos no han sido cambiados, destruidos o perdidos de manera no autorizada o de manera accidental [10].

NOTA: Este término se refiere a la constancia y la confianza en los valores de los datos, no a la información de que los valores representar o la confiabilidad de la fuente de los valores.

3.2.39 Descifrado

Proceso de cambiar el texto cifrado a texto plano utilizando un algoritmo criptográfico y una clave (ver 3.2.47) [10].

3.2.40 Defensa en profundidad

Provisión de múltiples protecciones de seguridad, especialmente en capas, con la intención de al menos retrasar si no es posible prevenir un ataque.

NOTA: La defensa en profundidad implica capas de seguridad y detección, incluso en sistemas únicos, y proporciona las siguientes características:

- los atacantes se enfrentan a romper o evitar cada capa sin ser detectados;
- una falla en una capa puede ser mitigada por las capacidades en otras capas;
- una seguridad del sistema se convierte en un conjunto de capas dentro de la seguridad general de la red.

3.2.41 Zona desmilitarizada

Segmento de red perimetral que se inserta lógicamente entre redes internas y externas

NOTA 1: El propósito de una zona desmilitarizada es hacer cumplir la política de la red interna para intercambiar información externa y proporcionar a fuentes externas no confiables con acceso restringido información liberable mientras se protege la red interna de ataques externos.

NOTA 2: En el contexto de los sistemas de automatización y control industrial, el término "red interna" se aplica típicamente a la red o segmento que es el foco principal de protección. Por ejemplo, una red de control podría ser considerado "interna" cuando está conectado a una red comercial "externa".

3.2.42 Negación de servicio

Prevención o interrupción del acceso autorizado a un recurso del sistema o la demora del sistema operaciones y funciones [10].

NOTA: En el contexto de la automatización industrial y los sistemas de control, la denegación de servicio puede referirse a la pérdida de proceso. función, no solo pérdida de comunicaciones de datos.

3.2.43 Firma digital

Resultado de una transformación criptográfica de datos que, cuando se implementa adecuadamente, proporciona los servicios de autenticación de origen, integridad de datos y no rechazo del firmante [11].

3.2.44 Sistema de control distribuido

Tipo de sistema de control en el que los elementos del sistema están dispersos, pero operan acoplados entre sí.

NOTA1: Los sistemas de control distribuido pueden tener constantes de tiempo de acoplamiento, más cortas que las que se encuentran típicamente en Sistemas SCADA.

NOTA 2: Los sistemas de control distribuido se asocian comúnmente con procesos continuos como la generación energía eléctrica, refinación de petróleo y gas, química, farmacéutica y fabricación de papel, así como procesos discretos tales como la fabricación, empaque y almacenamiento de automóviles y otros bienes.

3.2.45 Dominio

Entorno o contexto definido por una política de seguridad, modelo de seguridad, o arquitectura de seguridad para incluir un conjunto de recursos del sistema y el conjunto de entidades del sistema que tienen derecho de acceso a los recursos [10].

3.2.46 Espionaje

Monitoreo o registro de información comunicada por partes no autorizadas.

3.2.47 Cifrado

Transformación criptográfica de texto plano en texto cifrado que oculta los datos originales para evitar que se conozca o se use (véase 3.2.39) [10].

NOTA: Si la transformación es reversible, el proceso de reversión correspondiente se llama "descifrado", que es una transformación que restaura los datos cifrados a su estado original.

3.2.48 Empresa

Entidad comercial que produce o transporta productos u opera y mantiene infraestructura de servicios.

3.2.49 Sistema empresarial

Colección de elementos de tecnología de la información (es decir, hardware, software y servicios) instalados con la intención de facilitar el proceso o procesos comerciales de una organización (administrativos o proyecto).

3.2.50 Equipo bajo control

Equipos, maquinaria, aparatos o plantas utilizadas para la fabricación, proceso, transporte, actividades médicas u otras [13].

3.2.51 Red de E / S de campo

Enlace de comunicaciones (por cable o inalámbrico) que conecta sensores y actuadores al equipo de control.

3.2.52 Cortafuegos

Dispositivo de conexión entre redes que restringe el tráfico de comunicación de datos entre dos redes conectadas [10].

NOTA: Un firewall puede ser una aplicación instalada en una computadora de uso general o una plataforma dedicada (dispositivo) que reenvía o rechaza / descarta paquetes en una red. Por lo general, los firewalls se utilizan para definir los bordes de la zona. Los cortafuegos generalmente tienen reglas que restringen qué puertos están abiertos.

3.2.53 Puerta

Mecanismo de retransmisión que se conecta a dos (o más) redes de computadoras que tienen funciones similares, pero implementaciones diferentes y eso permite a las computadoras host en una red comunicarse con los hosts en el otro [10].

NOTA: También se describe como un sistema intermedio que es la interfaz de traducción entre dos redes de computadoras.

3.2.54 Sitio geográfico

Subconjunto del grupo de activos físicos, geográficos o lógicos de una empresa.

NOTA: Un sitio geográfico puede contener áreas, líneas de fabricación, celdas de proceso, unidades de proceso, centros de control, y vehículos y pueden estar conectados a otros sitios mediante una red de área amplia.

3.2.55 Guardia

Puerta de enlace que se interpone entre dos redes (o computadoras u otros sistemas de información) opera en diferentes niveles de seguridad (una red suele ser más segura que la otra) y es confiable para mediar en todas las transferencias de información entre las dos redes, ya sea para asegurar que la información no confidencial de la red más segura se divulgue a la red menos segura, o para proteger la integridad de los datos en la red más segura [10].

3.2.56 Host

Computadora que está conectada a una subred de comunicación o entre redes y puede usar servicios proporcionados por la red para intercambiar datos con otros sistemas conectados [10].

3.2.57 Sistemas de Automatización y Control Industrial (IACS)

Recopilación de personal, hardware y software que puede afectar o influir en la seguridad, y operación confiable de un proceso industrial.

NOTA: Estos sistemas incluyen, entre otros:

- sistemas de control industrial, incluidos los sistemas de control distribuido (DCS), controladores lógicos programables (PLC), unidades terminales remotas (RTU), dispositivos electrónicos inteligentes, control supervisado y adquisición de datos (SCADA), detección y control electrónico en red, y sistemas de monitoreo y diagnóstico. (En este contexto, Los sistemas de control de procesos incluyen funciones básicas del sistema de control de procesos y del sistema instrumentado de seguridad (SIS), si están físicamente separados o integrados).

• sistemas de información asociados, como control avanzado o multivariable, optimizadores en línea, monitoreo de equipos dedicado, interfaces gráficas, historiadores de procesos, sistemas de ejecución de fabricación y sistemas de gestión de información de planta.
• interfaces internas, humanas, de red o de máquina asociadas que se utilizan para proporcionar control, seguridad y funcionalidad de operaciones de fabricación en procesos continuos, por lotes, discretos y de otro tipo.

3.2.58 Riesgo inicial

Riesgo antes de que se hayan aplicado controles o contramedidas (véase 3.2.87).

3.2.59 Agente interno (insider)

Persona de confianza, empleado, contratista o proveedor que tiene información que generalmente no es conocido por el público (ver 3.2.74).

3.2.60 Integridad

Calidad de un sistema que refleja la corrección lógica y la confiabilidad del sistema operativo, la integridad lógica del hardware y software que implementan los mecanismos de protección, y la consistencia de las estructuras de datos y la existencia de los datos almacenados.

NOTA: En un modo de seguridad formal, la integridad a menudo se interpreta más estrictamente como protección contra modificación no autorizada o destrucción de información.

3.2.61 Intercepción (Sniffing)

Captura y divulgación del contenido del mensaje o uso de análisis de tráfico para comprometer la confidencialidad de un sistema de comunicación basado en el destino u origen del mensaje, frecuencia o duración de la transmisión y otros atributos de comunicación.

3.2.62 Interfaz

Punto de entrada o salida lógica que proporciona acceso al módulo para flujos de información lógica.

3.2.63 Intrusión

Acto no autorizado que comprometer un sistema (ver 3.2.9).

3.2.64 Detección de intrusiones

Servicio de seguridad que monitorea y analiza eventos del sistema con el propósito de encontrar y proporcionar advertencias en tiempo real o casi en tiempo real de intentos de acceder a los recursos del sistema de manera no autorizada.

3.2.65 Dirección IP

Dirección de una computadora o dispositivo asignado para identificación y comunicación utilizando el protocolo de Internet y otros protocolos.

3.2.66 ISO

Organización internacional para la estandarización

NOTA: ISO no es un acrónimo. El nombre deriva de la palabra griega iso, que significa igual.

3.2.67 Gestión de claves

Proceso de manejo y control de claves criptográficas y material relacionado (como valores de inicialización) durante su ciclo de vida en un sistema criptográfico, incluido el pedido, generar, distribuir, almacenar, cargar, custodiar, archivar, auditar y destruir las llaves y material relacionado [10].

3.2.68 Líneas, unidades, celdas

Elementos de nivel inferior que realizan funciones de fabricación, control de dispositivos de campo o vehículos.

NOTA: Las entidades en este nivel pueden estar conectadas entre sí por una red de control de área y pueden contener sistemas de información relacionados con las operaciones que se realiza en esa entidad.

3.2.69 Red de área local

Red de comunicaciones diseñada para conectar computadoras y otros dispositivos inteligentes en un área geográfica limitada (típicamente menos de 10 km) [9].

3.2.70 Código malicioso

Programas o códigos escritos con el propósito de recopilar información sobre sistemas o usuarios, destruyendo datos del sistema, proporcionando un punto de apoyo para una mayor intrusión en un sistema, falsificando datos e informes del sistema, o proporcionar irritación que consume mucho tiempo a las operaciones del sistema y personal de mantenimiento.

NOTA 1: Los ataques de código malicioso pueden tomar la forma de virus, gusanos, caballos de Troya u otras vulnerabilidades automatizadas.

NOTA 2: El código malicioso también se suele denominar "malware".

3.2.71 Operaciones de manufactura

Recopilación de operaciones de producción, mantenimiento y aseguramiento de la calidad y su relación con otras actividades de una instalación de producción.

NOTA: Las operaciones de fabricación incluyen:

- Actividades de instalaciones de fabricación o procesamiento que coordinan el personal, el equipo y el material involucrado en la conversión de materias primas o partes de productos;
- Funciones que pueden ser realizadas por equipos físicos, esfuerzo humano y sistemas de información;
- Administrar información sobre los horarios, el uso, la capacidad, la definición, el historial y el estado de todos los recursos (personal, equipo y material) dentro de las instalaciones de fabricación.

3.2.72 No repudio

Servicio de seguridad que brinda protección contra la falsa negación de participación en una comunicación [10].

3.2.73 OPC

Conjunto de especificaciones para el intercambio de información en un entorno de control de procesos.

NOTA: La abreviatura OPC originalmente vino de "OLE para Control de Procesos", donde OLE era la abreviatura de "Unir e incluir objetos".

3.2.74 Forastero, persona externa (outsider)

Persona o grupo en el que no se confía el acceso interno, que puede o no ser conocido por la organización (ver 3.2.59).

NOTA: Los agentes externos pueden o no haber sido agentes internos al mismo tiempo.

3.2.75 Penetración

Acceso exitoso no autorizado a un recurso del sistema protegido [10].

3.2.76 Suplantación de identidad

Tipo de ataque de seguridad que atrae a las víctimas a revelar información, presentando un correo electrónico falsificado a atraer al destinatario a un sitio web que parece estar asociado con una fuente legítima.

3.2.77 Texto plano

Datos no codificados que se ingresan y se transforman mediante un proceso de cifrado, o que se generan mediante un proceso de descifrado [10].

3.2.78 Privilegio

Autorización o conjunto de autorizaciones para realizar funciones específicas, especialmente en el contexto de un sistema operativo de una computadora [10].

EJEMPLO: Las funciones que se controlan mediante el uso de privilegios incluyen; reconocimiento de alarmas, cambio de puntos de ajuste y algoritmos de control de modificación.

3.2.79 Proceso

Serie de operaciones realizadas en la fabricación, tratamiento o transporte de un producto o material.

NOTA: Esta especificación técnica hace un uso extensivo del término "proceso" para describir el equipo bajo control del sistema de automatización y control industrial.

3.2.80 Protocolo

Conjunto de reglas (es decir, formatos y procedimientos) para implementar y controlar algún tipo de asociación (p. ej., comunicación) entre sistemas [10].

3.2.81 Modelo de referencia

Estructura que permite que los módulos e interfaces de un sistema se describan de manera consistente.

3.2.82 Fiabilidad

Capacidad de un sistema para realizar una función requerida bajo las condiciones establecidas por un período de tiempo específico.

3.2.83 Acceso remoto

Uso de sistemas que están dentro del perímetro de la zona de seguridad que se está abordando desde una ubicación geográfica diferente con los mismos derechos que cuando está físicamente presente en la ubicación.

NOTA: La definición exacta de "remoto" puede variar según la situación. Por ejemplo, el acceso puede provenir de una ubicación remota a la zona específica, pero aún dentro de los límites de una empresa u organización. Esto podría representar un riesgo menor que el acceso que se origina en una ubicación remota fuera de la empresa fronteras.

3.2.84 Cliente remoto

Activo fuera de la red de control que está conectado temporal o permanentemente a un host dentro la red de control a través de un enlace de comunicación para acceder directa o indirectamente a partes del equipo de control en la red de control.

3.2.85 Repudio

Negación por parte de una de las entidades involucradas en una comunicación de haber participado en todo o parte de la comunicación.

3.2.86 Riesgo residual

Riesgo restante después de que se hayan aplicado los controles de seguridad o las contramedidas.

3.2.87 Riesgo

Expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote a una particular vulnerabilidad con una consecuencia particular [10].

3.2.88 Evaluación de riesgos

Proceso que identifica sistemáticamente vulnerabilidades potenciales a recursos valiosos del

sistema y amenazas a esos recursos, cuantifica las exposiciones a pérdidas y las consecuencias en función de la probabilidad de ocurrencia, y (opcionalmente) recomienda cómo asignar recursos a contramedidas para minimizar la exposición total.

NOTA 1: Los tipos de recursos incluyen físico, lógico y humano.

NOTA 2: Las evaluaciones de riesgos a menudo se combinan con evaluaciones de vulnerabilidad para identificar vulnerabilidades y cuantificar el riesgo asociado. Se llevan a cabo inicialmente y periódicamente para reflejar los cambios en la organización, tolerancia al riesgo, vulnerabilidades, procedimientos, personal y cambios tecnológicos.

3.2.89 Gestión de riesgos

Proceso de identificación y aplicación de contramedidas acordes con el valor de los activos protegidos, basados en una evaluación de riesgos.

3.2.90 Controles de mitigación de riesgos

Combinación de contramedidas y planes de continuidad del negocio.

3.2.91 Nivel de tolerancia al riesgo

Nivel de riesgo residual que es aceptable para una organización.

3.2.92 Control de acceso basado en roles

Forma de control de acceso basado en la identidad, donde las entidades del sistema que se identifican y controlados son puestos funcionales en una organización o proceso [10].

3.2.93 Enrutador

Puerta de enlace entre dos redes en la capa 3 de OSI que retransmite y dirige paquetes de datos a entre redes. La forma más común de enrutador son los paquetes de Protocolo de Internet (IP) [10].

3.2.94 Seguridad

Nivel del riesgo inaceptable [3].

3.2.95 Sistema instrumentado de seguridad

Sistema utilizado para implementar una o más funciones instrumentadas de seguridad [3].

NOTA: Un sistema instrumentado de seguridad se compone de cualquier combinación de sensor (es), solucionador (es) lógico (s) y actuador (es).

3.2.96 Nivel de Integridad Seguro

Nivel discreto (del uno al cuatro) para especificar los requisitos de integridad de seguridad de las funciones instrumentadas de seguridad que se asignarán a los sistemas instrumentados de seguridad [3].

NOTA: El nivel de integridad de seguridad 4 tiene el nivel más alto; El nivel 1 es el más bajo.

3.2.97 Red de seguridad

Red que conecta sistemas instrumentados de seguridad para la comunicación segura de la información.

3.2.98 Secreto

Condición de que la información esté protegida de ser conocida por cualquier entidad del sistema, excepto aquellas destinado a saberlo [10].

3.2.99 Seguridad

a) medidas tomadas para proteger un sistema,
b) condición de un sistema que resulta del establecimiento y mantenimiento de medidas para proteger el sistema,
c) condición de que los recursos del sistema estén libres de acceso no autorizado y de personas no autorizadas o cambio accidental, destrucción o pérdida [10],
d) capacidad de un sistema informático para proporcionar la confianza adecuada de que las personas y los sistemas no autorizados, no pueden modificar el software y sus datos, ni acceder a funciones del sistema y, sin embargo, garantiza que esto no se le niegue a las personas y sistemas autorizados [13],

e) prevención de penetración ilegal o no deseada a, o interferencia con el destinado a realizar las operaciones previstas de un sistema de control y automatización industrial.

NOTA: Las medidas pueden ser controles relacionados con la seguridad física (control del acceso físico a los activos informáticos) o seguridad lógica (capacidad para iniciar sesión en un sistema y aplicación dada).

3.2.100 Arquitectura de seguridad

Plan y conjunto de principios que describen los servicios de seguridad que un sistema debe proporcionar para satisfacer las necesidades de sus usuarios, los elementos del sistema necesarios para implementar los servicios, y los niveles de rendimiento requeridos en los elementos para lidiar con el entorno de amenaza [10].

NOTA: En este contexto, la arquitectura de seguridad sería una arquitectura para proteger la red de control de eventos de seguridad intencionales o no intencionales.

3.2.101 Auditoria de seguridad

Revisión y examen independiente de los registros y actividades de un sistema para determinar adecuación de los sistemas control, garantizar el cumplimiento de la política y procedimientos de seguridad establecidos, detectar infracciones en los servicios de seguridad y recomendar cualquier cambio que sea indicado para contramedidas [8].

3.2.102 Componentes de seguridad

Activos como firewalls, módulos de autenticación o software de encriptación utilizados para mejorar el desempeño de seguridad de un sistema de automatización y control industrial (ver 3.2.33).

3.2.103 Control de seguridad

ver 3.2.33

NOTA: El término contramedida se ha elegido para este documento para evitar confusiones con el término "control" en el contexto del control del proceso.

3.2.104 Evento de seguridad

Ocurrencia en un sistema que es relevante para la seguridad del sistema [10].

3.2.105 Función de seguridad

Función de una zona o conducto para evitar intervenciones electrónicas no autorizadas que puedan afectar o influir en el funcionamiento normal de dispositivos y sistemas dentro de la zona o conducto.

3.2.106 Incidente de seguridad

Evento adverso en un sistema o red, o la amenaza de la ocurrencia de tal evento [9].

NOTA: El término "casi incidente" a veces se usa para describir un evento que podría haber sido un incidente bajo circunstancias ligeramente diferentes.

3.2.107 Intrusión de seguridad

Evento de seguridad o una combinación de múltiples eventos de seguridad, que constituye un incidente de seguridad en el que un intruso obtiene o intenta obtener acceso a un sistema (o recurso del sistema) sin tener autorización para hacerlo [10].

3.2.108 Nivel de seguridad

Nivel correspondiente a la efectividad requerida de contramedidas y seguridad inherente, propiedades de dispositivos y sistemas para una zona o conducto basado en la evaluación del riesgo para zona o conducto [12].

3.2.109 Objetivo de seguridad

Aspecto de seguridad cuyo propósito es usar ciertas medidas de mitigación, como la confidencialidad, integridad, disponibilidad, autenticidad del usuario, autorización de acceso, responsabilidad, etc.

3.2.110 Perímetro de seguridad

Límite (lógico o físico) del dominio en el que una política de seguridad o arquitectura de seguridad se aplica, es decir, el límite del espacio en el que los servicios de seguridad protegen los recursos del sistema [10].

3.2.111 Rendimiento de seguridad

Cumplimiento del programa, integridad de las medidas para proporcionar protección específica, análisis posterior de las amenazas, revisión y cambio de los requisitos comerciales, nuevas amenazas y vulnerabilidad de la información y auditorías periódicas de los sistemas de control para garantizar que las medidas de seguridad sigan siendo efectivas y apropiado.

NOTA: Se requieren pruebas, auditorías, herramientas, medidas u otros métodos para evaluar el desempeño en la práctica de la seguridad.

3.2.112 Política de seguridad

Conjunto de reglas que especifican o regulan cómo un sistema u organización que proporciona servicios de seguridad para proteger sus activos [10].

3.2.113 Procedimientos de seguridad

Definiciones que indican exactamente cómo se implementan y ejecutan en la práctica.

NOTA: Los procedimientos de seguridad se implementan a través de acciones de entrenamiento y capacitación del personal, utilizando la tecnología actualmente disponible e instalada.

3.2.114 Programa de seguridad

Combinación de todos los aspectos de la gestión de la seguridad, desde la definición y la comunicación de políticas a través de la implementación de las mejores prácticas de la industria, operación continua y auditoría.

3.2.115 Servicios de seguridad

Mecanismos utilizados para proporcionar confidencialidad, integridad de datos, autenticación o no repudio de información [10].

3.2.116 Violación de seguridad

Acto o evento que desobedece o viola la política de seguridad a través de una intrusión o acciones de un agente interno.

3.2.117 Zona de seguridad

Agrupación de activos lógicos o físicos que comparten requisitos de seguridad comunes.

NOTA 1: Se debe suponer que todos los usos no calificados del término "zona" en este documento se refieren a una zona de seguridad.

NOTA 2: Una zona tiene un borde claro con otras zonas. La política de seguridad de una zona generalmente se hace cumplir por una combinación de mecanismos tanto en el borde de la zona como dentro de la zona. Las zonas pueden ser jerárquicas en el sentido de que pueden estar formados por una colección de subzonas.

3.2.118 Sensores y actuadores

Elementos de medición o actuación conectados al equipo de proceso y al sistema de control.

3.2.119 Servidor

Dispositivo o aplicación que proporciona información o servicios a las aplicaciones y dispositivos del cliente [10].

3.2.120 Rastreador (Sniffing)

ver 3.2.61

3.2.121 Suplantación de identidad (Spoof)

Pretender ser un usuario autorizado y realizar una acción no autorizada [10].

3.2.122 Sistema de control supervisado y adquisición de datos (SCADA)

Tipo de sistema de monitoreo y control distribuido débilmente acoplado comúnmente asociado con sistemas de transmisión y distribución de energía eléctrica, oleoductos y gasoductos, agua y sistemas de alcantarillado.

NOTA: Los sistemas de control de supervisión también se utilizan en plantas de fabricación discontinua, continua y discreta para centralizar las actividades de monitoreo y control de estos sitios.

3.2.123 Sistema

Elementos interactivos, interrelacionados o interdependientes que forman un todo complejo.

3.2.124 Software del sistema

Software especialmente diseñado para un sistema informático específico o una familia de sistemas informáticos para facilitar la operación y el mantenimiento del sistema informático y los programas asociados y datos [11].

3.2.125 Amenaza

Potencial de violación de la seguridad, que existe cuando existe una circunstancia, capacidad, acción o evento que podría violar la seguridad y causar daños [10].

3.2.126 Acción de amenaza
Asalto a la seguridad del sistema [10].

3.2.127 Agente de amenaza
Agente causal de una acción de amenaza.

3.2.128 Análisis de tráfico

Inferencia de información de características observables de flujo (s) de datos, incluso cuando los datos están encriptados o no están disponibles directamente, incluidas las identidades y ubicaciones de fuente (s) y destino (s) y la presencia, cantidad, frecuencia y duración de ocurrencia.

3.2.129 Caballo de Troya

Programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente función maliciosa que evade los mecanismos de seguridad, a veces explotando legítimamente autorizaciones de una entidad del sistema que invoca el programa [10].

3.2.130 Canal de confianza
Enlace de comunicación que puede proporcionar una comunicación segura entre zonas de seguridad.

3.2.131 Canal no confiable

Enlace de comunicación que no puede proporcionar una comunicación segura entre zonas de seguridad.

3.2.132 Caso de uso

Técnica para capturar requisitos funcionales potenciales que emplea el uso de uno o más escenarios que transmiten cómo debe interactuar el sistema con el usuario final u otro sistema para lograr un objetivo específico.

NOTA: Normalmente, los casos de uso tratan el sistema como una caja negra y las interacciones con el sistema, incluido el sistema de respuestas que se percibe desde fuera del sistema. Los casos de uso son populares porque simplifican descripción de los requisitos y evitar el problema de hacer suposiciones sobre cómo será esta funcionalidad consumada.

3.2.133 Usuario

Persona, entidad de organización o proceso automatizado que accede a un sistema, ya sea autorizado hacerlo o no [10].

3.2.134 Virus

Programa de autorreplicable o autoreproducible que se propaga insertando copias de sí mismo en otro código ejecutable o documentos.

3.2.135 Vulnerabilidad

Falla o debilidad en el diseño, implementación u operación y administración de un sistema que podría ser explotado para violar la integridad del sistema o la política de seguridad [10].

3.2.136 Red de área amplia

Red de comunicaciones diseñada para conectar computadoras, redes y otros dispositivos a través de una gran distancia, como a través de un país o el mundo [11].

3.2.137 Intervención a la línea

Ataque que intercepta y accede a datos y otra información contenida en un flujo en un sistema de comunicación [10].

NOTA 1: Aunque el término originalmente se refería a hacer una conexión mecánica a un conductor eléctrico que enlaza dos nodos, ahora se usa para referirse a la lectura de información de cualquier tipo de medio utilizado un enlace o incluso directamente desde un nodo, como una puerta de enlace o un conmutador de subred.

NOTA 2: Las escuchas telefónicas activas intentan alterar los datos o afectar el flujo de otra manera, mientras las escuchas telefónicas pasivas solo intentan observar el flujo y obtener conocimiento de la información que contiene.

3.2.138 Gusano

Programa informático que puede ejecutarse de forma independiente, puede propagar una versión de trabajo completa a otros hosts en una red y puede consumir recursos informáticos de forma destructiva [10].

3.2.139 Zona

ver 3.2.117

NOTA: Se debe suponer que todos los usos no calificados del término "zona" en este documento se refieren a una zona de seguridad.

3.3 Abreviaturas

Esta subcláusula define las abreviaturas utilizadas en esta especificación técnica.

ANSI: Instituto Nacional Americano de Normas
CIA: Confidencialidad, integridad y disponibilidad
CN: Control Network
COTS: Comercial fuera de la plataforma
CSMS: Sistema de gestión de ciberseguridad
DCS: Sistema de control distribuido
DDoS: Denegación de servicio distribuida
DoS: denegación de servicio

DMZ: Zona desmilitarizada
FIPS: U. S. Normas federales de procesamiento de información
IACS: Sistemas de Automatización y Control Industrial
IEC: Comisión Electrotécnica Internacional
IEEE: Instituto de Ingenieros Eléctricos y Electrónicos
E / S: Entrada / salida
IP: Protocolo de internet
TI: Tecnología de la información
LAN: Red de área local
NASA: U. S. Administración Nacional de Aeronáutica y del Espacio
NOST: Oficina de Normas y Tecnología de la NASA
OSI: Sistemas abiertos de interconexión
PLC: Controlador lógico programable
RTU: Unidad terminal remota
SCADA: Control supervisado y adquisición de datos
SIL: Nivel de seguridad integridad
SIS: Sistema instrumentado de seguridad
WAN: Red de área amplia

4 La situación

4.1 General

Los sistemas de automatización y control industrial operan dentro de un entorno complejo. Las organizaciones comparten cada vez más información entre las empresas y la automatización industrial del sistema, socios en una empresa comercial pueden ser competidores en otra. Sin embargo, los equipos de sistemas de automatización y control industrial se conectan directamente a un proceso, la pérdida de secretos comerciales y la interrupción en el flujo de información no son las únicas consecuencias de una violación de seguridad. La pérdida potencial de vida o la producción, daños ambientales, violación de regulaciones y el compromiso con la seguridad operativa son consecuencias mucho más graves. Estas pueden tener ramificaciones más allá de la organización objetivo; pueden dañar gravemente la infraestructura de la región o nación anfitriona.

Las amenazas externas no son la única preocupación; Los agentes internos conocedoras con intenciones maliciosas o incluso un acto inocente involuntario pueden representar un grave riesgo de seguridad. Además, los sistemas de automatización y control industrial a menudo se integran con otros sistemas comerciales. La modificación o prueba de los sistemas operativos ha provocado efectos electrónicos no deseados en las operaciones del sistema. El personal externo al área de sistemas de control realiza cada vez más pruebas de seguridad en los sistemas, exacerbando el número y las consecuencias de estos efectos. Combinando todos estos factores, es fácil ver que el potencial de que alguien obtenga acceso no autorizado o perjudicial a un proceso industrial no es trivial

Aunque los cambios tecnológicos y las relaciones con los socios pueden ser buenos para los negocios, aumentar el riesgo potencial de comprometer la seguridad. A medida que aumentan las amenazas a las empresas, también lo hace la necesidad de seguridad.

4.2 Sistemas actuales

Los sistemas de control y automatización industrial han evolucionado de computadoras individuales y aisladas con sistemas operativos y redes propietarias a sistemas y aplicaciones interconectadas empleando tecnología comercial estándar (COTS) (es decir, sistemas operativos y protocolos). Estos sistemas ahora se están integrando con sistemas empresariales y otras aplicaciones de negocios a través de diversas redes de comunicación. Este mayor nivel de integración proporciona importantes beneficios comerciales, incluidos los siguientes:

a) mayor visibilidad de las actividades del sistema de control industrial (trabajo en proceso, estado del equipo, programas de producción) y sistemas de procesamiento integrados desde el nivel empresarial, contribuyendo a la capacidad mejorada de realizar análisis para reducir los costos de producción y mejorar la productividad;
b) sistemas integrados de fabricación y producción que tienen un acceso más directo a los niveles de información del negocio, lo que permite una empresa más receptiva;
c) interfaces comunes que reducen los costos generales de soporte y permiten el soporte remoto a los procesos de producción;
d) monitoreo remoto de los sistemas de control de procesos que reduce los costos de soporte y permite resolver problemas más rápidamente.

Es posible definir estándares para modelos, términos e intercambios de información que permitan a los Sistemas de Automatización y Control Industrial comunicarse para compartir información por una vía consistente. Sin embargo, esta capacidad de intercambiar información aumenta la vulnerabilidad al error y al ataque de individuos con intenciones maliciosas e introduce riesgos potenciales para la empresa usuaria de los Sistemas de Automatización y Control Industrial.

La configuración de los Sistemas de Automatización y Control Industrial pueden ser muy complejas en términos de hardware físico, programación y comunicaciones. Esta complejidad a menudo puede hacer difícil determinar los siguientes puntos:

- quién está autorizado para acceder a la información electrónica;
- cuando un usuario puede tener acceso a la información;
- a qué datos o funciones debe poder acceder un usuario;
- dónde se origina la solicitud de acceso;
- cómo se solicita el acceso.

4.3 Tendencias actuales

Varias tendencias contribuyen con mayor énfasis en la seguridad de a Sistemas de Automatización y Control Industrial:

a) En los últimos años ha habido un marcado aumento en los ataques de códigos maliciosos en los negocios y sistemas informáticos personales. Las empresas han reportado más intentos no autorizados (ya sea intencional o no) para acceder a información electrónica cada año que en el año anterior

b) Los sistemas de automatización y control industrial se están moviendo hacia los sistemas operativos y protocolos COTS y se interconectan con redes comerciales. Esto está haciendo estos sistemas susceptibles a los mismos ataques de software que los presentes en las empresas y los dispositivos de mesa.
c) Las herramientas automáticas para ataques están comúnmente disponibles en Internet. La amenaza externa del uso de estas herramientas ahora incluye a los ciberdelincuentes y ciberterroristas que pueden tener más recursos y conocimientos para atacar un sistema de automatización y control industrial.
d) El uso de conjuntos de empresas, alianzas de socios y servicios subcontratados en el sector industrial ha llevado a una situación más compleja con respecto al número de organizaciones y grupos contribuyendo a la seguridad del sistema de automatización y control industrial. Estas prácticas deben tenerse en cuenta al desarrollar seguridad para estos sistemas.
e) El enfoque en los accesos no autorizado se ha ampliado de atacantes aficionados o empleados descontentos a actividades criminales o terroristas deliberadas destinadas a impactar a grandes grupos e instalaciones.
f) La adopción por la industria de protocolos de documentos como el Protocolo de Internet (IP) para comunicación entre los Sistemas de Automatización y Control Industrial y dispositivos de campo. La implementación IP expone estos sistemas a las mismas vulnerabilidades que los sistemas empresariales en la capa de red.

Estas tendencias se han combinado con un incremento significativo de organizaciones de riesgos asociadas con el diseño y operación de Sistemas de Automatización y Control Industrial. Al mismo tiempo, la ciberseguridad de los sistemas de control industrial se ha convertido en una preocupación más significativa y reconocida ampliamente. Este cambio requiere pautas y procedimientos más estructurados para definir la ciberseguridad aplicable a la automatización industrial y sistemas control, así como a la respectiva conectividad a otros sistemas.

4.4 Impacto potencial

Las personas que conocen las características de los sistemas operativos y redes abiertos podrían potencialmente entrometerse en dispositivos de consola, dispositivos remotos, bases de datos y, en algunos casos, controlar plataformas. El efecto de los intrusos en la automatización industrial y sistemas control puede incluir los siguientes:

a) acceso no autorizado, robo o mal uso de información confidencial;
b) publicación de información a destinos no autorizados;
c) pérdida de integridad o fiabilidad de los datos del proceso y la información de producción;
d) pérdida de disponibilidad del sistema;
e) alteraciones del proceso que conducen a una funcionalidad del proceso comprometida, inferior calidad del producto, pérdida de capacidad de producción, seguridad de proceso comprometida o emisiones al medio ambiente;
f) daños a equipo;
g) lesiones personales;
h) violación de los requisitos legales y reglamentarios;
i) riesgo para la salud pública y la confianza;
j) amenaza a la seguridad de una nación.

5 Conceptos

5.1 General

Esta cláusula describe varios conceptos subyacentes que forman la base de las siguientes cláusulas y para otros estándares en la serie IEC 62443. Específicamente, aborda preguntas como:

a) ¿Cuáles son los conceptos principales que se utilizan para describir la seguridad?
b) ¿Cuáles son los conceptos importantes que forman la base para un programa comprensible de seguridad?

5.2 Objetivos de seguridad

La seguridad de la información se ha centrado tradicionalmente en lograr tres objetivos, confidencialidad, integridad y disponibilidad, que a menudo se abrevian con el acrónimo CIA (por sus siglas en ingles). Una estrategia de seguridad de tecnología de la información para típicas oficinas administrativas o los sistemas empresariales puede colocar el foco principal centrado en la confidencialidad y los controles de acceso necesarios para lograrlo. La integridad podría caer a la segunda prioridad, con disponibilidad como la más baja.

En el entorno de los Sistemas de Automatización y Control Industrial, la prioridad general de estos, son a menudo objetivos diferentes. La seguridad en estos sistemas se ocupa principalmente de mantener la disponibilidad de todos los componentes del sistema. Existen riesgos inherentes asociados con la industria, maquinaria controlada, supervisada o afectada por los Sistemas de Automatización y Control Industrial. Por lo tanto, la integridad es a menudo la segunda en importancia. Por lo general, la confidencialidad es de menor importancia, porque a menudo los datos son de forma cruda y deben analizarse dentro de contexto para tener algún valor.

La faceta del tiempo de respuesta es significativa. Los sistemas de control pueden tener requisitos de capacidad de respuesta del sistema en el rango de un milisegundo, mientras que los sistemas comerciales tradicionales son capaces de operar con éxito con tiempos de respuesta únicos o múltiples segundos.

En algunas situaciones, las prioridades están completamente invertidas, como se muestra en la Figura 1.

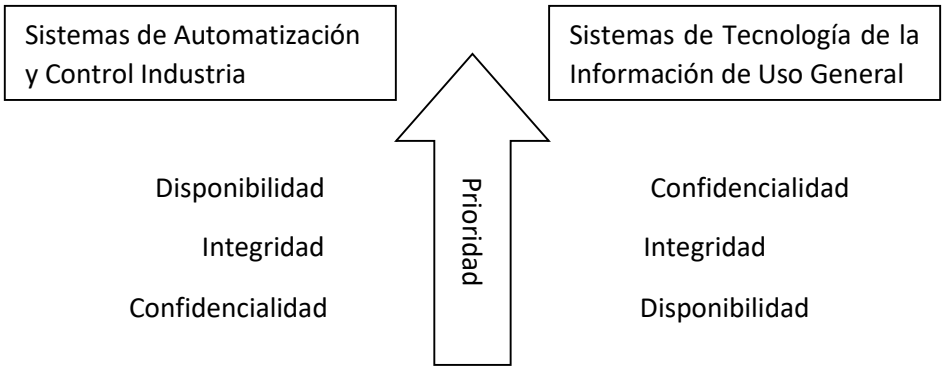

Figura 1 - Comparación de objetivos entre IACS y sistemas informáticos generales

Dependiendo de las circunstancias, la integridad del sistema también podría tener la mayor prioridad. Ciertos requisitos operativos causarían componentes individuales o sistemas como un conjunto que tienen diferentes prioridades para los objetivos (es decir, las preocupaciones de integridad o disponibilidad pueden superar la confidencialidad, o viceversa). Esto a su vez puede llevar a una organización a desplegar diferentes contramedidas para lograr estos objetivos de seguridad.

5.3 Requisitos fundamentales

El modelo simple de la CIA que se muestra en la Figura 1 no es adecuado para una comprensión completa de los requisitos de seguridad en Sistemas de Automatización y Control Industrial. Aunque está más allá el alcance de esta especificación técnica para describir una lista exhaustiva de requisitos detallados, hay varios requisitos básicos o fundamentales que se han identificado para la seguridad de la Automatización Industrial. Estos son los siguientes requisitos:

a) Control de acceso (AC): controla el acceso a dispositivos seleccionados, información o ambos para proteger contra la interrogación no autorizada del dispositivo o la información.
b) Control de uso (UC): controla el uso de dispositivos seleccionados, información o ambos para proteger contra operaciones no autorizada del dispositivo o uso de información.
c) Integridad de datos (DI): garantizar la integridad de los datos en los canales de comunicación seleccionados para proteger contra cambios no autorizados.
d) Confidencialidad de datos (DC): garantizar la confidencialidad de los datos en los canales comunicación seleccionados para protegerse contra las escuchas.
e) Restringir flujo de datos (RDF): restringir el flujo de datos en los canales de comunicación para proteger contra la publicación de información a fuentes no autorizadas.
f) Respuesta oportuna al evento (TRE): responda a las violaciones de seguridad notificando a la autoridad, informar evidencia forense necesaria de la violación y tomar automáticamente acción correctiva oportuna en situaciones de misión crítica o seguridad crítica.
g) Disponibilidad de recursos (RA): garantizar la disponibilidad de todos los recursos de red para proteger contra ataques de denegación de servicio.

Todos estos requisitos están dentro del alcance de esta especificación técnica, aunque en algunos casos se proporcionará información normativa más detallada por otras normas en el Serie IEC 62443. Por ejemplo, requisitos técnicos como integridad de los datos y confidencialidad de los datos se abordará en detalle en una parte futura de IEC 62443.

5.4 Defensa en profundidad

Por lo general, no es posible lograr los objetivos de seguridad mediante el uso solo de contramedida o técnica. Un enfoque superior es utilizar el concepto de defensa en profundidad, que implica aplicar múltiples contramedidas de manera escalonada o por pasos. Por ejemplo, los sistemas de detección de intrusos se pueden utilizar para señalar la penetración de un firewall.

5.5 Contexto de seguridad

El contexto de seguridad forma la base para la interpretación de terminología y conceptos y muestra cómo los diversos elementos de seguridad se relacionan entre sí. El término seguridad es considerado aquí como la prevención de la penetración o interferencia ilegal o no deseada de la

operación adecuada y prevista de un Sistema de Automatización y Control Industrial. La ciberseguridad incluye la computadora, la red u otros componentes programables del sistema.

El contexto de seguridad se basa en los conceptos de amenazas, riesgos y contramedidas, así como las relaciones entre ellos. La relación entre estos conceptos se puede mostrar en un modelo simple. Uno de estos modelos, descrito en ISO / IEC 15408-1 (Criterios Comunes), se reproduce en la Figura 2. Una vista diferente de la relación se muestra en la Figura 3

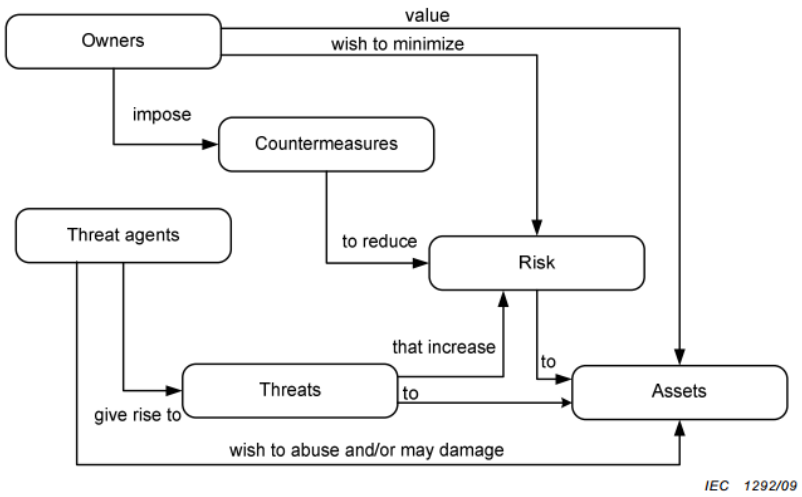

Figure 2 – Context element relationships

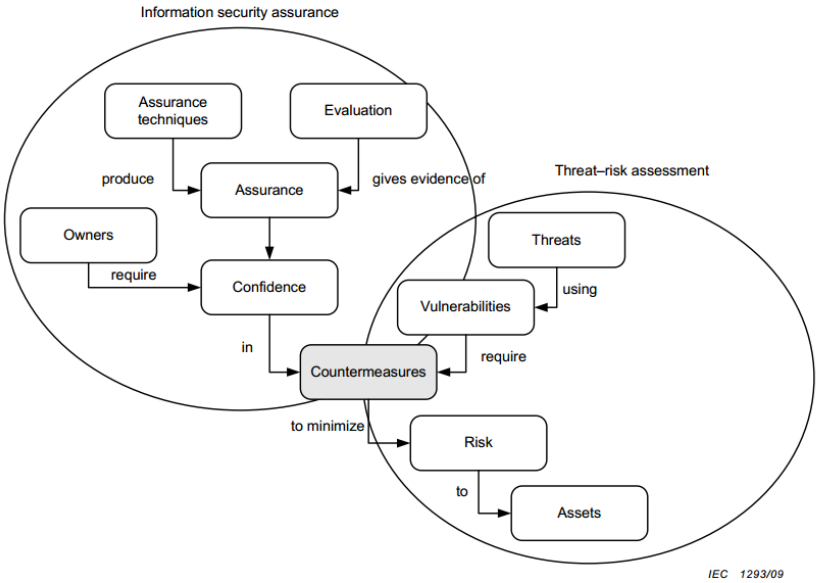

Figure 3 – Context model

Figura 3 - Modelo de contexto

El modelo de contexto de la Figura 3 muestra cómo se relaciona un conjunto ampliado de conceptos dentro de dos procesos interconectados de garantía de seguridad de la información y evaluación del riesgo de amenazas.

5.6 Evaluación del riesgo de amenaza

5.6.1 General

Dentro del proceso de evaluación del riesgo de amenaza, los activos están sujetos a riesgos. Estos riesgos son a su vez minimizado, mediante el uso de contramedidas, que se aplican para abordar vulnerabilidades que son utilizadas o explotadas por diversas amenazas. Cada uno de estos elementos se describe con más detalle en las siguientes subcláusulas.

5.6.2 Activos

5.6.2.1 Descripción general

Los activos son el foco de un programa de seguridad. Son lo que se está protegiendo. Con el fin de comprender el riesgo para un entorno IACS, primero es necesario crear un inventario de activos que requieren protección. Los activos pueden clasificarse en físicos, lógicos o humanos.

a) Activos físicos: los activos físicos incluyen cualquier componente físico o grupo de componentes pertenecientes a una organización. En el entorno industrial, estos pueden incluir sistemas de control, componentes físicos de red y medios de transmisión, sistemas de transporte, paredes, habitaciones, edificios, materiales u otros objetos físicos que estén involucrados de alguna manera con el control, monitoreo o análisis de los procesos de producción o en apoyo de los negocios en general. Los activos físicos más significativos son aquellos que componen el equipo que está bajo el control del sistema de automatización.
b) Activos lógicos: los activos lógicos son de naturaleza informativa. Pueden incluir propiedad intelectual, algoritmos, prácticas propietarias, conocimiento específico del proceso u otros elementos informativos que encapsulan la capacidad de una organización para operar o innovar. Además, estos tipos de activos pueden incluir reputación pública, confianza del comprador u otras medidas que, si son dañadas, afectan directamente al negocio. Los activos lógicos pueden estar en la forma de memoria personal, documentos, información contenida en medios físicos o electrónicos, registros de almacenamiento relacionados con el activo informativo. Los activos lógicos también pueden incluir pruebas, resultados, datos de cumplimiento normativo o cualquier otra información considerada confidencial o propietaria, o que podría proporcionar o producir una ventaja competitiva. La pérdida de activos lógicos a menudo causa efectos muy duraderos y perjudiciales para una organización.
   Los activos de automatización de procesos son una forma especial de activos lógicos. Contienen la lógica de automatización empleada en la ejecución del proceso industrial. Estos procesos son altamente dependientes de la ejecución repetitiva o continua de eventos definidos con precisión. El compromiso de los activos del proceso podría ser físico (por ejemplo, destrucción de medios) o no físicos (p. ej., modificación no autorizada), y resultan algún tipo de pérdida de integridad o disponibilidad del proceso en sí.
c) Activos humanos: los activos humanos incluyen a las personas y los conocimientos y habilidades que poseen asociados con sus actividades de producción. Pueden incluir

certificaciones requeridas, conocimiento específico del equipo u otras actividades no incluidas en la producción automatizada, procesos o habilidades importantes necesarias durante emergencias. Rara vez son procesadas instalaciones completamente automatizadas y la interrupción de las operaciones realizadas por personas podría tener un impacto importante en la producción, aunque los sistemas físicos y lógicos permanecen relativamente intacto. Por ejemplo, una alarma de planta errónea podría hacer que el personal inicie el cierre y evacuación de la planta, aunque nada fue interrumpido física o lógicamente en el Sistemas Control y Automatización Industrial. Cualquier accidente o ataque que hiera a una persona sería considerado como un impacto en un activo humano.

5.6.2.2 Valoración de activos

Para cumplir con los requisitos de un activo físico o lógico, el objeto debe ser propiedad de la organización o estar bajo su custodia. También necesita tener valor para la organización. El valor del activo puede expresarse en términos cualitativos o cuantitativos. Algunas organizaciones también considerarán la valoración cualitativa como un razonamiento adecuado para expresar la pérdida de activos en el proceso de análisis de riesgos.

a) Valoración cuantitativa de los activos: un activo dado una valoración cuantitativa tiene una pérdida monetaria precisa asociada. Esto podría ser en términos de costo de reemplazo, costo de ventas perdidas u otras medidas monetarias. El análisis cuantitativo requiere un análisis de costos riguroso para obtener un número preciso, pero le brinda a la organización una imagen mucho más clara del impacto potencial de una pérdida.
b) Valoración cualitativa de los activos: la pérdida cualitativa generalmente expresa un nivel de pérdida más abstracto, como un porcentaje o un valor relativo, como bajo impacto, alto impacto o ningún impacto. Muchos activos solo pueden analizarse en términos de pérdida cualitativa. El inicio de un proceso de evaluación de riesgos puede comenzar con una valoración cualitativa de los activos para documentar los riesgos de alto nivel y para justificar el argumento comercial de gastar dinero en remediación para reducir un riesgo, y luego contar con el respaldo de un análisis cuantitativo para obtener una imagen detallada de la exposición al riesgo.

El valor puede clasificarse según el tipo de pérdida incurrida, ya sea directa o indirecta.

c) Pérdida directa: la pérdida directa representa el costo de reemplazar el activo. Para un activo físico, esto podría incluir el costo de reemplazo del dispositivo en sí. Los activos lógicos tienen comparativamente baja pérdida directa en comparación con su valor de utilidad, porque el medio utilizado para almacenar el activo es típicamente de bajo costo.
d) Pérdida indirecta: la pérdida indirecta representa cualquier pérdida causada por la pérdida del activo que la organización puede realizar. Esto podría incluir pérdidas relacionadas con el tiempo de inactividad del proceso, repetición de trabajo u otros costos de producción debido a la pérdida del activo. Las pérdidas indirectas de activos físicos generalmente incluyen efectos posteriores debido a la pérdida del componente. Las pérdidas indirectas de activos lógicos son a menudo grandes. Incluyen la pérdida de la confianza del público, la pérdida de la licencia para operar debido a una violación de las normas y la pérdida de la ventaja competitiva de la liberación de la propiedad intelectual (por ejemplo, tecnología de proceso confidencial).

5.6.2.3 Categorización de la pérdida

Al combinar la información sobre los tipos de activos y la valoración, es posible mostrar los tipos de pérdidas por cada tipo de activo. Esto se resume en la Tabla 1

Tabla 1 - Tipos de pérdida por tipo de activo

Tipo de activo	Pérdida directa	Pérdida indirecta	Cualitativa o cuantitativa
Físico	Puede ser una pérdida directa alta, representada por el costo de reemplazo del activo. La pérdida directa proviene del daño a los activos físicos como resultado de la pérdida de integridad o disponibilidad, y la interrupción de la secuencia precisa o la naturaleza consistente de un proceso.	Efectos posteriores como resultado de la pérdida, incluida la pérdida de control, pérdida o daño a otros activos y pérdidas por tiempo de inactividad.	Cualitativo o cuantitativo, puede comenzar con cualitativo para riesgos de alto nivel, y luego ser cuantitativo para mayor precisión.
Lógica	Baja pérdida directa, ya que los medios de almacenamiento a menudo son baratos y fácilmente reemplazables.	Pérdida indirecta alta, a menudo debido a la pérdida de propiedad intelectual, compromiso de procedimientos patentados o violación del cumplimiento normativo. Las pérdidas indirectas causadas por daños en el equipo o la liberación de material pueden ocasionar tiempo de inactividad, retrabajo, reingeniería u otros esfuerzos para restablecer el control sobre el proceso industrial.	Principalmente cualitativo, pero algunos efectos posteriores pueden ser cuantitativos.
Humano	Pérdida directa de baja a media dependiendo de la extensión de la lesión a la persona. Las lesiones menores con tiempos de recuperación cortos pueden tener un impacto de baja pérdida directa para la compañía, aunque la lesión puede tener un impacto duradero en la persona que está lesionada.	Pérdida indirecta de baja a alta dependiendo de la extensión de la lesión y la importancia de la persona para el proceso. Los costos de horas extras y los costos de reemplazo temporal pueden variar considerablemente dependiendo del tiempo de recuperación del individuo. Las lesiones incapacitantes permanentes o la muerte pueden tener altos costos de pérdida indirecta cuando la responsabilidad social y los posibles litigios y laudos se tienen en cuenta en la evaluación.	Impacto cualitativo inmediato en la producción seguido de un impacto cuantitativo para la recuperación o el reemplazo.

5.6.3 Vulnerabilidades

En términos simples, las vulnerabilidades son debilidades inherentes en los sistemas, componentes u organizaciones.

Las vulnerabilidades pueden ser el resultado de elecciones de diseño intencionales o pueden ser accidentales, como resultado de la falta de comprensión del entorno operativo. También pueden surgir a medida que el equipo envejece y eventualmente se vuelve obsoleto, lo que ocurre en un tiempo más corto que el típico para el proceso subyacente o el equipo bajo control. Las vulnerabilidades no se limitan a los sistemas electrónicos o de red. Comprender la interacción entre

las vulnerabilidades físicas (incluidas las humanas) y electrónicas es fundamental para establecer una seguridad de sistema de control y automatización industrial efectiva.

Un sistema de automatización y control industrial que inicialmente tiene una vulnerabilidad limitada puede volverse más vulnerable con situaciones tales como un entorno cambiante, tecnología cambiante, falla de componentes del sistema, falta de disponibilidad de reemplazos de componentes, rotación de personal y mayor inteligencia de amenazas.

5.6.4 Riesgo

5.6.4.1 Descripción general

El riesgo generalmente se define como una expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad particular con una consecuencia particular. El riesgo es una función de amenaza, vulnerabilidad y consecuencia, donde la consecuencia es el impacto negativo que experimenta la organización debido al daño específico al activo o los activos de la organización por la amenaza o vulnerabilidad específica. Los componentes de amenaza y vulnerabilidad se pueden expresar en términos de probabilidad. La probabilidad es la probabilidad de que ocurra una acción específica.

Los propietarios de activos deben clasificar e incluir el costo de mitigación o el costo de reparación en su estimación de riesgo. También deben determinar las contramedidas apropiadas para mitigar la mayor cantidad de exposiciones de seguridad para la menor exposición financiera.

Cualquier metodología sólida de evaluación de riesgos debe analizar todos los sistemas involucrados en un enfoque por capas, comenzando con los sistemas más cercanos a la amenaza y trabajando hacia adentro. El proceso básico de evaluación de riesgos consta de tres pasos:

1) evaluar el riesgo inicial;
2) implementar contramedidas de mitigación de riesgos;
3) evaluar el riesgo residual.

Los pasos 2 y 3 de este proceso se repiten según sea necesario para reducir el riesgo residual a un nivel aceptable. Específicamente, el segundo paso incluye evaluar los controles existentes e implementar planes para agregar medidas correctivas o contramedidas adicionales. Se proporcionará una descripción más detallada del proceso de determinación de riesgos en una parte futura de IEC 62443.

Los riesgos típicos considerados incluyen los siguientes:

a) riesgos de seguridad del personal, como muerte o lesiones;
b) riesgos de seguridad del proceso, como daños en el equipo o interrupción del negocio;
c) riesgos de seguridad de la información como el costo, violaciones legales o pérdida de imagen de marca;
d) riesgo ambiental tal como aviso de violación, violaciones legales o impacto importante;
e) riesgos de continuidad del negocio, como la interrupción del negocio.

5.6.4.2 Nivel de tolerancia al riesgo

El resultado de un análisis de riesgo cualitativo consistirá en una lista de activos o escenarios con una probabilidad general y una clasificación de consecuencia. Es responsabilidad de la gerencia determinar la respuesta adecuada a los elementos en función de estas clasificaciones. Algunas organizaciones aceptan niveles de riesgo relativamente altos (como las empresas de crecimiento agresivo), mientras que algunas empresas son inherentemente conservadoras en cuanto a ser adversas al riesgo. Por lo tanto, un cierto nivel de riesgo residual puede ser aceptable para una organización y no para otra. Incluso dentro de la misma compañía, las plantas individuales pueden exhibir diferentes resignación o tolerancia de riesgo. La gerencia debe definir y comprender explícitamente cuál es su resignación o tolerancia al riesgo, para que pueda analizar mejor su nivel de respuesta a los riesgos residuales identificados.

Abordar la seguridad de los sistemas de automatización y control industrial, en general, no introduce nuevos riesgos, pero puede contribuir a una perspectiva diferente de los riesgos existentes. Por ejemplo, los riesgos relacionados con la seguridad suelen recibir más atención en un contexto de automatización industrial.

La seguridad de los Sistemas de Control y Automatización Industrial no necesita reinventar un proceso para definir el nivel de tolerancia al riesgo; simplemente se deriva de otras prácticas de gestión de riesgos en la organización.

5.6.4.3 Respuesta al riesgo

Hay varias respuestas potenciales al riesgo. Las organizaciones pueden tomar alguna combinación de acciones en cada situación, según las circunstancias.

a) Reducir el riesgo de diseño: una forma de mitigación es cambiar el diseño del sistema para eliminar el riesgo. Existen algunos riesgos simplemente porque el acceso está disponible para algo a lo que nunca se necesita acceso. Deshabilitar completamente la función innecesaria o soldar la función del acceso puede mitigar el riesgo. Las organizaciones pueden tomar las decisiones comerciales apropiadas para que no se corra el riesgo. Esta respuesta puede implicar decir no a algo, ya sea un nuevo producto, sistema o relación de proveedor.
b) Reduzca el riesgo: los riesgos pueden reducirse a un nivel aceptable mediante la implementación de contramedidas que reducen la probabilidad o consecuencia de un ataque. La clave aquí es lograr un nivel de seguridad suficientemente bueno, no eliminar el riesgo.
c) Aceptar el riesgo: siempre hay una opción para aceptar el riesgo, para verlo como el costo de hacer negocios. Las organizaciones deben asumir algunos riesgos, y no siempre pueden mitigarse o transferirse de manera rentable.
d) Transfiera o comparta el riesgo: puede ser posible establecer algún tipo de seguro o acuerdo que transfiera parte o la totalidad del riesgo a una tercera entidad. Un ejemplo típico de esto es la externalización de funciones o servicios específicos. Este enfoque no siempre puede ser efectivo, porque no siempre puede cubrir todos los activos por completo. Una política de ciberseguridad puede recuperar ciertos daños, pero no activos lógicos como la pérdida de confianza del cliente.

e) Eliminar o rediseñar controles redundantes o ineficaces: un buen proceso de evaluación de riesgos identificará este tipo de controles que deben abordarse para que se pueda centrar más la atención en controles que sean efectivos y eficientes.

5.6.5 Amenazas

5.6.5.1 Descripción general

Las amenazas describen las posibles acciones que se pueden tomar contra un sistema. Vienen en muchas formas diferentes, pero dos de las formas más comunes son:

a) Accidental: alguien que no esté familiarizado con el procedimiento y las políticas adecuadas o una supervisión honesta provoca un riesgo accidental. También es probable que una organización no conozca todos los riesgos y pueda descubrirlos por accidente, ya que opera Sistemas de Control y Automatización Industrial complejos.
b) Cambios no validados: las actualizaciones, correcciones y otros cambios en los sistemas operativos, los programas de aplicación, las configuraciones, la conectividad y el equipo pueden proporcionar una amenaza de seguridad inesperada para los Sistemas de Control y Automatización Industrial o la producción respectiva.

Agente de amenaza es el término utilizado para describir la entidad que presenta una amenaza. También son conocidos como adversarios o atacantes. Los agentes de amenaza vienen en muchas formas diferentes. Ejemplos:

c) Agente interno: un agente interno es una persona, empleado, contratista o proveedor de confianza que tiene información que generalmente no es conocida por el público. Un agente interno puede representar una amenaza incluso si no hay intención de hacer daño. Por ejemplo, la amenaza puede surgir como resultado de un agente interno que omite los controles de seguridad para hacer el trabajo.
d) Agente Externo: un agente externo es una persona o grupo en el que no se confía el acceso interno, que puede o no ser conocida por la organización objetivo. Los de afuera pueden o no haber sido de adentro al mismo tiempo.
e) Natural: los eventos naturales incluyen tormentas, terremotos, inundaciones y tornados, y generalmente se consideran una amenaza física

Las amenazas que se convierten en acción se conocen como ataques (a veces referidos como una intrusión). Ya sea diseñando componentes y sistemas o implementando un programa de seguridad dentro de un sitio u organización, es posible modelar ataques con el fin de garantizar que existan contramedidas para identificarlos y disuadirlos. El modelado de casos y los árboles de ataque son ejemplos de métodos que pueden usarse.

Las amenazas pueden ser pasivas o activas. Cada tipo se describe en las siguientes subcláusulas.

5.6.5.2 Amenazas pasivas

La recopilación pasiva de información puede proporcionar a un intruso potencial información valiosa. Los agentes de amenazas generalmente recopilan información pasiva mediante comunicaciones verbales casuales con empleados y contratistas. Sin embargo, las personas dentro o fuera de las instalaciones también pueden recopilar información pasiva con observaciones

visuales. La recopilación pasiva de información podría incluir datos sobre cambios de turno, operación de equipos, logística de suministros, horarios de patrullaje y otras vulnerabilidades. La recopilación pasiva de información puede ser difícil de detectar, especialmente cuando la información se recopila en pequeños incrementos de varias fuentes. Mantener la observación de personas inusualmente curiosas, fotógrafos y personal a menudo fuera de sus áreas de responsabilidad puede ayudar a las organizaciones a reconocer la recopilación pasiva de información, especialmente cuando se combina con información precisa de verificación de antecedentes.

Los Sniffing son un ejemplo de amenaza pasiva. Es el acto de monitorear datos en un flujo de comunicación. Las escuchas telefónicas, la interceptación de datos contenidos en un flujo de información, es el medio más ampliamente conocido de rastreo. Los Sniffing pueden ser muy sofisticados. Las herramientas están disponibles públicamente para rastrear datos en varias redes de comunicación. Aunque estos dispositivos se usan comúnmente para la gestión de la configuración, la resolución de problemas de redes y el análisis del tráfico de datos, también se pueden usar para recopilar datos específicos sobre cualquier transacción que ocurra en la red. Por ejemplo, en el rastreo de paquetes y el rastreo de contraseñas, el atacante se conecta secretamente a la red en un conmutador remoto o computadora. La herramienta de rastreo supervisa pasivamente la información enviada a través de la red y captura la información en un disco que luego puede descargarse y analizarse para obtener las identificaciones y contraseñas del usuario.

5.6.5.3 Amenazas activas

5.6.5.3.1 General

Las amenazas activas se presentan en varias formas, como se describe en las siguientes subcláusulas.

5.6.5.3.2 Comunicación

La intención de un ataque de comunicación es interrumpir las comunicaciones para un Sistema de Control y Automatización Industrial. Los ataques de comunicación pueden ocurrir en varias formas. Pueden ocurrir en varios niveles dentro del sistema desde la capa de procesador de la computadora hacia arriba y desde fuera de la empresa, como en un ataque de denegación de servicio en los sistemas de comunicaciones.

5.6.5.3.3 Inyección de base de datos

Una inyección es una forma de ataque en un sitio web basado en una base de datos en el que el atacante ejecuta comandos no autorizados aprovechando un código inseguro en un sistema conectado a Internet, sin pasar por el firewall. Los ataques de inyección se utilizan para robar información de una base de datos desde la cual los datos normalmente no estarían disponibles y / o para obtener acceso a las computadoras host de una organización a través de la computadora que aloja la base de datos.

5.6.5.3.4 Reproducción

Las señales pueden capturarse desde las rutas de comunicación del sistema de control y reproducirse más tarde para proporcionar acceso a sistemas seguros o para falsificar datos en el

Sistema de Control y Automatización Industrial. Los intrusos potenciales pueden reproducir señales de control de acceso, señales biométricas y otras señales del sistema para obtener acceso no autorizado a áreas o sistemas seguros, ocultar actividades ilegítimas o proporcionar distracciones falsas. Un sistema puede combinar múltiples rutas para la adquisición de datos, señalización y control para evitar que un solo toque recopile información de reproducción para un subsistema completo, equipo, aplicación o base de datos.

5.6.5.3.5 Suplantación de identidad

En redes, estos términos se usan para describir una variedad de formas en que se puede engañar al hardware y al software. Los atacantes pueden falsificar un encabezado de correo electrónico para que parezca que el mensaje proviene de algún lugar o de alguien que no sea la fuente real. La falsificación de IP, por ejemplo, implica un truco que hace que un mensaje aparezca como si viniera de una dirección IP autorizada.

5.6.5.3.6 Ingeniería social

Los agentes de amenazas también obtienen o intentan obtener datos seguros de otro modo, engañando a un individuo para que revele información segura. La ingeniería social es exitosa porque sus víctimas quieren confiar innatamente en otras personas y son naturalmente útiles. Las víctimas de la ingeniería social son engañadas para que divulguen información que no saben que se utilizará para atacar una red informática.

5.6.5.3.7 Engaño (Phishing)

Este es un tipo de ataque de seguridad que atrae a las víctimas a revelar información, presentando un correo electrónico falsificado para atraer al destinatario a un sitio web que parece estar asociado con una fuente legítima. El phishing se basa en la ingeniería social en que los humanos tienden a creer en la seguridad de un nombre de marca, asociándolo con la confiabilidad.

5.6.5.3.8 Código malicioso

El propósito de un código malicioso puede ser recopilar información sobre sistemas o usuarios, destruir datos del sistema, proporcionar un punto de apoyo para una mayor intrusión en el sistema, falsificar datos e informes del sistema o proporcionar irritación que lleva mucho tiempo al personal de operaciones y mantenimiento del sistema. Los ataques de código malicioso pueden tomar la forma de virus, gusanos, exploits automáticos, o caballos de Troya.

Un virus es un programa o fragmento de código dentro de otro programa que se carga en una computadora sin el conocimiento del usuario y que va en contra de sus deseos. Los virus también pueden replicarse a sí mismos. Todos los virus informáticos son artificiales. Un virus simple que puede hacer una copia de sí mismo una y otra vez es relativamente fácil de producir. Incluso un virus tan simple es peligroso, ya que utilizará rápidamente toda la memoria disponible y detendrá el sistema. Un tipo de virus aún más peligroso es uno capaz de transmitirse a través de redes y pasar por alto los sistemas de seguridad.

Se coloca un código exploit automático en el sistema para recopilar información o notificar a alguien u otros sistemas cuando ocurren eventos o transacciones específicas. Un código de exploit relativamente simple puede recopilar información para futuras intrusiones, explotación financiera

o fines estadísticos (marketing). Un código exploit automático puede utilizar otros recursos o aplicaciones que ya están dentro del sistema para mejorar sus capacidades para recopilar información o destruir datos. Un código de exploit totalmente automatizado generalmente se llama gusano. Un gusano es un programa o algoritmo autónomo que se replica a través de una red informática y generalmente realiza acciones maliciosas, como el uso de los recursos de la computadora y posiblemente apagar el sistema.

Un caballo de Troya es un programa destructivo que se hace pasar por una aplicación benigna. A diferencia de los virus, los caballos de Troya (también conocidos como "troyanos") no se replican, pero pueden ser igual de destructivos. Uno de los tipos más insidiosos de caballo de Troya es un programa que afirma deshacerse de virus en una computadora, pero en su lugar introduce virus en la computadora.

Se puede entregar un código malicioso en forma de botnet, definido como una colección de máquinas comprometidas que ejecutan programas bajo una infraestructura común de comando y control. El creador de un botnet puede controlar el grupo de forma remota, generalmente con fines nefastos.

5.6.5.3.9 Denegación de servicio

Los ataques de denegación (o degradación) de servicio afecta la disponibilidad de una red, sistema operativo o recursos de aplicaciones. Una forma popular de denegación de servicio basada en la red es el ataque de denegación de servicio distribuido (DDoS), que aprovecha múltiples dispositivos comprometidos para causar daños significativos a una red, dispositivo o aplicación.

5.6.5.3.10 Escalada de privilegios

Para montar un ataque efectivo contra un sistema, a menudo es necesario que los agentes de amenazas obtengan primero accesos privilegiados. Con estos mayores privilegios, el atacante puede realizar acciones que de otro modo se evitarían.

5.6.5.3.11 Destrucción física

Los ataques de destrucción física tienen como objetivo destruir o incapacitar componentes físicos (es decir, hardware, dispositivos de almacenamiento de software, conexiones, sensores y controladores) que forman parte del Sistema de Control y Automatización Industrial. Estos ataques pueden venir en forma de un ataque físico a los componentes mismos o mediante un ataque cibernético que hace que el sistema realice acciones que conducen a daños físicos, destrucción o incapacidad del componente.

5.6.6 Contramedidas

Las contramedidas son acciones tomadas, o disposiciones tomadas con el propósito de reducir el riesgo a un nivel aceptable, o para cumplir con las políticas de seguridad. Por lo general, no eliminan el riesgo. La naturaleza de las contramedidas empleadas depende de la naturaleza de la amenaza que se está abordando.

Existen varias posibles contramedidas para abordar las amenazas externas. Los ejemplos incluyen lo siguiente:

a) autenticación de usuarios y / o computadoras;
b) controles de acceso;
c) detección de intrusos;
d) cifrado;
e) firmas digitales;
f) aislamiento o segregación de recursos;
g) escanear en busca de software malicioso;
h) monitoreo de la actividad del sistema;
i) seguridad física.

En el caso de amenazas internas, puede ser necesario un enfoque diferente, ya que el atacante puede tener la capacidad de eludir algunas de las contramedidas normales, como el control de acceso. Esto hace que sea necesario hacer más hincapié en las contramedidas, como las políticas escritas, la separación de funciones, la supervisión de la actividad, la auditoría del sistema y el cifrado.

Las amenazas pasivas como los rastreadores (sniffing) son muy difíciles de detectar, porque la herramienta de rastreo solo lee la información que se mueve a través de los medios conectados y no proporciona señales en la ruta de señalización. El rastreador conectado de forma rígida se puede detectar con dispositivos de control de comunicación modernos, como los conmutadores de red de datos inteligentes, pero el rastreador inalámbrico es casi imposible de detectar incluso con equipos de radiocomunicación muy sofisticados y costosos. El acceso de rastreadores se puede reducir controlando y cerrando los puertos de voz y datos no utilizados en la planta y proporcionando inteligencia en el equipo de control de comunicación.

5.7 Madurez del programa de seguridad

5.7.1 Descripción general

Impulsadas por el aumento de los riesgos de ciberseguridad, muchas organizaciones han adoptado un enfoque proactivo para abordar los riesgos de seguridad de sus sistemas y redes de tecnología de la información. Están comenzando a darse cuenta de que abordar la ciberseguridad es una actividad o proceso continuo y no un proyecto con inicio y parada identificadas.

Históricamente, las organizaciones que proporcionan y respaldan sistemas de información empresarial y Sistemas de Control y Automatización Industrial operan en dos áreas mutuamente excluyentes. Las experiencias y los requisitos de cada organización no fueron comprendidos ni apreciados por la otra. Surgieron problemas cuando las organizaciones intentaron emplear prácticas comunes de seguridad de TI para los Sistemas de Control y Automatización Industrial.

En algunos casos, las prácticas de seguridad estaban en oposición a las prácticas de producción normales diseñadas para maximizar la seguridad y la continuidad de la producción. Debido a que las tecnologías de información abierta de hoy en día se utilizan ampliamente en los Sistemas de Control y Automatización Industrial, se requiere conocimiento adicional para emplear estas tecnologías de manera segura. Las organizaciones de TI y fabricación o producción deben trabajar juntas y unir sus conocimientos y habilidades para abordar los problemas de seguridad. En industrias con un alto

potencial de incidentes ambientales, de salud y seguridad, es importante involucrar también a la Gestión de Seguridad de Procesos (PSM) y al personal de seguridad física.

El objetivo es un programa de seguridad maduro que integre todos los aspectos de la ciberseguridad, incorporando sistemas informáticos de escritorio y empresariales con Sistemas de Control y Automatización Industrial. La Figura 4 muestra el viaje de integración que enfrentan muchas empresas. Muchas organizaciones tienen programas de ciberseguridad bastante detallados y completos para sus sistemas informáticos empresariales, pero las prácticas de gestión de ciberseguridad no están tan desarrolladas para IACS.

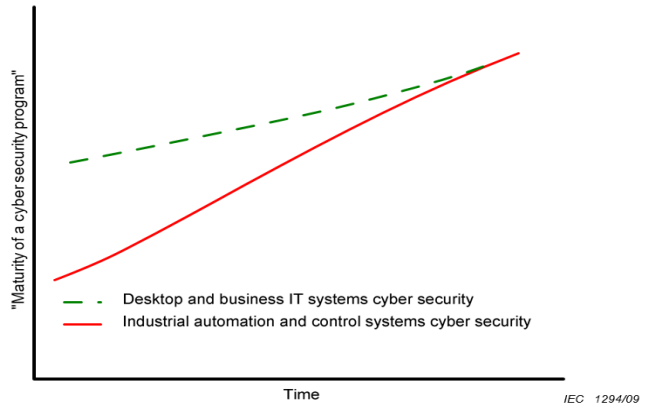

Figura 4: Integración de la ciberseguridad empresarial y IACS

Un error común es abordar la ciberseguridad como un proyecto con una fecha de inicio y finalización. Cuando esto ocurre, el nivel de seguridad a menudo disminuye con el tiempo, como se muestra en la Figura 5. Los riesgos de ciberseguridad cambian constantemente a medida que surgen nuevas amenazas y vulnerabilidades junto con implementaciones tecnológicas en constante cambio. Se necesita un enfoque diferente para mantener las ganancias de seguridad y mantener el riesgo a un nivel aceptable.

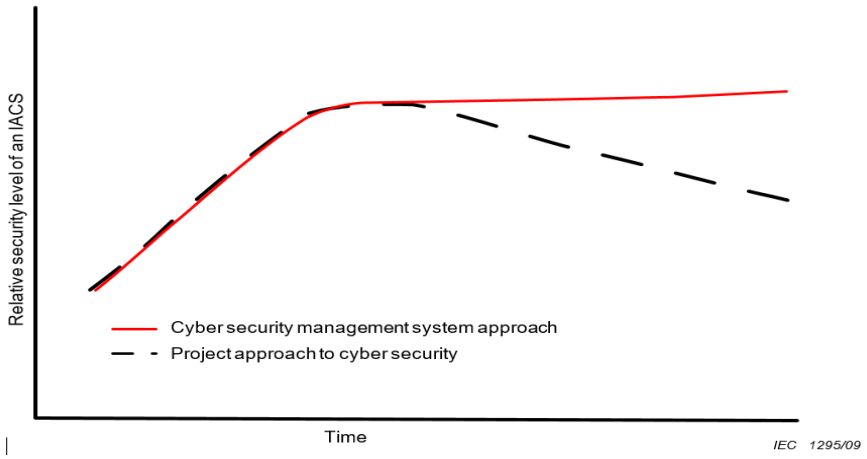

Figura 5 - Nivel de ciberseguridad a lo largo del tiempo

La recomendación es desarrollar e implementar un sistema de gestión de seguridad cibernética (CSMS) para toda la organización que incluya elementos del programa para reevaluar el riesgo y tomar medidas correctivas para eliminar la tendencia a que los niveles de seguridad disminuyan con el tiempo. En el segundo documento de esta serie se proporciona una descripción detallada de los elementos clave de un sistema de gestión de ciberseguridad. [8]

La vía de cada organización para implementar un sistema de gestión de ciberseguridad será diferente según los objetivos de la organización y la tolerancia al riesgo. La integración de la ciberseguridad en las prácticas documentales de una organización es un cambio cultural que requiere tiempo y recursos. Como sugieren las figuras, no se puede lograr en un solo paso. Es un proceso evolutivo que estandariza el enfoque de la ciberseguridad. Las prácticas de seguridad que se implementarán deben ser proporcionales al nivel de riesgo y variarán de una organización a otra, e incluso pueden ser diferentes para varias operaciones dentro de la misma organización en función de las necesidades y requisitos globales. Las políticas y procedimientos individuales también pueden ser diferentes para cada clase de sistema dentro de una organización porque el nivel de riesgo y los requisitos de seguridad pueden ser diferentes. Un sistema de gestión de ciberseguridad establece el programa general que acomoda estas diferencias.

La educación y la conciencia son fundamentales para abordar con éxito los riesgos de ciberseguridad de IACS como se señaló anteriormente. Hay varias opciones a considerar:

a) Capacitar al personal de IACS para comprender los problemas actuales de tecnología de la información y ciberseguridad.
b) Capacitar al personal de TI para comprender las tecnologías IACS, junto con los procesos y métodos de gestión de seguridad de procesos.
c) Desarrollar prácticas que se unan al conjunto de habilidades de todas las organizaciones para lidiar con la ciberseguridad en colaboración.

Para que el programa de ciberseguridad tenga éxito, es necesario reunir la combinación correcta de personas tanto en los proyectos de mitigación como en el desarrollo general del programa CSMS. La Figura 6 ilustra una gama típica de habilidades y comprensión que se deben reunir de múltiples grupos de personas para alcanzar el estado deseado de programa de seguridad cibernética integrado y maduro.

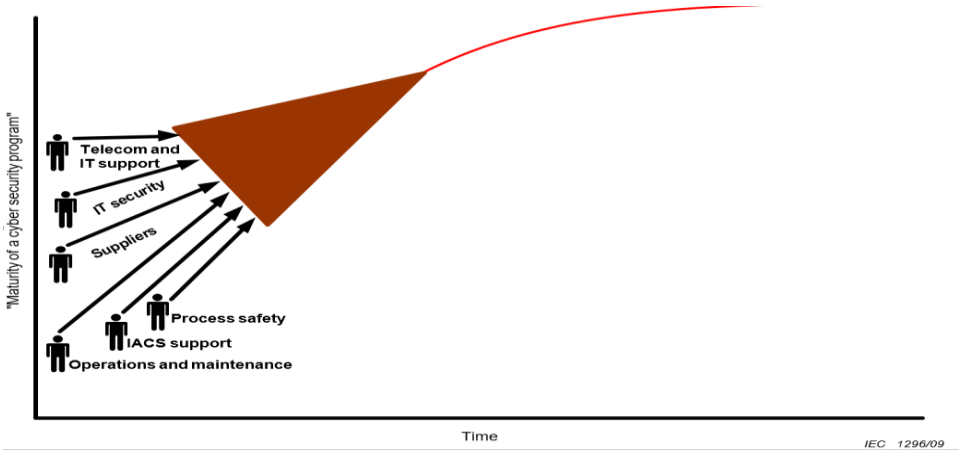

Figura 6 - Integración de recursos para desarrollar el CSMS

5.7.2 Fases de madurez

Es posible describir la madurez relativa de un programa de ciberseguridad en términos de un ciclo de vida que consta de varias fases. Cada una de estas fases consta de uno o más pasos.

Algunas partes del Sistema de Control y Automatización Industrial, o zonas de control dentro de un sistema de control pueden estar en diferentes fases de madurez. Hay varias razones para esta situación, incluyendo restricciones presupuestarias, evaluaciones de vulnerabilidad y amenaza, cronogramas contra resultados de análisis de riesgos, actualizaciones de automatización, planes de disolución o reemplazo, planes para vender un segmento de la instalación o negocio, o la disponibilidad de otros recursos para actualizar los sistemas de seguridad a una fase más madura.

Las organizaciones pueden lograr una evaluación más detallada de la madurez de la seguridad mediante la evaluación de los logros dentro de partes del sistema de automatización y control industrial en términos de las fases y pasos que se muestran en la Tabla 2.

Tabla 2 - Fases de madurez de seguridad

Fase	Paso
Concepto	Identificación de concepto
Análisis funcional	Definición
Implementación	Diseño funcional Diseño detallado Construcción
Operaciones	Operaciones Monitoreo de cumplimiento
Reciclaje y Disposición	Eliminación Disoluciones

De la Tabla 3 a la Tabla 7, se proporcionan descripciones generales para cada una de las fases y pasos en la madurez de un ciclo de vida.

Tabla 3 - Fase conceptual

Paso	Descripción
Identificación	Reconocer la necesidad de protección de bienes, activos, servicios o personal Comienza a desarrollar el programa de seguridad
Concepto	Continuar desarrollando el programa de seguridad Documentar los activos, servicios y personal que necesitan algún nivel de protección Documentar posibles amenazas internas y externas para la empresa. Establecer misión de seguridad, visiones y valores. Desarrollar políticas de seguridad para sistemas y equipos de automatización y control industrial, sistemas de información y personal.

Tabla 4 - Fase de análisis funcional

Paso	Descripción
Definición	Continuar desarrollando el programa de seguridad Establecer requisitos funcionales de seguridad para sistemas y equipos de automatización y control industrial, sistemas de producción, sistemas de información y personal. Realizar una evaluación de vulnerabilidad de las instalaciones y servicios asociados en relación con la lista de posibles amenazas. Descubrir y determinar los requisitos legales para los Sistemas de Control y Automatización Industrial.

	Realizar un análisis de riesgos de posibles vulnerabilidades y amenazas. Clasificar los riesgos, los posibles impactos para la empresa y las posibles mitigaciones. Segmentar el trabajo de seguridad en tareas y módulos controlables para el desarrollo de diseños funcionales Establecer definiciones funcionales de red para porciones de seguridad de Sistemas de Control y Automatización Industrial.

Tabla 5 - Fase de implementación

Paso	Descripción
Diseño funcional	El desarrollo del programa de seguridad se completa en esta fase. Defina requisitos de seguridad funcionales para zonas empresariales, zonas de plantas y zonas de control. Las actividades y eventos potenciales se definen y documentan para cumplir con los requisitos funcionales e implementar planes para una empresa segura Definir la organización y estructura de seguridad funcional. Definir las funciones requeridas en el plan de implementación. Defina y publique zonas de seguridad, fronteras y portales de control de acceso. Complete y emita políticas y procedimientos de seguridad
Diseño detallado	Diseñar sistemas físicos y lógicos para realizar los requisitos funcionales previamente definidos para seguridad Realizar programas de capacitación Implementar el plan desarrollado completamente Iniciar programas de gestión de activos y gestión de cambios. Diseñar bordes y portales de control de acceso para zonas protegidas.
Construcción	Se ejecuta el plan de implementación. Se instalan equipos de seguridad física, aplicaciones lógicas, configuraciones, procedimientos de personal para completar las zonas y fronteras seguras dentro de la empresa. Los atributos del portal de control de acceso se activan y mantienen Programas de entrenamiento completados Los programas de gestión de activos y gestión de cambios son funcionales y operativos. Los paquetes de rotación del sistema de seguridad están completos y listos para su aceptación por el personal de operaciones y mantenimiento

Tabla 6 - Fase de operaciones

Paso	Descripción
Operaciones	Los equipos, servicios, aplicaciones y configuraciones de seguridad se completan y aceptan mediante operaciones y mantenimiento Se capacita al personal y se brinda capacitación continua sobre asuntos de seguridad El mantenimiento monitorea porciones de seguridad de la empresa, planta o zonas de control y las mantiene funcionando correctamente La gestión de activos y la gestión de cambios es operativa y mantenida
Cumplimiento de Monitoreo	Auditorías internas Revisiones de riesgo Auditorías externas

Tabla 7 - Reciclaje y fase de eliminación

Paso	Descripción
Disposición	Los sistemas de seguridad obsoletos se desmontan y desechan adecuadamente. Las fronteras de seguridad se actualizan o recrean para proteger la zona Los portales de control de acceso se crean, redefinen, reconfiguran o cierran Se informa al personal sobre los cambios en los sistemas y elementos de seguridad junto con el impacto en los sistemas de seguridad asociados.
Disolución	La propiedad intelectual se recopila, documenta y archiva o destruye de forma segura. Los portales de control de acceso y los enlaces respectivos están cerrados. Se informa al personal sobre la disolución de los sistemas y elementos de seguridad junto con el impacto en los sistemas de seguridad restantes

5.8 Políticas

5.8.1 Descripción general

Las políticas de seguridad permiten a una organización seguir un programa consistente para mantener un nivel aceptable de seguridad. Las políticas se definen en diferentes niveles en una organización, desde políticas de gobierno o gestión establecidas a nivel empresarial hasta políticas de operación que definen los detalles de la administración de seguridad. Las políticas al nivel más específico son el documento de la organización contra el cual las auditorías de seguridad pueden medir el cumplimiento.

Las políticas de seguridad son las reglas que especifican o regulan cómo una organización protege los recursos sensibles y críticos del sistema. Las políticas establecen inequívocamente lo que es obligatorio. Debido a que las políticas son obligatorias y sin ambigüedades, hacen posibles las auditorías. Las políticas de seguridad de la organización también tienen en cuenta las obligaciones legales, reglamentarias y contractuales. Son la varilla de medición contra el cual las auditorías prueban las prácticas reales de la organización.

Las políticas complementarias son procedimientos. Los procedimientos de seguridad definen en detalle la secuencia de pasos necesarios para proporcionar una determinada medida de seguridad. Debido a su nivel de detalle, los procedimientos se aplican a un tema específico. Pueden pertenecer a una tecnología específica. Las políticas hacen referencia a los procedimientos y exigen su uso.

Contrastando con las políticas y los procedimientos hay pautas. Las pautas no son obligatorias. Su objetivo es describir una forma de hacer algo que sea deseable pero no obligatorio. Debido a que las pautas no son obligatorias y pueden ser ambiguas, las prácticas no pueden ser auditadas según las pautas. Las pautas a veces son escritas por un grupo que no tiene la autoridad para exigir que se sigan. Las pautas son inapropiadas para describir prácticas que son obligatorias.

Debido a que las políticas y procedimientos para diferentes partes de una organización son a menudo diferentes, es importante que estén adecuadamente coordinados. Específicamente, la política de seguridad para los Sistemas de Control y Automatización Industrial debe coordinarse con políticas similares para la seguridad informática de uso general. El programa de seguridad funcionará más exitosamente si hay buenas relaciones de trabajo entre las partes, y un conjunto de políticas bien coordinadas puede apoyar las buenas relaciones.

Una cierta coherencia con la estructura de las diversas políticas y procedimientos aumenta la coherencia del conjunto general de políticas y procedimientos. Cada documento de política o procedimiento tiene una declaración breve pero precisa de su propósito. También tiene una declaración de alcance que define dónde se aplica el documento. Tiene una descripción de los riesgos que se pretende reducir y de los principios clave del documento. Estos elementos comunes guían al lector al proporcionar más información sobre la intención de la política o procedimiento. También describen la intención del documento de proporcionar orientación, lo cual es útil cuando el documento necesita ser revisado.

Las diferentes fases en el ciclo de vida de un sistema tienen diferentes perfiles de problemas de seguridad. Las políticas y procedimientos de seguridad pueden abordar solo ciertas fases del ciclo de vida. Algunas políticas y procedimientos pueden especificar que solo pertenecen a ciertas fases. Todas las preocupaciones de seguridad de todas las diversas fases se abordan en los lugares correspondientes en el conjunto de políticas y procedimientos de seguridad.

Las políticas y procedimientos de seguridad contienen instrucciones sobre cómo la organización medirá el cumplimiento y actualizará las políticas. Las organizaciones a menudo reconocen que las políticas deben actualizarse al realizar o evaluar auditorías. Las auditorías pueden identificar ambigüedades en políticas y procedimientos, así como partes de políticas y procedimientos que no aclaran el proceso o resultado requerido. Las auditorías pueden identificar problemas que deben agregarse a las políticas y procedimientos. Las auditorías también pueden identificar requisitos que deben ser reevaluados y ajustados o posiblemente retractados.

Las políticas y los procedimientos deben permitir circunstancias imprevistas que hagan inviable seguirlas. Las políticas también deben indicar cómo documentar y aprobar las excepciones a las políticas y procedimientos. Documentar las excepciones aprobadas conduce a un estado de seguridad más claro que dejar imprecisión y ambigüedad en las políticas y procedimientos.

Además, las organizaciones deben ser inequívocas sobre lo que es un requisito frente a lo que es asesoramiento opcional en una política. El uso preciso de verbos como deberá, debería, puede y es, elimina la ambigüedad. Las declaraciones de política pueden definir estas palabras en sus secciones de introducción para ser más precisos. "Deberá" se utiliza para requisitos; "debería" se utiliza para recomendaciones. "Puede" se usa para consejos opcionales. Puede ser apropiado proporcionar opciones para abordar un requisito. Frases como "cuando sea posible" o "a menos que sea necesario" introducen ambigüedad a menos que la declaración también describa cómo determinar si el caso es posible o necesario.

Las políticas y los procedimientos identifican quién es responsable de qué. ¿Es el personal de control de procesos responsable de la red de control? ¿Es responsable de una zona desmilitarizada (DMZ) entre la red de control y la red empresarial? Si un departamento de sistemas de información corporativo es responsable de las condiciones que requieren que el personal de control de procesos realice ciertas operaciones, entonces estas operaciones deben describirse.

Para una organización que recién comienza a crear su programa de seguridad, las políticas y los procedimientos son un buen lugar para comenzar. Inicialmente, se pueden escribir para cubrir el conjunto de prácticas de seguridad que la organización está preparada para manejar en el corto plazo. Con el tiempo, pueden revisarse y ajustarse a medida que crece la capacidad de la

organización. Se pueden implementar sin el tiempo de entrega e instalación de sistemas y dispositivos.

5.8.2 Política de nivel empresarial

La política a nivel empresarial exige el programa de seguridad y establece la dirección. Establece los objetivos generales de seguridad de la organización.

La declaración de política de la alta dirección debe ser lo suficientemente circunspecta como para seguir siendo pertinente y precisa a través de cambios en la estructura de la organización, cambios en el sistema y la tecnología de seguridad, y cambios en los tipos de amenazas de seguridad. Al ser circunspecto, la política puede ser estable y deberá reescribirse solo cuando cambie la posición básica de la organización sobre la seguridad. Sin embargo, la declaración de política también es inequívoca; identifica claramente lo que se requiere.

La política a nivel de empresa identifica áreas de responsabilidad y asigna responsabilidad para esas áreas. La política puede definir la relación entre el departamento de TI y las operaciones de la planta e identificar sus diferentes responsabilidades. La política puede diferenciar los objetivos de seguridad del sistema de control de los de la red empresarial. Por ejemplo, mantener la confidencialidad puede ser una de las principales consideraciones de seguridad para la red empresarial, mientras que mantener el funcionamiento continuo puede ser una de las principales consideraciones para el sistema de control. Además, la política identifica estándares y regulaciones particulares que se aplican a la organización. Puede identificar la capacitación como un componente importante del programa de seguridad. La política también puede indicar las consecuencias por infracciones de la política.

La gerencia debe comunicar la política en toda la organización para que todos los empleados la entiendan.

5.8.3 Políticas y procedimientos operacionales

Las políticas y procedimientos operativos se desarrollan en los niveles inferiores de la organización para especificar cómo se implementa la política a nivel de la empresa en un conjunto específico de circunstancias. Los procedimientos de seguridad ponen en vigencia la política. Definen lo que hará la organización para lograr los objetivos y cumplir con los requisitos de la política. Los procedimientos establecen procesos que abordarán todas las inquietudes de la política.

Los procedimientos abordan todos los componentes necesarios en un programa de seguridad, incluidos los siguientes:

a) diseño del sistema;
b) adquisiciones;
a) instalación;
b) operación del proceso;
c) mantenimiento del sistema;
d) personal;
e) auditoría;
f) entrenamiento.

Los procedimientos identifican actividades específicas, quién es responsable de su desempeño y cuándo se realizarán las actividades.

Los procedimientos escritos describen el proceso mediante el cual se cambiarán cuando la situación cambie. Cada política o procedimiento tiene un propietario identificado responsable de reconocer cuándo se necesitan actualizaciones y de asegurarse de que se realicen.

La efectividad de las políticas y procedimientos debe medirse para verificar si cumplen con el propósito previsto. El costo para la organización también debe medirse, de modo que la organización pueda determinar si el equilibrio de la reducción del riesgo se alinea con el costo para implementar las políticas. Si el saldo es inaceptable, la política y los procedimientos pueden tener que ajustarse. Los procedimientos también deben actualizarse para reflejar los cambios en la tecnología.

Los procedimientos pueden respaldar auditorías. Una auditoría de seguridad compara las acciones observadas de la organización con los procedimientos escritos.

5.8.4 Temas cubiertos por políticas y procedimientos

5.8.4.1 General

Hay varios temas que las políticas y los procedimientos pueden cubrir. Cada organización es diferente y debe determinar las políticas y procedimientos apropiados que sean aplicables para sus sistemas de automatización y control industrial. Los posibles temas incluyen:

5.8.4.2 Gestión de riesgos

La gestión de riesgos es vital para desarrollar un programa de seguridad rentable que proporcione una capa uniforme de seguridad adecuada, pero que no requiera equipos o procedimientos que sean demasiado costosos y significativamente más allá del rango de seguridad adecuada. Sin embargo, la gestión de riesgos es compleja y debe adaptarse a la organización. La política de gestión de riesgos define cómo se determina un nivel de riesgo aceptable y cómo controlar el riesgo. Este nivel varía según los objetivos y las circunstancias de una organización en particular. El proceso para determinar el nivel de riesgo debe repetirse periódicamente para acomodar los cambios en el medio ambiente.

5.8.4.3 Gestión de acceso

La seguridad se mejora en un sistema al restringir el acceso solo a aquellos usuarios que necesitan y se les confía el acceso. Una política de administración de acceso identifica diferentes roles de usuarios y qué tipo de acceso necesita cada rol para cada clase de activo (físico o lógico). Especifica las responsabilidades de los empleados para proteger los activos y las responsabilidades de los administradores para mantener los procedimientos de gestión de acceso. La autorización para estos privilegios de acceso debe tener una aprobación bien documentada por parte de la administración y debe revisarse periódicamente. La gestión de acceso puede ser tan importante o incluso más importante para la integridad y disponibilidad del sistema como la necesidad de proteger la confidencialidad de los datos.

5.8.4.4 Disponibilidad y planificación de continuidad

Las políticas en esta área proporcionan el marco necesario y las expectativas de requisitos para el respaldo y la recuperación, así como la continuidad del negocio y la planificación de la recuperación ante desastres. También definen características de archivo (por ejemplo, cuánto tiempo se deben conservar los datos).

5.8.4.5 Seguridad física

La seguridad del sistema de control depende de la seguridad física del espacio que contiene el sistema de control. Es posible que el sitio de la planta ya tenga una política de seguridad física antes de que la política de seguridad se escriba para el sistema de control. Sin embargo, las políticas relacionadas con el acceso físico de los sistemas pueden diferir de las que involucran activos que no son sistemas. Por ejemplo, todo el personal de la refinería de petróleo puede tener acceso general a casi todas las instalaciones dentro de las cercas de la planta, pero las salas de infraestructura de TI pueden necesitar tener acceso limitado solo al personal relacionado con TI, aunque solo sea para evitar daños accidentales. La política de seguridad del sistema de control debe incluir una referencia a la política de seguridad física y establecer su dependencia.

La política de seguridad para el sistema de control debe contener suficientes detalles sobre seguridad física para realizar cualquier aplicación específica de la política de seguridad física del sitio al sistema de control. Por ejemplo, una política de este tipo podría decir: "algunos equipos deben estar en gabinetes cerrados y las llaves deben mantenerse en un lugar restringido".

5.8.4.6 Arquitectura

Las políticas y los procedimientos describen configuraciones seguras de los sistemas de control que incluyen cuestiones como las siguientes:

a) diseños de red recomendadas;
b) configuración de firewall recomendada;
c) autorización y autenticación del usuario;
d) interconectar diferentes redes de control de procesos;
e) uso de comunicaciones inalámbricas;
f) dominios y relaciones de confianza;
g) gestión de parches (incluida la autenticación);
h) gestión antivirus;
i) endurecimiento del sistema en términos de cerrar puertos de software, deshabilitar o vitar servicios no utilizados o peligrosos, y deshabilitar el uso de dispositivos de almacenamiento extraíbles;
j) acceso a redes externas (es decir, Internet);
k) uso apropiado del correo electrónico.

5.8.4.7 Dispositivos portátiles

Los dispositivos portátiles poseen todos los riesgos de seguridad de los equipos estacionarios, pero su movilidad hace que sea menos probable que estén cubiertos por los procedimientos normales de seguridad desde la instalación hasta la auditoría. Su portabilidad brinda oportunidades

adicionales para la corrupción mientras está fuera de las zonas de seguridad física o para la intercepción de información mientras se conecta a zonas seguras. Por lo tanto, a menudo se necesita una política especial para cubrir los dispositivos portátiles. La política debe requerir la misma protección de seguridad que un dispositivo estacionario, pero los mecanismos técnicos y administrativos que brindan esta protección pueden ser diferentes.

5.8.4.8 Dispositivos inalámbricos y sensores

El equipo de control que utiliza transmisión de radiofrecuencia en lugar de cables se ha utilizado ampliamente en ciertas aplicaciones de sistemas de control durante muchos años. A medida que los costos disminuyen y surgen nuevos estándares, las aplicaciones potenciales en los sistemas de automatización y control continúan expandiéndose, en parte debido a los menores costos de instalación. Una diferencia clave entre los dispositivos con cable e inalámbricos es que, en este último caso, las señales no están confinadas dentro de un límite de seguridad física, lo que las hace más propensas a la intercepción y la corrupción. Por lo tanto, una política de seguridad específica para dispositivos inalámbricos es apropiada para organizaciones que actualmente usan o pueden implementar dispositivos inalámbricos o sensores en sus operaciones en el futuro. La política puede especificar qué aplicaciones pueden usar dispositivos inalámbricos, qué protección y métodos administrativos son necesarios y cómo se interconectan las redes cableadas e inalámbricas.

5.8.4.9 Acceso remoto

El acceso remoto omite los controles de seguridad física locales de los límites del sistema. Extiende el acceso a la zona de confianza a una ubicación geográfica completamente diferente e incluye una computadora que puede no haberse sometido a las verificaciones de seguridad de las computadoras que se encuentran físicamente en el área de la zona de confianza. Se requieren diferentes mecanismos para proporcionar el mismo nivel de seguridad que la zona de confianza.

5.8.4.10 Personal

Es probable que los problemas de personal se definan en las políticas de seguridad de personal y TI de la empresa. La política de seguridad del sistema de control proporciona detalles específicos, mientras que las políticas más generales no incluyen aspectos del sistema de control. Por ejemplo, las políticas de seguridad del sistema de control coordinan los roles de acceso al sistema de control con las prácticas de detección y monitoreo del personal.

5.8.4.11 Política de subcontratista

Los problemas de seguridad incluyen el trabajo que puede involucrar a subcontratistas en funciones como proveedor, integrador, proveedor de servicios de mantenimiento o consultor. Una política de seguridad que cubre a los subcontratistas aborda las interacciones con el subcontratista que podrían abrir vulnerabilidades. La política identifica las responsabilidades de las diferentes partes. Aborda las responsabilidades cambiantes a medida que los proyectos avanzan a través de sus fases y a medida que se entregan los materiales y sistemas. La política puede requerir que ciertos términos se escriban en contratos con subcontratistas.

Sin una gestión adecuada de los programadores por contrato, la integridad de la aplicación puede verse comprometida o el código de programación puede no ser mantenible. Es importante encontrar programadores de contratos bien calificados que sigan los estándares de programación y

documentación de la organización y realicen las pruebas adecuadas, además de ser confiables y oportunos.

5.8.4.12 Auditoría

La seguridad del sistema se audita periódicamente para medir el grado de cumplimiento de las políticas y prácticas de seguridad. La política de seguridad aborda la necesidad de auditorías y especifica la responsabilidad, la regularidad y el requisito de acción correctiva. Un proceso de auditoría integral puede abordar aspectos distintos de la seguridad, como la eficiencia y eficacia del proceso y el cumplimiento normativo.

5.8.4.13 Actualización de la política de seguridad

La política de seguridad se supervisa para determinar los cambios necesarios en las políticas mismas. El monitoreo de la política de seguridad es parte de cada documento de política y procedimiento, y la política de seguridad de la empresa establece el enfoque general. Cada documento de política y procedimiento operativo contiene una declaración de cuándo y quién debe revisar y actualizar la política o procedimiento en sí.

Deben existir programas de capacitación para nuevas contrataciones, operaciones, mantenimiento, actualizaciones y planificación de la sucesión. Los programas de capacitación deben estar bien documentados, estructurados y actualizados a intervalos regulares para incorporar cambios en el entorno operativo.

5.9 Zonas de seguridad

5.9.1 General

Cada situación tiene un nivel de seguridad aceptable diferente. Para sistemas grandes o complejos, puede no ser práctico o necesario aplicar el mismo nivel de seguridad a todos los componentes. Las diferencias pueden abordarse utilizando el concepto de zona de seguridad o área bajo protección. Una zona de seguridad es una agrupación lógica de activos físicos, informativos y de aplicaciones que comparten requisitos de seguridad comunes. Este concepto se aplica al entorno electrónico donde algunos sistemas están incluidos en la zona de seguridad y todos los demás están fuera de la zona. También puede haber zonas dentro de zonas, o subzonas, que brindan seguridad en capas, brindando defensa en profundidad y abordando múltiples niveles de requisitos de seguridad. La defensa en profundidad también se puede lograr asignando diferentes propiedades a las zonas de seguridad.

Una zona de seguridad tiene un borde, que es el límite entre los elementos incluidos y excluidos. El concepto de zona también implica la necesidad de acceder a los activos en una zona desde dentro y desde fuera. Esto define la comunicación y el acceso necesarios para permitir que la información y las personas se muevan dentro y entre las zonas de seguridad. Las zonas pueden considerarse confiables o no confiables.

Las zonas de seguridad se pueden definir en un sentido físico (una zona física) o de manera lógica (zona virtual). Las zonas físicas se definen agrupando los activos por ubicación física. En este tipo de zona es fácil determinar qué activos están dentro de cada zona. Las zonas virtuales se definen

agrupando activos, o partes de activos físicos, en zonas de seguridad basadas en la funcionalidad u otras características, en lugar de la ubicación real de los activos.

5.9.2 Determinación de requisitos

5.9.2.1 Descripción general

Al definir una zona de seguridad, una organización primero debe evaluar los requisitos de seguridad (objetivos de seguridad) y luego determinar si un activo en particular debe considerarse dentro o fuera de la zona. Los requisitos de seguridad se pueden dividir en los siguientes tipos:

5.9.2.2 Acceso a las comunicaciones

Para que un grupo de activos dentro de una frontera de seguridad proporcione valor, deben estar vinculados a activos fuera de la zona de seguridad. Este acceso puede ser de muchas formas, incluido el movimiento físico de activos (productos) y personas (empleados y proveedores) o comunicación electrónica con entidades fuera de la zona de seguridad.

La comunicación remota es la transferencia de información hacia y desde entidades que no están próximas entre sí. Para los fines de esta especificación técnica, el acceso remoto se define como la comunicación con activos que están fuera del perímetro de la zona de seguridad que se está abordando.

El acceso local generalmente se considera como comunicación entre activos dentro de una sola zona de seguridad.

5.9.2.3 Acceso físico y proximidad

Las zonas de seguridad física se usan para limitar el acceso a un área en particular porque todos los sistemas en esa área requieren el mismo nivel de confianza de sus operadores humanos, mantenedores y desarrolladores. Esto no impide tener una zona de seguridad física de nivel superior incrustada dentro de una zona de seguridad física de nivel inferior o una zona de acceso de comunicación de nivel superior dentro de una zona de seguridad física de nivel inferior. Para zonas físicas, las cerraduras en las puertas u otros medios físicos protegen contra el acceso no autorizado. El límite es la pared o gabinete que restringe el acceso. Las zonas físicas deben tener límites físicos acordes con el nivel de seguridad deseado y alineados con otros planes de seguridad de activos.

Un ejemplo de una zona de seguridad física es una planta de fabricación típica. Las personas autorizadas pueden ingresar a la planta por un agente autorizador (guardia de seguridad o identificación), y las personas no autorizadas tienen acceso restringido por el mismo agente autorizador y por cercas.

Los activos que se encuentran dentro de la frontera de seguridad son aquellos que deben protegerse a un determinado nivel de seguridad o política. Todos los dispositivos que se encuentran dentro de la frontera deben compartir el mismo nivel mínimo de requisitos de seguridad. En otros términos, deben protegerse para cumplir con la misma política de seguridad. Los mecanismos de protección pueden diferir según el activo que se protege.

Los activos que están fuera de la zona de seguridad están, por definición, en un nivel de seguridad menor o diferente. No están protegidos con el mismo nivel de seguridad y, por definición, no se puede confiar en el mismo nivel o política de seguridad.

5.10 Conductos

5.10.1 General

La información debe fluir dentro, fuera y dentro de una zona de seguridad. Incluso en un sistema no conectado en red, existe cierta comunicación (por ejemplo, conexión intermitente de dispositivos de programación para crear y mantener los sistemas). Para cubrir los aspectos de seguridad de la comunicación y proporcionar una construcción que abarque los requisitos únicos de las comunicaciones, este documento define un tipo especial de zona de seguridad: un conducto de comunicaciones.

Un conducto es un tipo particular de zona de seguridad que agrupa las comunicaciones que pueden organizarse lógicamente en una agrupación de flujos de información dentro y también fuera de una zona. Puede ser un único servicio (es decir, una única red Ethernet) o puede estar compuesto por múltiples portadores de datos (múltiples cables de red y accesos físicos directos). Al igual que con las zonas, puede estar hecho de construcciones físicas y lógicas. Los conductos pueden conectar entidades dentro de una zona o pueden conectar diferentes zonas.

Al igual que con las zonas, los conductos pueden ser confiables o no confiables. Los procesos de comunicación dentro de la zona suelen confiar en los conductos que no cruzan los límites de la zona. Los conductos de confianza que cruzan los límites de la zona deben utilizar un proceso seguro de extremo a extremo.

Los conductos no confiables son aquellos que no tienen el mismo nivel de seguridad que el punto final de la zona. En este caso, la seguridad de la comunicación real se convierte en responsabilidad del canal individual. Esto se ilustra en la Figura 7.

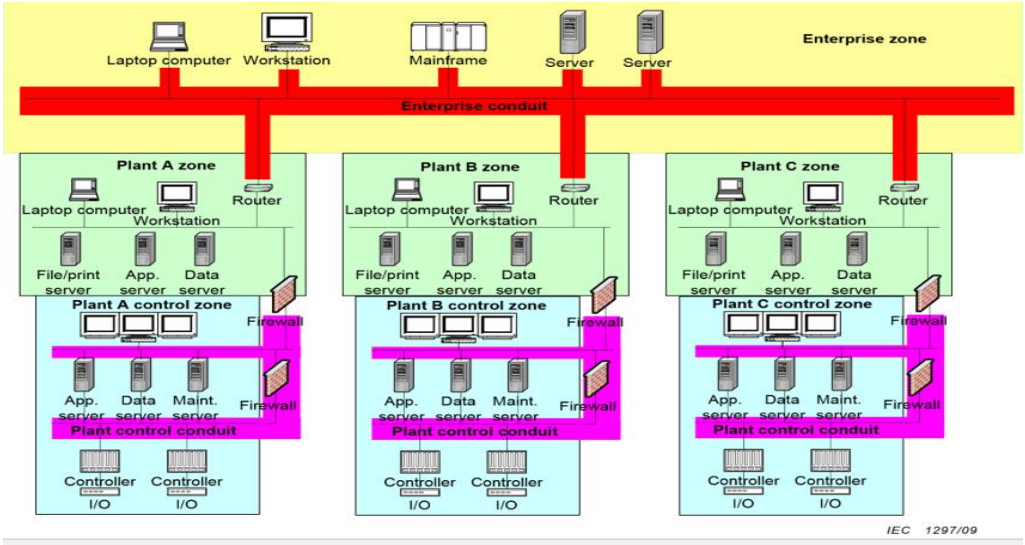

Figura 7 - Ejemplo de conducto

La Figura 7 representa una organización de tres plantas con sedes corporativas separadas. Las tres plantas están conectadas a la red empresarial para permitir las comunicaciones con la sede y las otras plantas. En el dibujo se definen cuatro posibles conductos (otros también se definirían, pero se omiten por brevedad). El primero es el conducto empresarial, que se muestra en la parte superior de la figura. Conecta varias plantas en diferentes ubicaciones al centro de datos corporativo. Si la red de área amplia (WAN) se construye utilizando comunicaciones arrendadas o privadas, entonces podría considerarse un conducto confiable. Si utiliza redes públicas y privadas, puede clasificarse como no confiable. En el conducto se incluyen todos los equipos de comunicaciones y firewalls que conforman los enlaces de la planta.

Las instancias de la segunda clase de conducto se muestran en cada planta. Aquí cada una de las plantas tiene su propio conducto de confianza para permitir la comunicación de control.

5.10.2 Canales

Los canales son los enlaces de comunicación específicos establecidos dentro de un conducto de comunicación. Los canales heredan las propiedades de seguridad del conducto utilizado como medio de comunicación (es decir, un canal dentro de un conducto seguro mantendrá el nivel de seguridad del conducto seguro). Los canales pueden ser confiables o no confiables. Los canales de confianza son enlaces de comunicación que permiten una comunicación segura con otras zonas de seguridad. Se puede usar un canal confiable para extender una zona de seguridad virtual para incluir entidades fuera de la zona de seguridad física.

Los canales no confiables son vías de comunicación que no tienen el mismo nivel de seguridad que la zona de seguridad en estudio. Las comunicaciones hacia y desde la zona de referencia (la zona que define la comunicación como no segura) deben validarse antes de aceptar la información.

5.11 Niveles de seguridad

5.11.1 General

El concepto de nivel de seguridad se ha creado para enfocarse en pensar en la seguridad en función de la zona en lugar de en un dispositivo individual o en un sistema. A menudo, un IACS consta de dispositivos y sistemas de múltiples proveedores, todos funcionando juntos para proporcionar las funciones de automatización integradas para la operación industrial. Así como las capacidades funcionales de los dispositivos individuales contribuyen a la capacidad del IACS, las capacidades de seguridad de los dispositivos individuales y las contramedidas implementadas deben funcionar entre sí para lograr el nivel de seguridad deseado para una zona. Los niveles de seguridad proporcionan un marco de referencia para tomar decisiones sobre el uso de contramedidas y dispositivos con diferentes capacidades de seguridad inherentes.

Los niveles de seguridad proporcionan un enfoque cualitativo para abordar la seguridad de una zona. Como método cualitativo, la definición del nivel de seguridad tiene aplicabilidad para comparar y administrar la seguridad de las zonas dentro de una organización. A medida que haya más datos disponibles y se desarrollen las representaciones matemáticas de riesgos, amenazas e incidentes de seguridad, este concepto pasará a un enfoque cuantitativo para la selección y

verificación de los Niveles de Seguridad (SL). Tendrá aplicabilidad tanto para compañías de usuarios finales como para proveedores de IACS y productos de seguridad. Se usará para seleccionar dispositivos IACS y contramedidas para usar dentro de una zona e identificar y comparar la seguridad de zonas en diferentes organizaciones en todos los segmentos de la industria.

Cada organización que utilice el método de nivel de seguridad debe establecer una definición de lo que representa cada nivel y cómo medir el nivel de seguridad de la zona. Esta definición o caracterización debe usarse de manera consistente en toda la organización. El nivel de seguridad se puede usar para identificar una estrategia integral de defensa en profundidad en capas para una zona que incluye contramedidas técnicas basadas en hardware y software junto con contramedidas de tipo administrativo.

El nivel de seguridad corresponde a la efectividad requerida de las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas para una zona o conducto en función de la evaluación del riesgo para la zona o conducto. El método de nivel de seguridad proporciona la capacidad de clasificar el riesgo para una zona o conducto. También ayuda a definir la efectividad requerida de las contramedidas utilizadas para evitar una intervención electrónica no autorizada que pueda leer o afectar el funcionamiento normal de los dispositivos y sistemas dentro de la zona o conducto. El nivel de seguridad es una propiedad de una zona y conducto en lugar de un dispositivo, sistema o cualquier parte de un sistema.

Se recomienda un mínimo de tres niveles de seguridad. Los tres niveles se pueden describir cualitativamente como se muestra en la Tabla 8. Las organizaciones pueden optar por ampliar esto y definir niveles de seguridad adicionales para describir sus requisitos de seguridad únicos.

Tabla 8 - Niveles de seguridad

Nivel de seguridad	Descripción cualitativa
1	bajo
2	medianas
3	alto

5.11.2 Tipos de niveles de seguridad

5.11.2.1 General

Se pueden definir tres tipos diferentes de niveles de seguridad de la siguiente manera:

a) SL (objetivo): nivel de seguridad objetivo para una zona o conducto;
b) SL (logrado): nivel de seguridad alcanzado de una zona o conducto;
c) SL (capacidad): capacidad de nivel de seguridad de contramedidas asociadas con una zona o conducto o capacidad de nivel de seguridad inherente de dispositivos o sistemas dentro de una zona o conducto.

5.11.2.2 SL (objetivo) - nivel de seguridad objetivo

Se debe asignar un nivel de seguridad objetivo a una zona. Se puede asignar un nivel de seguridad objetivo a un conducto. SL (objetivo) para una zona y conducto se determina durante la evaluación de riesgos. No es necesario asignar un nivel de seguridad objetivo a los conductos siempre que las propiedades de seguridad asociadas con el conducto se tengan en cuenta durante la evaluación del riesgo de las zonas que utilizan el conducto en consideración. La evaluación de riesgos debe tener en cuenta la probabilidad y las consecuencias de la seguridad de una zona o conducto comprometido. La evaluación de riesgos puede ser cualitativa, semicuantitativa o cuantitativa. SL (objetivo) determina la efectividad requerida de contramedidas, dispositivos y sistemas que deben estar en su lugar para evitar que la seguridad de la zona o el conducto se vea comprometida.

Las contramedidas pueden ser:

a) contramedidas técnicas (cortafuegos, software antivirus, etc.);
b) contramedidas administrativas (políticas y procedimientos);
c) contramedidas físicas (puertas cerradas, etc.).

Los factores que influyen en la determinación de SL (objetivo) para una zona y conducto son:

d) arquitectura de red con límites y conductos de zona definidos;
e) SL (objetivo) de las zonas con las que se comunicará la zona considerada;
f) SL (objetivo) del conducto, si está asignado, utilizado para la comunicación por la zona;
g) acceso físico a dispositivos y sistemas dentro de la zona.

Dentro de la zona, calcular el nivel de seguridad objetivo debe basarse en capas de seguridad y su impacto en el conjunto.

5.11.2.3 SL (logrado) - nivel de seguridad alcanzado

El SL (logrado) de una zona o conducto depende de las propiedades de seguridad inherentes de los dispositivos y sistemas dentro de la zona o conducto y / o propiedades de contramedidas que están en su lugar para evitar que la seguridad de la zona o conducto se vea comprometida. SL (logrado) es una función del tiempo y disminuye con el tiempo debido a la degradación de las contramedidas, las nuevas vulnerabilidades, las amenazas ajustadas o los métodos de ataque, la violación de las capas de seguridad y las propiedades de seguridad inherentes de los dispositivos y sistemas hasta que se revisen, actualicen o perfeccionen.

El objetivo es asegurar que en cualquier momento dado SL (logrado) de una zona o conducto sea mayor o igual que SL (objetivo) para la zona o conducto.

5.11.2.4 SL (capacidad): capacidad de nivel de seguridad de contramedidas, dispositivos o sistemas

SL (capacidad) se define para contramedidas y propiedades de seguridad inherentes de dispositivos y sistemas dentro de una zona o conducto que contribuyen a la seguridad de una zona o conducto. Es una medida de la efectividad de la contramedida, dispositivo o sistema para la propiedad de seguridad que abordan.

A continuación, se dan ejemplos de propiedades de seguridad que pueden ser abordadas por una contramedida, dispositivo o sistema:

a) probar la autenticidad de la entidad par;
b) preservar la autenticidad e integridad de los mensajes;
c) preservar la confidencialidad de los mensajes / información / comunicación;
d) garantizar la rendición de cuentas (no repudio);
e) hacer cumplir las políticas de control de acceso;
f) prevenir ataques de denegación de servicio;
g) mantener la confiabilidad de la plataforma;
h) detectar la manipulación;
i) monitorear el estado de seguridad.

El SL (capacidad) de una contramedida, dispositivo o sistema dentro de una zona o conducto contribuye al SL (logrado) en función de las propiedades de seguridad relevantes abordadas por las contramedidas, dispositivos o sistemas para esa zona o conducto.

5.11.3 Factores que influyen en el SL (logrado) de una zona o conducto

5.11.3.1 General

Hay varios factores que contribuyen al SL (logrado) de una zona o conducto. El SL (logrado) de una zona o conducto puede expresarse en función de estos factores:

SL (logrado) = f (x1,…, xn, t)

Donde los factores xi (1 <= i <= n) incluyen, pero no se limitan a lo siguiente:
x1: SL (capacidad) de contramedidas asociadas con la zona o conducto y las propiedades de seguridad inherentes de los dispositivos y sistemas dentro de una zona o conducto;
x2: SL (logrado) por las zonas con las cuales se establecerá la comunicación;
x3: Tipo de conductos y propiedades de seguridad asociados con los conductos utilizados para comunicarse con otras zonas (aplicable solo a zonas);
x4: Efectividad de las contramedidas;
x5: Intervalo de auditoría y prueba de contramedidas y propiedades de seguridad inherentes de dispositivos y sistemas dentro de una zona o conducto;
x6: Experiencia del atacante y recursos disponibles para el atacante;
x7: degradación de contramedidas y propiedades de seguridad inherentes de dispositivos y sistemas;
x8: detección de intrusiones;
t: tiempo.

Estos parámetros se describen con más detalle en las siguientes subcláusulas.

5.11.3.2 SL (capacidad) de contramedidas y propiedades de seguridad inherentes

Las propiedades de seguridad relevantes abordadas por contramedidas, dispositivos y sistemas dentro de la zona o conducto y su efectividad contribuyen al SL (logrado) por una zona o conducto.

Las contramedidas pueden ser capaces de abordar varias propiedades de seguridad, pero si ninguna de ellas es relevante para la seguridad de la zona o conducto, tales contramedidas no contribuyen al SL (logrado) de esa zona o conducto. De manera similar, si las propiedades de seguridad inherentes de los dispositivos y sistemas dentro de la zona o conducto no son relevantes para la seguridad de la zona o conducto, no contribuyen al SL (logrado) de esa zona o conducto.

5.11.3.3 SL (logrado) por zonas con las cuales se establecerá la comunicación

La seguridad de una zona o conducto no puede considerarse de forma aislada. Se ve afectado por el SL (logrado) de las zonas con las que se comunica.

Por ejemplo, considere un SIS en una planta química que se comunica con un DCS a través de un enlace en serie. Suponiendo que el DCS y el SIS están en dos zonas separadas, el SL (logrado) por la zona SIS estará influenciado por el SL (logrado) por la zona DCS.

5.11.3.4 Tipo de conductos y propiedades de seguridad asociadas con los conductos

El conducto puede ser un enlace punto a punto, LAN o WAN con propiedades de seguridad inherentes. El conducto puede incluir contramedidas que mejoran las propiedades de seguridad del conducto. Las propiedades de seguridad de un conducto que contribuyen a la seguridad del conducto contribuirán al SL (logrado) por el conducto. Las propiedades de seguridad de un conducto, utilizadas por una zona para comunicarse con otras zonas, contribuirán al SL (logrado) por la zona.

5.11.3.5 Efectividad de las contramedidas

Se pueden implementar contramedidas técnicas y administrativas para ayudar a lograr el SL (objetivo) deseado para una zona o conducto.

Varias contramedidas técnicas que abordan diferentes propiedades de seguridad están disponibles para su implementación con un IACS. Las contramedidas técnicas deben abordar las propiedades de seguridad relevantes para la zona, pero si esas propiedades de seguridad no son efectivas para esa zona, entonces su contribución a SL (lograda) por la zona es muy baja o ninguna. Los ejemplos de contramedidas técnicas incluyen sistemas de detección de intrusos (IDS), firewalls y software antivirus.

Una evaluación de la efectividad de las contramedidas técnicas debe tener en cuenta lo siguiente:

a) Proceso de desarrollo: disponibilidad de procedimientos escritos, plan de gestión de calidad, etc. Esto ayudará a reducir errores sistemáticos como errores de software o fugas de memoria que pueden afectar la seguridad.
b) Pruebas: nivel de prueba para cada propiedad de seguridad abordada por las contramedidas, dispositivos o sistemas. Los datos de prueba también pueden inferirse de sistemas evaluados previamente.
c) Recopilación de datos: número de veces que una zona o conducto se vio comprometido debido a una falla en una contramedida, dispositivo o sistema similar; tasa y criticidad de vulnerabilidades descubiertas para la contramedida, dispositivo o sistema.

Las contramedidas administrativas deben usarse cuando las contramedidas técnicas no son factibles. Un ejemplo de una medida administrativa es restringir el acceso físico a los componentes de IACS.

5.11.3.6 Intervalo de auditoría y prueba de contramedidas

La efectividad de las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas deben auditarse y / o probarse a intervalos regulares según los procedimientos que auditarán y / o probarán al menos las propiedades de seguridad relevantes para una zona. En algunos casos, el descubrimiento de nuevas vulnerabilidades también puede desencadenar una auditoría o prueba.

5.11.3.7 Experiencia del atacante y recursos disponibles para el atacante

La experiencia del atacante y los recursos, incluidas las herramientas y el tiempo, disponibles para un atacante afectan el SL (logrado) de una zona o conducto. Se deben asumir las capacidades y herramientas del atacante aceptadas por la industria. El tiempo disponible para que un atacante comprometa la seguridad de una zona dependerá de la aplicación y las contramedidas implementadas para la zona o conducto.

5.11.3.8 Degradación de las contramedidas

Las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas se degradarán efectivamente con el tiempo, disminuyendo así el SL (logrado) de una zona o conducto. La degradación de las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas ocurre debido a lo siguiente:

a) descubrimiento de nuevas vulnerabilidades;
b) habilidades mejoradas de los atacantes;
c) familiaridad del atacante con las contramedidas existentes;
d) disponibilidad de mejores recursos para los atacantes.

5.11.3.9 Detección de intrusos

Las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas pueden incluir la detección de intrusos. El tiempo disponible para responder a una intrusión detectada impacta el SL (logrado) de una zona y conducto.

5.11.4 Impacto de contramedidas y propiedades de seguridad inherentes de dispositivos y sistemas

El uso de contramedidas y propiedades de seguridad inherentes de los dispositivos y sistemas para lograr el SL (objetivo) puede provocar una degradación en el rendimiento de la comunicación. La degradación en el rendimiento de la comunicación debido a las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas deben evaluarse para garantizar que aún se cumplan los requisitos funcionales mínimos de la zona.

Por ejemplo, la velocidad de respuesta es un requisito importante para un IACS. Las contramedidas pueden agregar latencia a la comunicación, lo que puede no ser aceptable en ciertas aplicaciones.

5.12 Ciclo de vida del nivel de seguridad

5.12.1 General

Los niveles de seguridad se convierten en una parte importante del ciclo de vida de seguridad de una zona IACS una vez que se han definido los límites y conductos de la zona. Es importante reconocer que el ciclo de vida del nivel de seguridad se centra en el nivel de seguridad de una zona o conducto a lo largo del tiempo. No debe confundirse con las fases del ciclo de vida de los activos físicos reales que comprenden los IACS dentro de la zona. Aunque hay muchas actividades superpuestas y complementarias asociadas con el ciclo de vida de los activos y el ciclo de vida del nivel de seguridad de la zona, cada uno tiene diferentes puntos de activación para moverse de una fase a otra. Además, un cambio en un activo físico puede desencadenar un conjunto de actividades de nivel de seguridad, o un cambio en las vulnerabilidades de seguridad o, un activo puede desencadenar un cambio en el activo físico.

La Figura 8 muestra el ciclo de vida del nivel de seguridad. A una zona se le asigna un SL (objetivo) durante la fase de evaluación del ciclo de vida de la seguridad. Las contramedidas se implementan durante la fase de Implementación para cumplir con el SL (objetivo) de la zona. SL (logrado) por una zona depende de varios factores. Para garantizar que el SL (logrado) sea mejor o igual que el SL (objetivo) para la zona en todo momento, las contramedidas se auditan y / o prueban y actualizan, si es necesario, durante la fase de Mantenimiento del ciclo de vida de la seguridad.

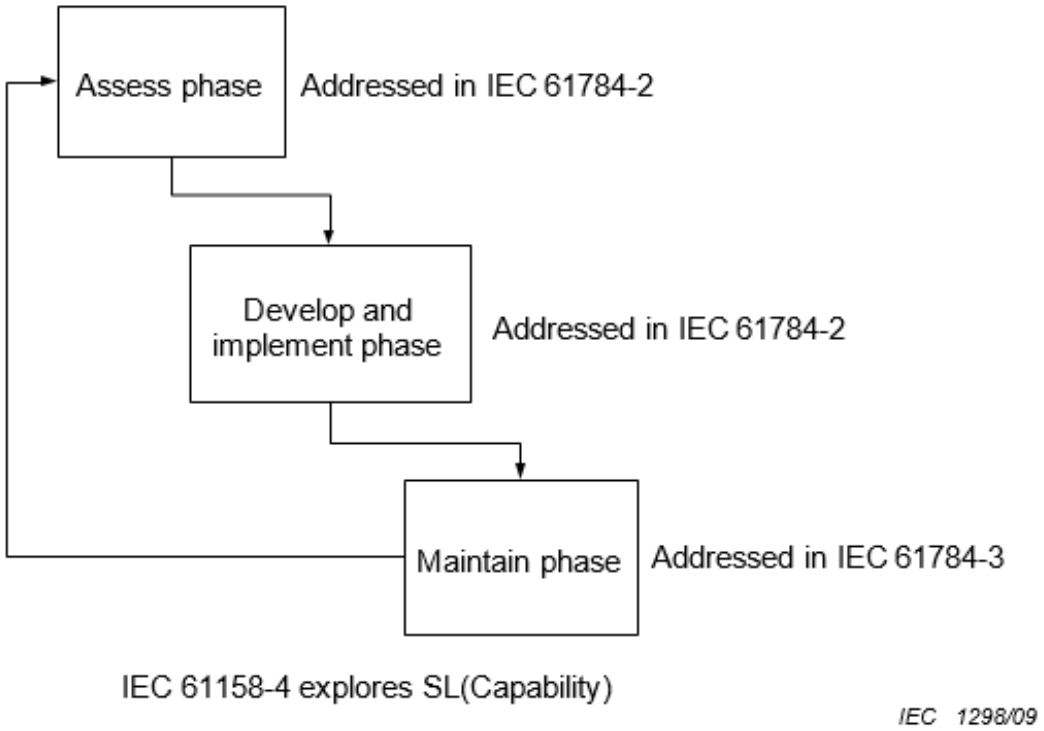

Figura 8 - Ciclo de vida del nivel de seguridad

5.12.2 Fase de evaluación

La fase de evaluación del ciclo de vida del nivel de seguridad incluye las actividades que se muestran en la Figura 9. Antes de asignar SL (objetivo) a una zona, es necesario establecer lo siguiente:

a) límites de zona;
b) los criterios de tolerancia al riesgo de la organización.

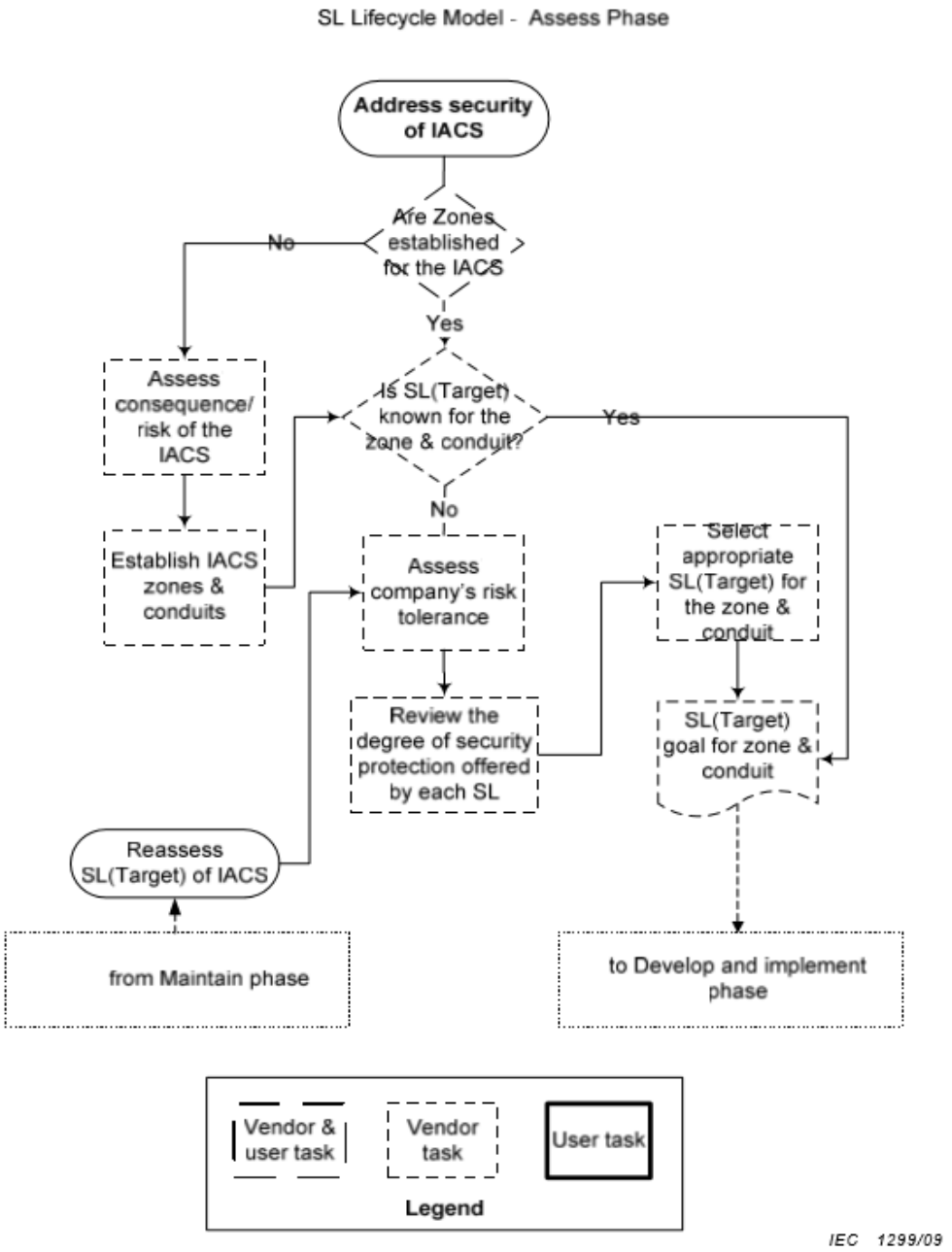

Figura 9 - Ciclo de vida del nivel de seguridad - Fase de evaluación

Se debe realizar una evaluación de riesgos para una zona y asignar SL (objetivo) a la zona. Los detalles de la evaluación de riesgos y otras actividades asociadas con la fase de evaluación se abordarán en una parte futura de IEC 62443.

5.12.3 Fase de desarrollo e implementación

Una vez que se ha asignado un SL (objetivo) a una zona en la fase de evaluación, se deben implementar contramedidas para alcanzar SL (logrado) mejor o igual a SL (objetivo) para la zona. La Figura 10 muestra las actividades, para zonas IACS nuevas y existentes, en la fase de Implementación del ciclo de vida del nivel de seguridad. El SL (logrado) se determina después de que el sistema se haya validado según los requisitos de seguridad para la zona.

Los detalles de las actividades asociadas con la fase de implementación se abordarán en una parte futura de IEC 62443.

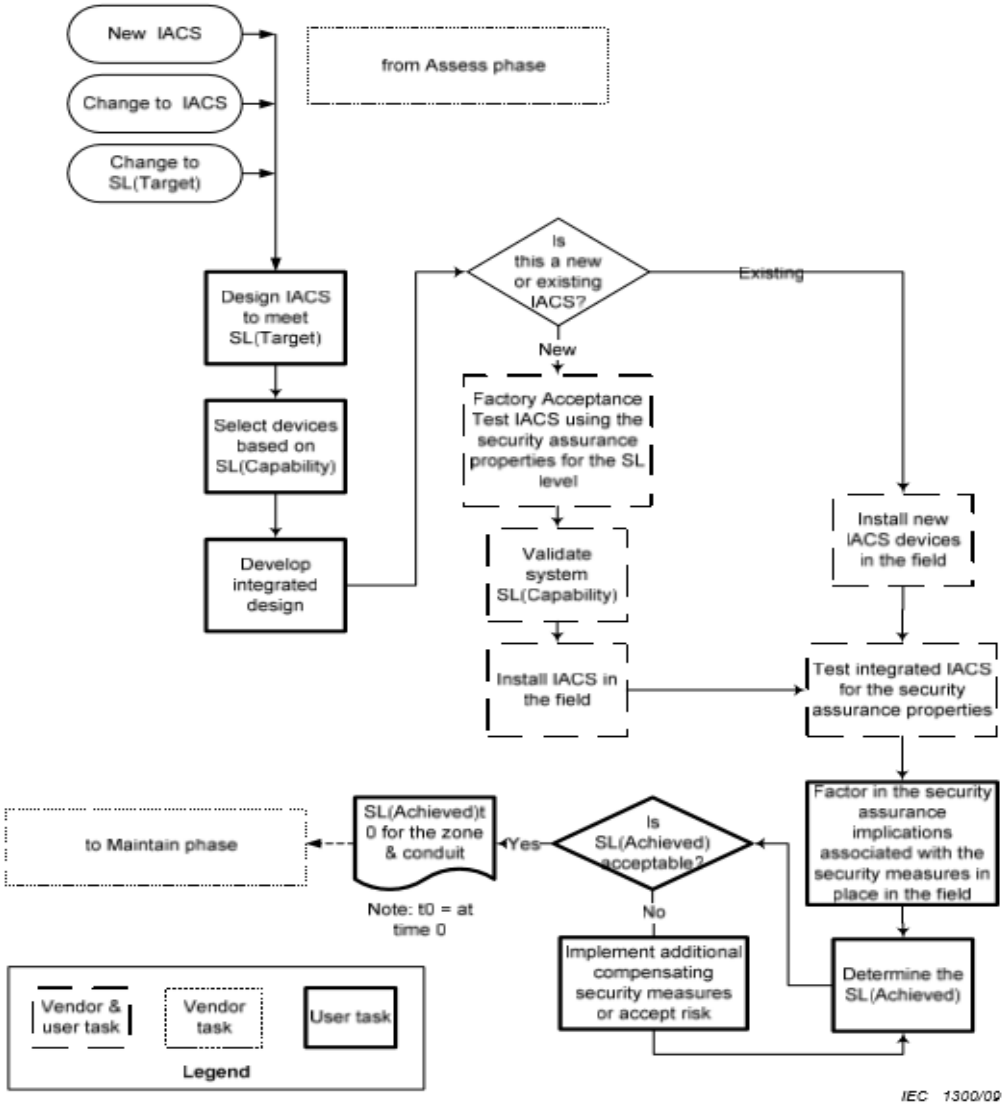

Figura 10 - Ciclo de vida del nivel de seguridad - Fase de implementación

5.12.4 Fase de mantenimiento

Las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas se degradan con el tiempo. Las propiedades de seguridad relevantes para la zona, incluidos los conductos asociados con la zona, deben auditarse y / o probarse a intervalos regulares o siempre que se descubra una nueva vulnerabilidad para garantizar que SL (logrado) sea mejor o igual a SL (objetivo) para la zona en cualquier momento. Las actividades asociadas con el mantenimiento del SL (logrado) por una zona se muestran en la Figura 11.

Los detalles de las actividades asociadas con la fase de mantenimiento se abordarán en una parte futura de IEC 62443

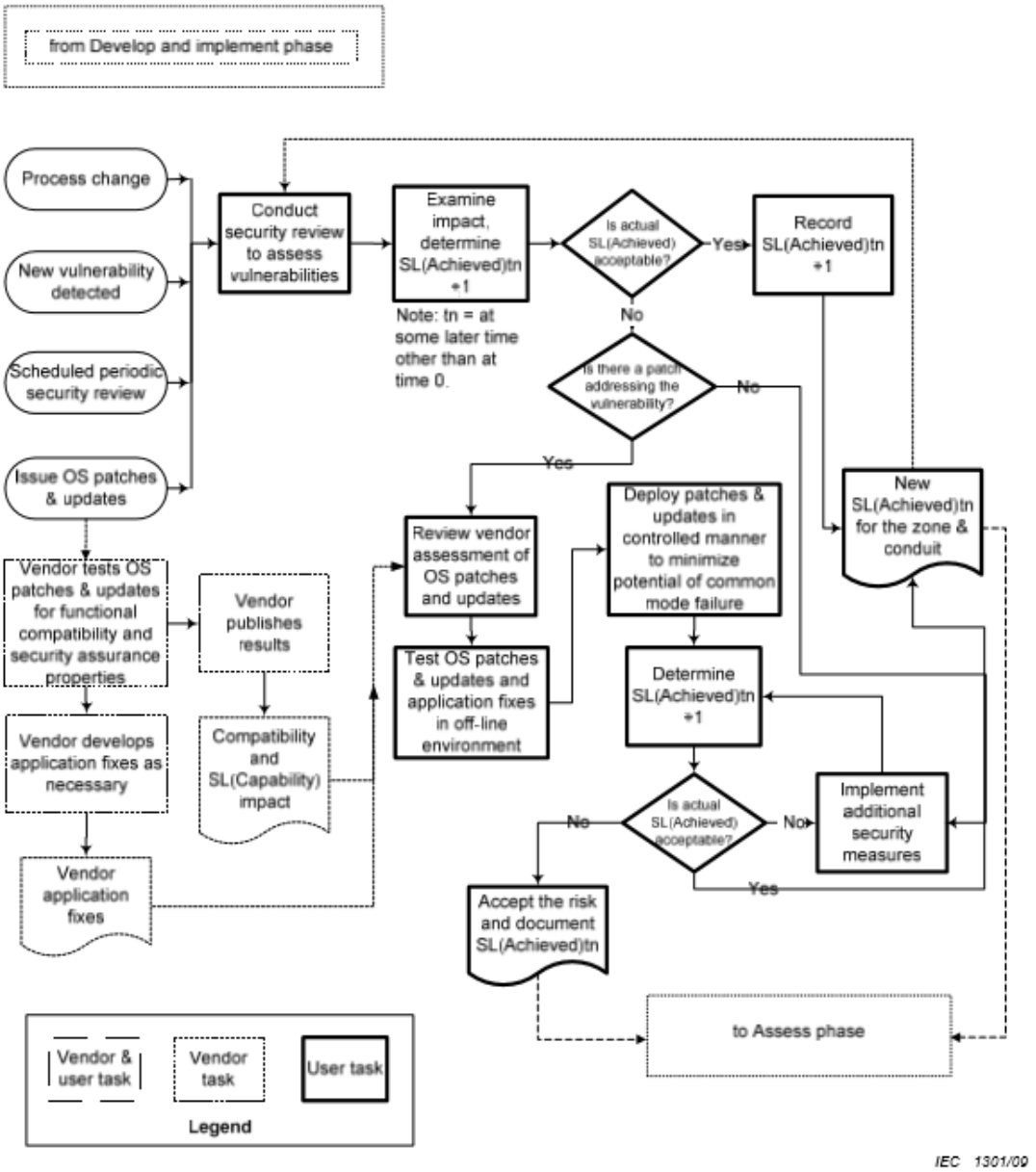

Figura 11 - Ciclo de vida del nivel de seguridad - Fase de mantenimiento

6 Modelos

6.1 General

Esta cláusula describe una serie de modelos que pueden usarse en el diseño de un programa de seguridad apropiado. El objetivo es identificar las necesidades de seguridad y las características importantes del entorno a un nivel de detalle necesario para abordar los problemas de seguridad con una comprensión común del marco y el vocabulario. Estos modelos vienen en varias formas, que incluyen:

a) Modelos de referencia que proporcionan la base conceptual general para los modelos más detallados que siguen.
b) Modelos de activos que describen las relaciones entre activos dentro de un sistema de automatización y control industrial.
c) Una arquitectura de referencia que describe la configuración de los activos. Una arquitectura de referencia puede ser única para cada empresa o subconjunto de la empresa. Es único para cada situación, dependiendo del alcance del Sistema de Control y Automatización Industrial que se está revisando.
d) Un modelo de zona que agrupa elementos de arquitectura de referencia de acuerdo con características definidas. Esto proporciona un contexto para la definición de políticas, procedimientos y pautas, que a su vez se aplican a los activos.

Toda esta información se utiliza para desarrollar un programa detallado para gestionar la seguridad de un sistema de automatización y control industrial.

Cada uno de los principales tipos de modelos se describe con más detalle en las siguientes subcláusulas.

6.2 Modelos de referencia

6.2.1 Descripción general

Un modelo de referencia establece un marco de referencia para la información más detallada que sigue. El término "modelo de referencia" se hizo popular con el éxito del modelo ISO de siete capas para la interconexión de sistemas abiertos (OSI). La Oficina de Estándares y Tecnología (NOST) de la NASA de EE. UU. Define el término como:

“Un modelo de referencia es un marco para comprender relaciones significativas entre las entidades de algún entorno y para el desarrollo de estándares o especificaciones consistentes que respalden ese entorno. Un modelo de referencia se basa en un pequeño número de conceptos unificadores y puede usarse como base para la educación y para explicar los estándares a especialista." [8]

Un modelo de referencia describe una vista genérica de un sistema integrado de fabricación o producción, expresado como una serie de niveles lógicos. El modelo de referencia utilizado por la serie de normas IEC 62443 aparece en la Figura 12. Este modelo se deriva del modelo general utilizado en IEC 62264-1.

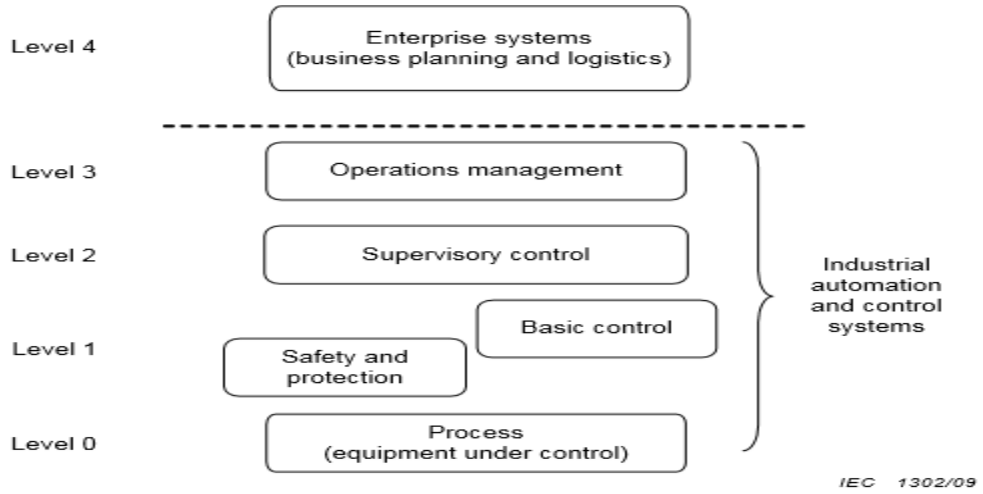

Figura 12 - Modelo de referencia para estándares IEC 62443

Se puede utilizar una vista ligeramente diferente del modelo de referencia para aplicaciones SCADA. Esta vista se muestra en la Figura 13.

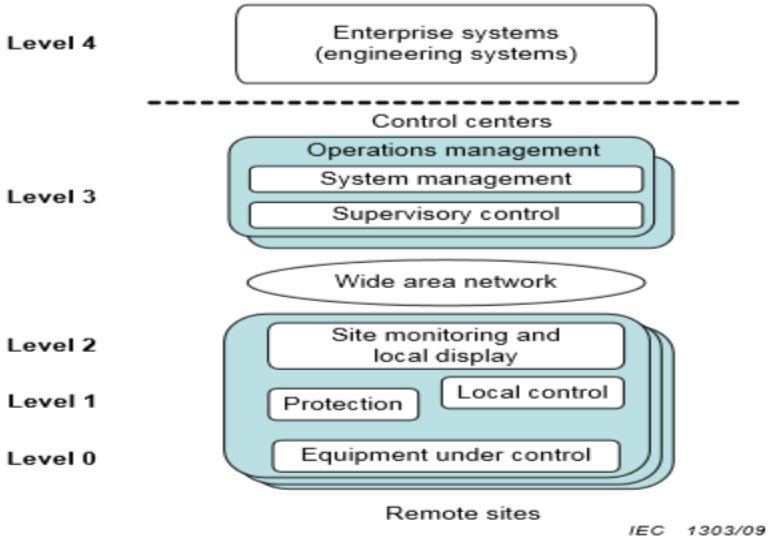

Figura 13 - Modelo de referencia SCADA

6.2.2 Niveles del modelo de referencia

6.2.2.1 General

Ambos modelos consisten en los mismos niveles básicos, cada uno representando una clase particular de funcionalidad. Las definiciones de nivel se basan en el modelo de jerarquía funcional de IEC 62264-1 y describen las funciones y actividades desde el proceso (Nivel 0) hasta la empresa (Nivel 4).

Las siguientes subcláusulas describen cada uno de los niveles de este modelo con más detalle.

6.2.2.2 Nivel 4 - Sistemas empresariales

Este nivel, descrito como planificación empresarial y logística en IEC 62264-1, se define como la inclusión de las funciones involucradas en las actividades relacionadas con el negocio necesarias para administrar una organización de fabricación. Las funciones incluyen sistemas financieros regionales o empresariales y otros componentes de infraestructura empresarial, tales como programación de producción, gestión operativa y gestión de mantenimiento para una planta o sitio individual en una empresa. A los fines de esta especificación técnica, los sistemas de ingeniería también se consideran en este nivel.

Las actividades de nivel 4 incluyen las siguientes actividades:

a) Recopilar y mantener el uso de materias primas y repuestos y el inventario disponible, y proporcionar datos para la compra de materias primas y repuestos.
b) Recopilar y mantener el uso general de energía y el inventario disponible y proporcionar datos para la compra de la fuente de energía.
c) Recopilar y mantener bienes generales en los archivos de inventario de proceso y producción.
d) Recopilar y mantener archivos de control de calidad en relación con los requisitos del cliente.
e) Recopilar y mantener el uso de maquinaria y equipos y los archivos de historial de vida necesarios para la planificación del mantenimiento preventivo y predictivo.
f) Recopilar y mantener datos de uso de mano de obra para su transmisión al personal y contabilidad.
g) Establecer el cronograma básico de producción de la planta.
h) Modificar el cronograma básico de producción de la planta para los pedidos recibidos en función de los cambios de disponibilidad de recursos, fuentes de energía disponibles, niveles de demanda de energía y requisitos de mantenimiento.
i) Desarrollar programas óptimos de mantenimiento preventivo y renovación de equipos en coordinación con el programa básico de producción de la planta.
j) Determinar los niveles óptimos de inventario de materias primas, fuentes de energía, repuestos y bienes en proceso en cada punto de almacenamiento. Estas funciones también incluyen la planificación de necesidades de materiales (MRP) y la adquisición de repuestos.
k) Modificar el cronograma básico de producción de la planta según sea necesario siempre que ocurran interrupciones importantes de la producción.
l) Planificación de la capacidad basada en todas las actividades anteriores.

6.2.2.3 Nivel 3 - Gestión de operaciones

El nivel 3 incluye las funciones involucradas en la gestión de los flujos de trabajo para producir los productos finales deseados. Los ejemplos incluyen el despacho de producción, la programación detallada de la producción, la garantía de confiabilidad y la optimización del control en todo el sitio.

Las actividades de nivel 3 incluyen las siguientes actividades:

a) Informar sobre la producción en el área, incluidos los costos variables de fabricación.
b) Recopilar y mantener datos del área sobre producción, inventario, mano de obra, materias primas, repuestos y uso de energía.
c) Realizar la recopilación de datos y el análisis fuera de línea según lo requieran las funciones de ingeniería. Esto puede incluir análisis estadísticos de calidad y funciones de control relacionadas.

d) Llevar a cabo las funciones necesarias del personal, tales como: estadísticas del período de trabajo (por ejemplo: tiempo, tarea), horario de vacaciones, horarios de la fuerza laboral, línea de progresión sindical, capacitación interna y calificación del personal.
e) Establecer el cronograma de producción detallado inmediato para su propia área, incluido el mantenimiento, el transporte y otras necesidades relacionadas con la producción.
f) Optimización local de los costos para su área de producción individual mientras se lleva a cabo el cronograma de producción establecido por las funciones de Nivel 4.
g) Modificar los cronogramas de producción para compensar las interrupciones en la producción de la planta que puedan ocurrir en su área de responsabilidad.

6.2.2.4 Nivel 2 - Control de supervisión

El nivel 2 incluye las funciones involucradas en el monitoreo y control del proceso físico. Por lo general, hay varias áreas de producción en una planta, como la destilación, la conversión, la mezcla en una refinería o la plataforma de la turbina, y las instalaciones de procesamiento de carbón en una planta de servicios públicos.

Las funciones de nivel 2 incluyen lo siguiente:

a) interfaz de operador hombre-máquina;
b) alarmas y alertas del operador;
c) funciones de control de supervisión;
d) recopilación del historial de procesos.

6.2.2.5 Nivel 1 - Control local o básico

El nivel 1 incluye las funciones involucradas en la detección y manipulación del proceso físico.

El equipo de monitoreo de procesos lee los datos de los sensores, ejecuta algoritmos si es necesario y mantiene el historial del proceso. Los ejemplos de sistemas de monitoreo de procesos incluyen sistemas de medición de tanques, monitores de emisión continua, sistemas de monitoreo de equipos rotativos y sistemas de indicación de temperatura. El equipo de control de proceso es similar. Lee datos de sensores, ejecuta un algoritmo de control, y envía una salida a un elemento final (por ejemplo, válvulas de control o accionamientos de compuerta). Los controladores de nivel 1 están conectados directamente a los sensores y actuadores del proceso.

El nivel 1 incluye control continuo, control de secuencia, control de lotes y control discreto. Muchos controladores modernos incluyen todo tipo de control en un solo dispositivo.

También se incluyen en el Nivel 1 los sistemas de seguridad y protección[4] que monitorean el proceso y automáticamente lo devuelven a un estado seguro si excede los límites seguros. Esta categoría también incluye sistemas que monitorean el proceso y alertan a un operador de condiciones peligrosas inminentes.

_____
4 Estos sistemas se denominan sistemas instrumentados de seguridad en estándares como la serie IEC 61511.

Los sistemas de seguridad y protección se han implementado tradicionalmente usando controladores físicamente separados, pero más recientemente se ha hecho posible implementarlos usando un método conocido como separación lógica, dentro de una infraestructura común. La representación que se muestra en este modelo de referencia se eligió para enfatizar la necesidad de esta separación (lógica o física) para garantizar la integridad de las funciones de seguridad. El equipo de nivel 1 incluye, pero no se limita a lo siguiente:

a) controladores DCS;
b) PLCs;
c) RTU.

Los sistemas de seguridad y protección a menudo tienen requisitos de seguridad adicionales que pueden no ser consistentes o relevantes para los requisitos de seguridad cibernética. Estos sistemas incluyen los sistemas de seguridad en uso en plantas químicas y petroquímicas como se identifica en la serie de normas IEC 61511, sistemas de seguridad de plantas nucleares o sistemas relacionados con la seguridad como se identifica en la serie IEC 61513 y funciones de protección como se identifica en los estándares de IEEE Power Engineering Society.

6.2.2.6 Nivel 0 – Proceso

El nivel 0 es el proceso físico real. El proceso incluye varios tipos diferentes de instalaciones de producción en todos los sectores, que incluyen, entre otros, fabricación de piezas discretas, procesamiento de hidrocarburos, distribución de productos, productos farmacéuticos, pulpa y papel y energía eléctrica.

El nivel 0 incluye los sensores y actuadores conectados directamente al proceso y al equipo del proceso.

6.3 Modelos de activos

6.3.1 Descripción general

Los sistemas de control modernos son redes informáticas complejas con muchos componentes interconectados que realizan una variedad de tareas para operar de manera segura y eficiente plantas químicas, plantas de fabricación de autopartes, tuberías, instalaciones de generación eléctrica, redes de transmisión y distribución, y muchos otros tipos de instalaciones industriales, transporte sistemas y utilidades.

Hubo un tiempo en que estos sistemas estaban aislados de otras computadoras en la empresa y usaban hardware, software y protocolos de red patentados. Este ya no es el caso, ya que los proveedores de sistemas de control han adaptado la tecnología de información COTS debido a sus ventajas de costos, y las necesidades comerciales han impulsado la integración de los sistemas de control con los sistemas de información empresarial.

Desde una perspectiva de seguridad, la preocupación es con el equipo de control en sí, los usuarios

de ese equipo, las conexiones entre los componentes del sistema de control y las interconexiones con los sistemas comerciales y otras redes.

Este documento está destinado a aplicarse a la amplia gama de Sistemas de Control y Automatización Industrial utilizados en múltiples segmentos de la industria. Por lo tanto, el modelo de activos debe comenzar en un nivel alto y ser lo suficientemente genérico como para adaptarse a las muchas situaciones en las que se implementan los sistemas de control. Ver Figura 14.

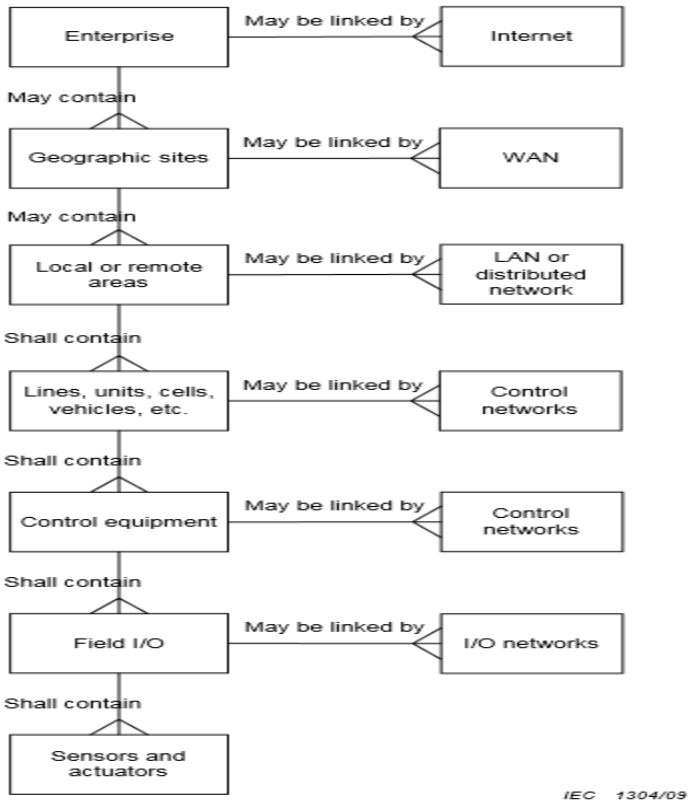

Figura 14 - Ejemplo de modelo de activos de fabricación de procesos

Debido a que las redes juegan un papel importante en la seguridad, el modelo de activos incluye explícitamente los elementos de red típicamente presentes en cada nivel de la jerarquía. En cada nivel, el equipo (o instalaciones) está unido por el tipo de red apropiado. Aunque las redes mismas pueden estar vinculadas entre sí, este modelo no representa ese vínculo.

Como es el caso con el modelo de referencia, hay una vista ligeramente diferente para las aplicaciones SCADA. Un modelo típico de activos SCADA se muestra en la Figura 15.

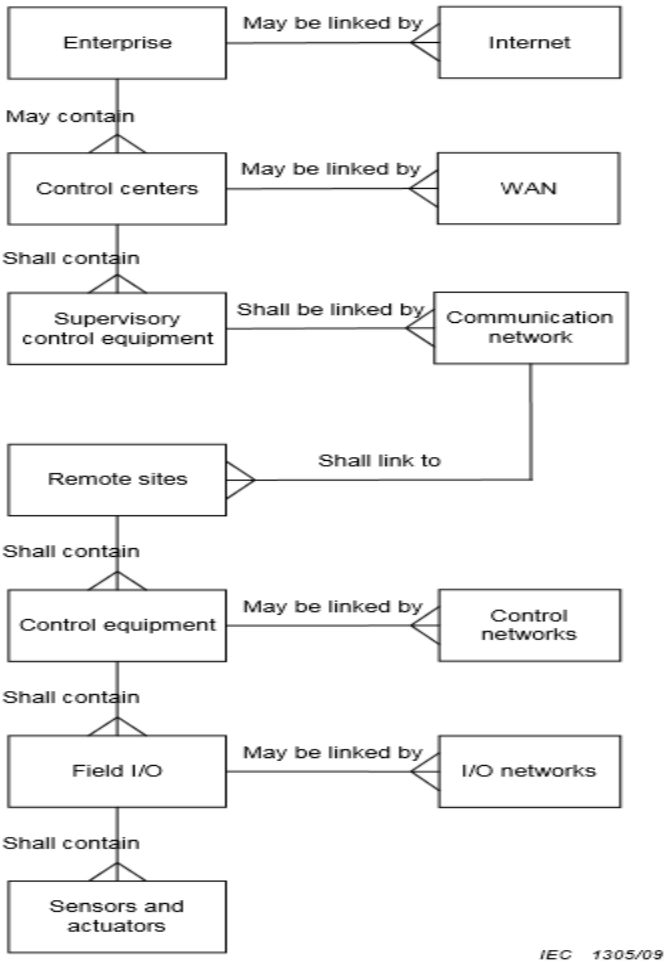

Figura 15 - Ejemplo de modelo de activos del sistema SCADA

El modelo de activos representa sistemas de información auxiliar que pueden estar presentes en varios niveles de la jerarquía. Estos sistemas no controlan directamente el proceso, pero interactúan con el equipo de control al recopilar datos y enviar recetas e instrucciones de proceso. Los sistemas de información de línea, área y sitio también actúan como repositorios para servir información de producción a los usuarios de toda la empresa y pueden interactuar con las aplicaciones de planificación de recursos empresariales que se ejecutan en el centro de datos corporativo.

El modelo se puede contraer o expandir según sea necesario para reflejar la entidad bajo revisión, siempre que sea coherente con los otros modelos y puntos de vista. Por ejemplo, una planta que solo tiene un área podría omitir la clasificación de área, siempre que la arquitectura de referencia y la zona posterior reflejen el modelo de activo colapsado.

6.3.2 Empresa

Una empresa es una entidad comercial que produce y transporta productos u opera y mantiene servicios de infraestructura. Las empresas a menudo están conectadas a Internet para comunicarse con otras empresas o para proporcionar información y servicios (como correo electrónico) a los empleados. Las empresas suelen operar uno o más centros de datos para respaldar sus requisitos

de procesamiento de información. La seguridad de los procesos comerciales respaldados por estos activos de TI está fuera del alcance de esta especificación técnica.

6.3.3 Sitios geográficos

6.3.3.1 General

Un sitio es un subconjunto del grupo de activos físicos, geográficos o lógicos de una empresa. Puede contener áreas, líneas de fabricación, celdas de proceso, unidades de proceso, centros de control y vehículos. Los sitios pueden estar conectados a otros sitios mediante una WAN. Un sitio puede incluir sistemas de información como un sistema de ejecución de fabricación que coordina las actividades de producción en el sitio.

6.3.3.2 Centro de control

Un centro de control es un tipo especial de sitio. Las industrias de infraestructura generalmente usan uno o más centros de control para supervisar o coordinar sus operaciones. Si la empresa tiene múltiples centros de control (por ejemplo: un centro de respaldo en un sitio separado), generalmente están conectados entre sí a través de una WAN. El centro de control contiene las computadoras Host SCADA y los dispositivos de visualización del operador asociados, además de los sistemas de información auxiliar, como un historiador.

6.3.3.3 Sitio remoto

Los sitios remotos contienen equipos en forma de PLC, unidades terminales remotas (RTU) o dispositivos electrónicos inteligentes (IED) que son responsables de monitorear y controlar las operaciones locales en el sitio. Los sitios remotos están conectados al centro de control mediante una red de comunicación (a veces denominada red de telemetría). Los sitios remotos también pueden conectarse entre sí (para facilitar funciones tales como la retransmisión protectora entre subestaciones en una red de transmisión eléctrica, por ejemplo).

6.3.4 Área

Un área es un subconjunto del grupo de activos físicos, geográficos o lógicos de un sitio. Puede contener líneas de fabricación, celdas de proceso y unidades de producción. Las áreas pueden estar conectadas entre sí por una LAN del sitio y pueden contener sistemas de información relacionados con las operaciones realizadas en esa área.

6.3.5 Líneas, unidades, celdas, vehículos

Las áreas están formadas por elementos de nivel inferior que realizan las funciones de fabricación, control de infraestructura o vehículo. Las entidades a este nivel pueden estar conectadas entre sí por una red de control de área y pueden contener sistemas de información relacionados con las operaciones realizadas en esa entidad.

6.3.6 Equipo de control de supervisión

El equipo de control de supervisión incluye los servidores de la computadora, HMI, redes de área local y dispositivos de comunicación que permiten a los operadores monitorear y controlar de forma remota las instalaciones que se extienden en un área geográfica amplia.

6.3.7 Equipo de control

El equipo de control incluye DCS, PLC, controladores de movimiento, unidades inteligentes y consolas de interfaz de operador asociadas que se utilizan para administrar y controlar el proceso. También incluye redes de bus de campo donde la lógica de control y los algoritmos se ejecutan en dispositivos de campo inteligentes que coordinan sus acciones.

6.3.8 Red de E / S de campo

La red de entrada / salida de campo (E / S) es el enlace de comunicaciones (por cable o inalámbrico) que conecta estos elementos al equipo de control.

6.3.9 Sensores y actuadores

Los sensores y actuadores son los elementos finales conectados al equipo de proceso.

6.3.10 Equipo bajo control

Debajo de los activos del sistema de control están los activos que conforman el equipo bajo control. Este nivel también se conoce como el proceso físico u operativo.

6.4 Arquitectura de referencia

La arquitectura de referencia se construye a partir de las entidades definidas en el modelo de activos. Una arquitectura de referencia es específica para cada situación bajo revisión y será específica para ese análisis. Cada organización crea una o más arquitecturas de referencia en función de las funciones empresariales realizadas, así como las funciones bajo revisión. Sería común que una organización tenga una arquitectura de referencia única para la corporación que se ha generalizado para cubrir todas las instalaciones operativas. Cada instalación o tipo de instalación también puede tener un diagrama de arquitectura de red de referencia más detallado que se expande en el modelo empresarial. En la Figura 16 se muestra un ejemplo de una arquitectura de referencia simplificada para una función de fabricación.

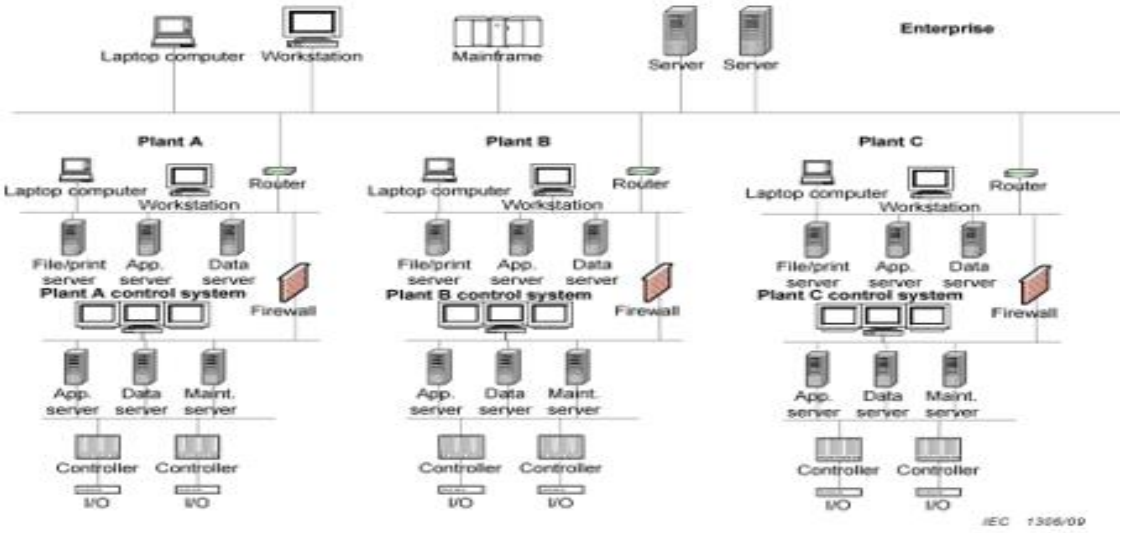

Figura 16 - Ejemplo de arquitectura de referencia

6.5 Modelo de zona y conducto

6.5.1 General

Se desarrolla un modelo de zona y conducto a partir de la arquitectura de referencia. Se utiliza para describir las agrupaciones lógicas de activos dentro de una empresa o un subconjunto de la empresa. Los activos se agrupan en entidades (por ejemplo, negocios, instalaciones, sitio o IACS) que luego se pueden analizar para conocer las políticas de seguridad y, por lo tanto, los requisitos. El modelo ayuda a evaluar amenazas comunes, vulnerabilidades y las contramedidas correspondientes necesarias para alcanzar el nivel de seguridad (nivel de seguridad objetivo) requerido para proteger los activos agrupados. Al agrupar los activos de esta manera, se puede definir una política de seguridad para todos los activos que son miembros de la zona. Este análisis se puede utilizar para determinar la protección adecuada requerida en función de las actividades realizadas en la zona.

NOTA: Se debe suponer que todos los usos no calificados del término "zona" en esta especificación técnica se refieren a una zona de seguridad.

6.5.2 Definición de zonas de seguridad

Al crear un programa de seguridad, las zonas son una de las herramientas más importantes para el éxito del programa, y la definición adecuada de las zonas es el aspecto más importante del proceso. Al definir las zonas, las organizaciones deben usar tanto la arquitectura de referencia como el modelo de activos para desarrollar las zonas de seguridad y los niveles de seguridad adecuados para cumplir con los objetivos de seguridad establecidos en la política de seguridad de los Sistemas de Control y Automatización Industrial.

Cuando se realizan actividades de diferentes niveles dentro de un dispositivo físico, una organización puede asignar el dispositivo físico a los requisitos de seguridad más estrictos, o crear una zona separada con una política de seguridad de zona separada que es una política combinada entre las dos zonas. Un ejemplo típico de esto ocurre en los servidores de historiador de procesos. Para que sea efectivo, el servidor necesita acceso a los dispositivos de control críticos que son la fuente de los datos que se recopilarán. Sin embargo, para satisfacer la necesidad comercial de presentar esos datos a los supervisores y los equipos de optimización de procesos, se requiere un acceso más liberal al dispositivo de lo que permiten los requisitos de seguridad del sistema de control típico.

Si se ejecutan múltiples aplicaciones que involucran diferentes niveles de actividades en un solo dispositivo físico, también se puede crear un límite de zona lógica. En este caso, el acceso a una aplicación particular está restringido a personas que tienen privilegios para ese nivel de aplicación. Un ejemplo es una sola máquina que ejecuta un servidor OPC y herramientas de análisis basadas en el cliente OPC. El acceso al servidor OPC está restringido a las personas que tienen privilegios de nivel superior, mientras que el acceso a las hojas de cálculo que utilizan el complemento de cliente OPC está disponible para todos los empleados.

6.5.3 Identificación de zona

Las zonas pueden ser una agrupación de activos independientes, una agrupación de subzonas o una combinación de activos independientes y activos que también se agrupan en subzonas contenidas

dentro de la zona principal. Las zonas tienen la característica de herencia, lo que significa que una zona secundaria (o subzona) debe cumplir con todos los requisitos de la zona principal. En la Figura 17 se muestra un modelo simplificado de zonas multiplantantes. Aquí la zona empresarial es la matriz y cada planta es una subzona secundaria con una subzona de control contenida dentro de la subzona de la planta.

NOTA: Hay una clara ventaja en alinear zonas de seguridad con áreas físicas o zonas en una instalación, por ejemplo, alinear un centro de control con una zona de seguridad de control.

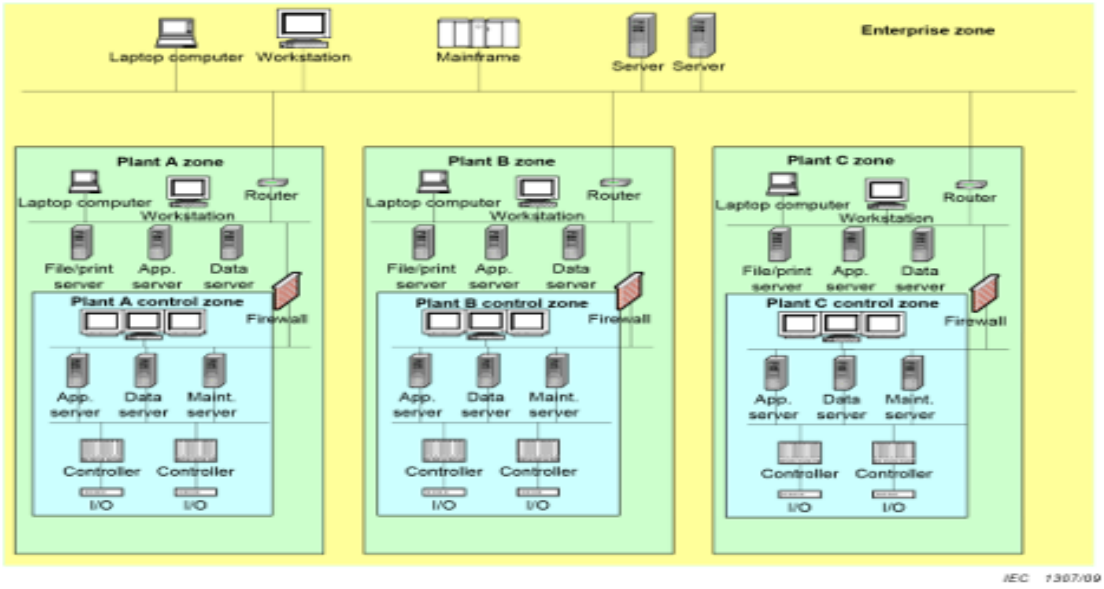

Figura 17 - Ejemplo de zona multiplanta

La misma arquitectura empresarial podría agruparse en zonas separadas como en la Figura 18. En este modelo, las políticas de zona serían independientes, y cada zona podría tener políticas de seguridad totalmente diferentes.

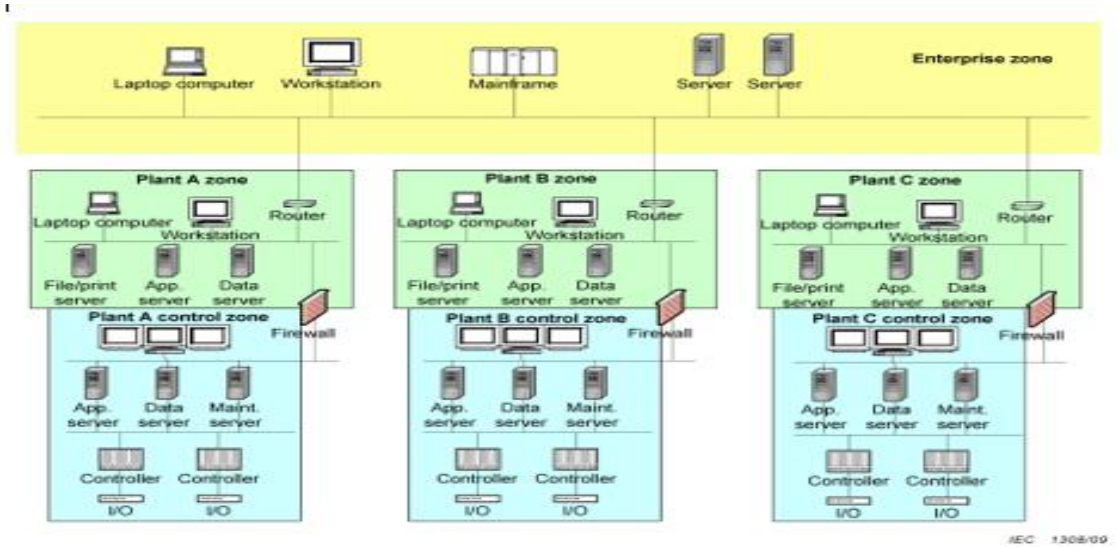

Figura 18 - Ejemplo de zonas separadas

Se pueden construir modelos similares para aplicaciones SCADA, como se muestra en la Figura 19 y la Figura 20.

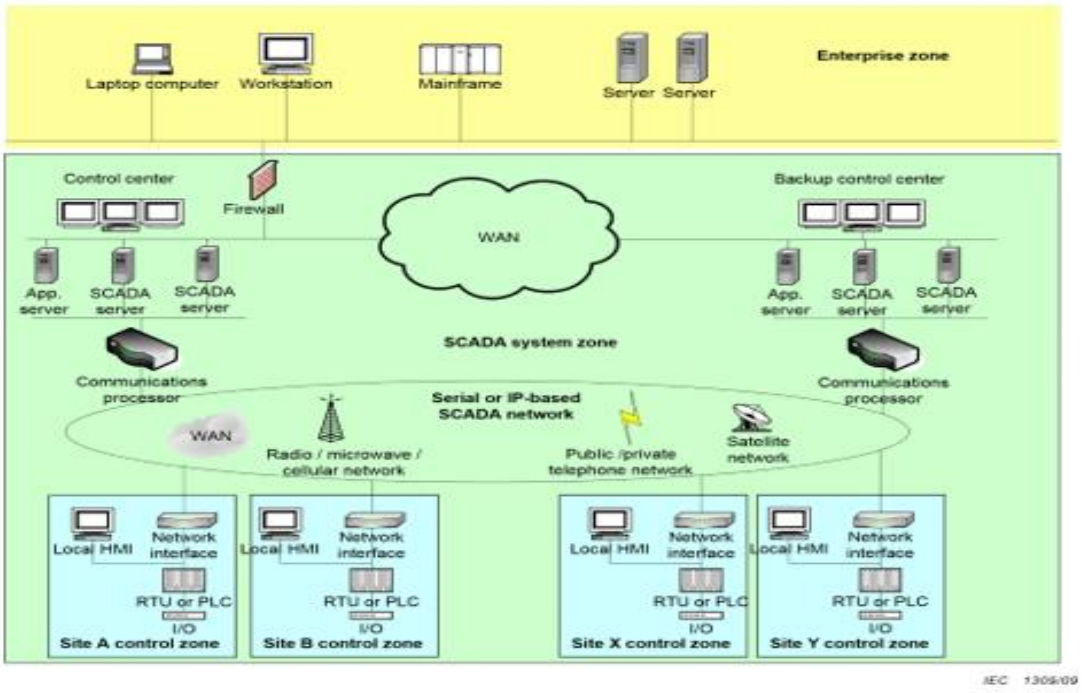

Figura 19 - Ejemplo de zona SCADA

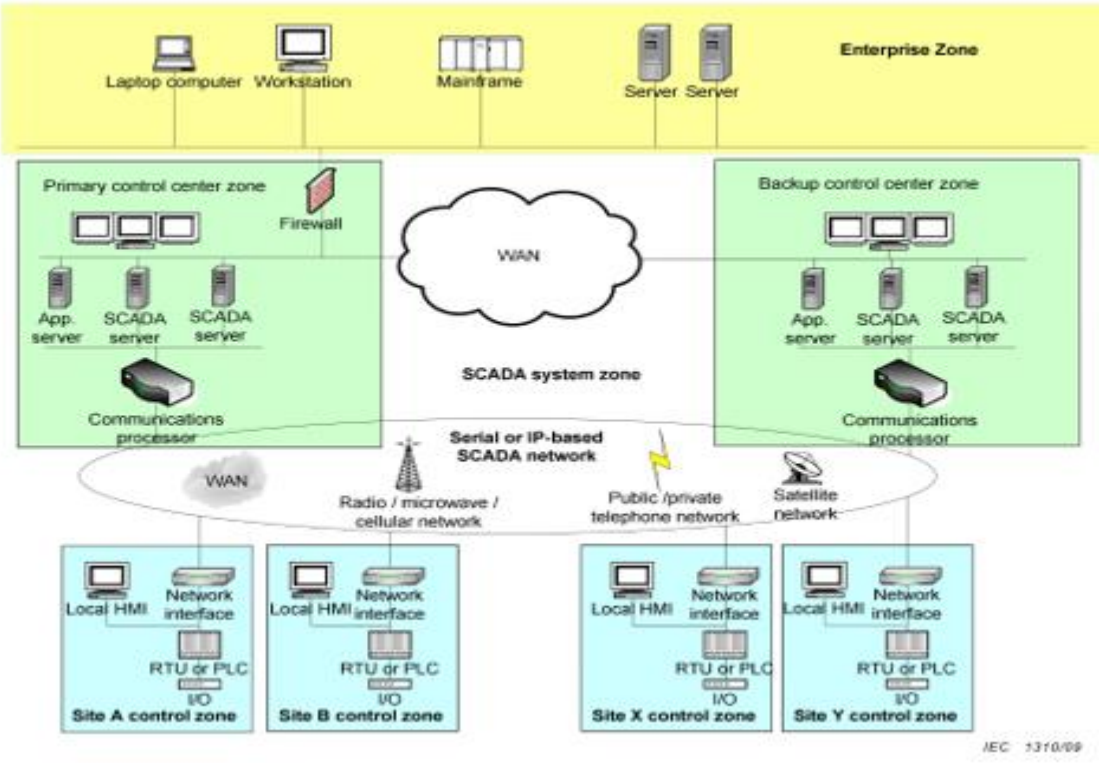

Figura 20 - Ejemplo de zonas separadas SCADA

6.5.4 Características de la zona

6.5.4.1 Descripción general

Cada zona tiene un conjunto de características y requisitos de seguridad que son sus atributos. Estos toman la forma de los siguientes atributos:

a) políticas de seguridad;
b) inventario de activos;
c) requisitos de acceso y controles;
d) amenazas y vulnerabilidades;
e) consecuencias de una violación de seguridad;
f) tecnología autorizada;
g) proceso de gestión del cambio.

Estos atributos se describen con más detalle en las siguientes subcláusulas.

6.5.4.2 Políticas de seguridad

Cada zona tiene un documento de control que describe los objetivos generales de seguridad y cómo garantizar que se cumpla el nivel de seguridad objetivo. Esto incluye lo siguiente:

a) el alcance de la zona;
b) el nivel de seguridad de la zona;
c) la estructura organizacional y las responsabilidades para hacer cumplir la política de seguridad;
d) los riesgos asociados con la zona;
e) la estrategia de seguridad para cumplir los objetivos requeridos;
f) las medidas de seguridad que se deben hacer cumplir;
g) los tipos de actividades que se permiten dentro de la zona;
h) los tipos de comunicación que permitieron acceso a la zona;
i) documentación de los atributos de la zona.

Todo lo anterior está documentado y combinado en la política de seguridad de la zona, que se utiliza para guiar y medir la construcción y el mantenimiento de los activos contenidos dentro de la zona.

6.5.4.3 Inventario de activos

Para mantener la seguridad dentro de una zona, una organización necesita mantener una lista de todos los activos (físicos y lógicos). Esta lista se utiliza para evaluar el riesgo y las vulnerabilidades y para determinar y mantener las medidas de seguridad apropiadas requeridas para cumplir con los objetivos de la política de seguridad. La precisión del inventario es un factor clave para cumplir los objetivos de seguridad establecidos en la política de seguridad. La lista debe actualizarse cuando cambian los activos dentro de la zona, o cambian sus conexiones electrónicas, así como cuando se agregan nuevos activos a la zona para garantizar que se cumplan los objetivos de seguridad.

Los activos y componentes físicos son los dispositivos físicos contenidos dentro de la zona. Algunos ejemplos incluyen los siguientes dispositivos:

a) hardware de la computadora (por ejemplo, estaciones de trabajo, servidores, instrumentos, controles, fuentes de alimentación, unidades de disco o copias de seguridad en cinta);
b) equipos de red (por ejemplo, enrutadores, conmutadores, concentradores, cortafuegos o cables físicos);
c) enlaces de comunicaciones (por ejemplo, buses, enlaces, módems y otras interfaces de red, antenas);
d) acceder a equipos de autenticación y autorización (por ejemplo, controladores de dominio, servidores de radio, lectores y escáneres);
e) hardware del sistema de desarrollo;
f) hardware de sistema de simulación y entrenamiento;
g) hardware externo del sistema;
h) inventarios de repuestos;
i) dispositivos de monitoreo y control (por ejemplo, sensores, interruptores y controladores);
j) manuales de referencia e información.

Los activos lógicos incluyen todo el software y los datos utilizados en la zona. Algunos ejemplos son los siguientes:

k) software de sistema informático (por ejemplo, aplicaciones, sistemas operativos, interfaces de comunicación, tablas de configuración, herramientas de desarrollo, herramientas de análisis y utilidades);
l) parches y actualizaciones para sistemas operativos y conjuntos de herramientas de aplicación;
m) bases de datos;
n) archivos de datos;
o) archivos de configuración de equipos;
p) copias de software y datos mantenidos con fines de respaldo y recuperación;
q) documentación básica de diseño (por ejemplo, requisitos funcionales que incluyen información y activos, clasificación de seguridad y niveles de protección, diseño físico y de software, evaluación de vulnerabilidad, perímetro de seguridad, pruebas de referencia, ensamblaje y documentos de instalación);
r) recursos del proveedor (por ejemplo, actualizaciones de productos, parches, paquetes de servicios, utilidades y pruebas de validación).

6.5.4.4 Requisitos y controles de acceso

Por su naturaleza, una zona implica que el acceso está limitado a un pequeño conjunto de todas las posibles entidades que podrían tener acceso. Una política de seguridad para una zona necesita articular el acceso requerido para que la zona cumpla con sus objetivos comerciales y cómo se controla este acceso

6.5.4.5 Evaluación de amenazas y vulnerabilidades

Existen amenazas y vulnerabilidades correspondientes dentro de una zona determinada. Las organizaciones necesitan identificar y evaluar estas amenazas y vulnerabilidades para determinar su riesgo de causar que los activos dentro de la zona no cumplan con sus objetivos comerciales. El proceso de documentar las amenazas y vulnerabilidades ocurre en la evaluación de amenazas y vulnerabilidades que forma parte de la política de seguridad de la zona.

Existen muchas posibles contramedidas para reducir el riesgo de una amenaza que explota una vulnerabilidad dada dentro de una zona. La política de seguridad debe describir qué tipos de contramedidas son apropiadas para cumplir con el nivel de seguridad objetivo para la zona, dentro de la compensación de costo versus riesgo.

6.5.4.6 Tecnología autorizada

A medida que los sistemas de automatización y control industrial evolucionan para satisfacer las cambiantes necesidades comerciales, la tecnología utilizada para implementar los cambios necesita ser controlada. Cada una de las tecnologías utilizadas en estos sistemas trae consigo un conjunto de vulnerabilidades y los riesgos correspondientes. Para minimizar los riesgos para una zona determinada, la política de seguridad de la zona debe tener una lista dinámica de tecnologías permitidas en la zona, así como aquellas no permitidas.

6.5.4.7 Proceso de gestión de cambios

Se requiere un proceso formal y preciso para mantener la precisión del inventario de activos de una zona determinada y cómo se realizan los cambios en la política de seguridad de la zona. Un proceso formal asegura que los cambios y adiciones a la zona no comprometan los objetivos de seguridad. Además, se requiere una forma de adaptarse a las cambiantes amenazas y objetivos de seguridad. Las amenazas y vulnerabilidades, con sus riesgos asociados, cambiarán con el tiempo.

6.5.5 Definición de conductos

Los conductos son zonas de seguridad que se aplican a procesos específicos de comunicaciones. Como zonas de seguridad, son una agrupación lógica de activos (activos de comunicación en este caso). Un conducto de seguridad protege la seguridad de los canales que contiene de la misma manera que el conducto físico protege los cables del daño físico. Los conductos pueden considerarse tuberías que conectan zonas o que se utilizan para la comunicación dentro de una zona. Los conductos internos (dentro de la zona) y externos (fuera de la zona) encierran o protegen los canales de comunicación (conceptualmente cables) que proporcionan los enlaces entre los activos. Muy a menudo, en un entorno IACS, el conducto es el mismo que la red. Es decir, el conducto es el cableado, enrutadores, conmutadores y dispositivos de gestión de red que conforman las comunicaciones en estudio. Los conductos pueden ser agrupaciones de tecnologías de red diferentes, así como los canales de comunicación que pueden ocurrir dentro de una sola computadora. Los conductos se utilizan para analizar las amenazas y vulnerabilidades de comunicación que pueden existir en las comunicaciones dentro y entre zonas.

Los conductos pueden considerarse tuberías que contienen datos y / o proporcionan conexiones físicas para la comunicación entre zonas. Un conducto puede tener subconductos para proporcionar una comunicación de zona uno a uno o uno a muchos. Se puede lograr una comunicación segura para el conducto mediante la implementación de la política de seguridad de zona apropiada.

6.5.6 Características del conducto

6.5.6.1 Descripción general

Físicamente, un conducto puede ser un cable que conecta zonas para fines de comunicación. Un conducto es un tipo de zona que no puede tener subzonas; es decir, un conducto no está

compuesto de subconductos. Los conductos están definidos por la lista de todas las zonas que comparten los canales de comunicación dados. Tanto los dispositivos físicos como las aplicaciones que usan los canales contenidos en un conducto definen los puntos finales del conducto. El conducto de la empresa se destaca en la Figura 21.

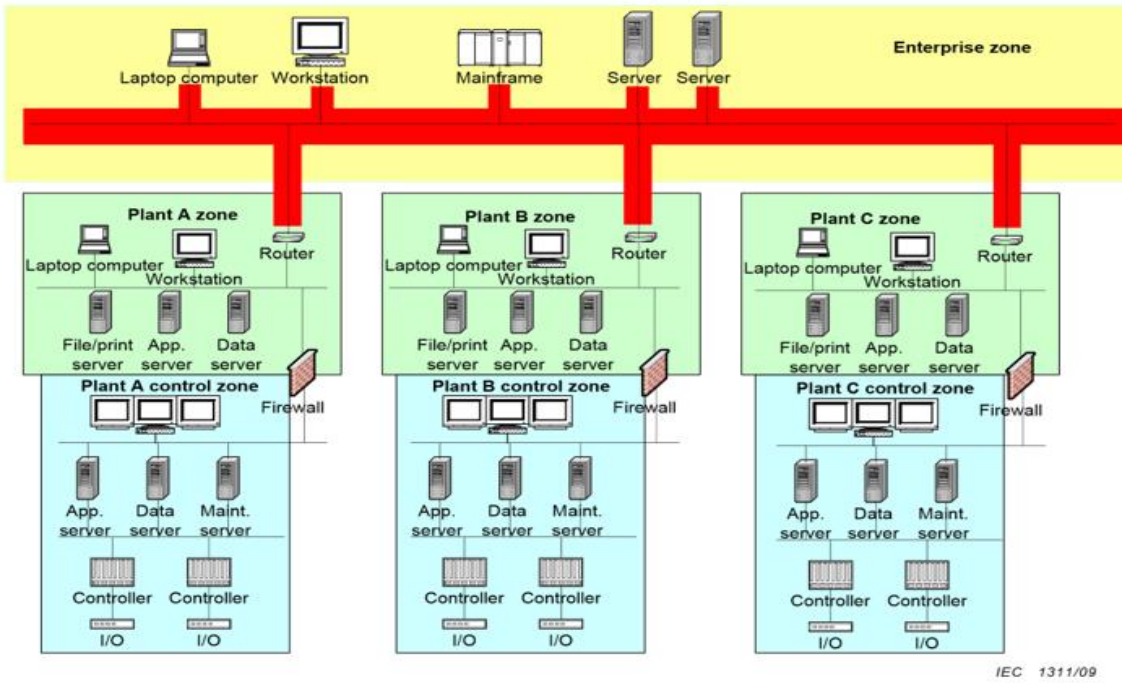

Figura 21 - Conducto empresarial

Al igual que con las zonas, se puede construir una vista similar para usar en aplicaciones SCADA. Un ejemplo se muestra en la Figura 22.

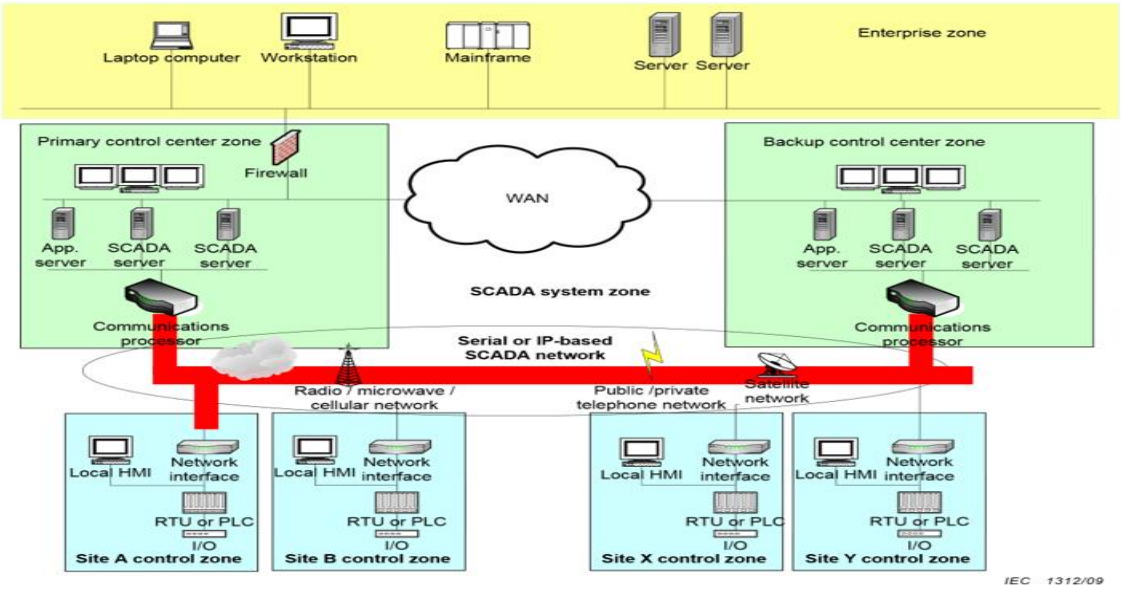

Figura 22 - Ejemplo de conducto SCADA

Al igual que una zona, cada conducto tiene un conjunto de características y requisitos de seguridad que son sus atributos. Estos toman la forma de los siguientes atributos:

a) políticas de seguridad;
b) inventario de activos;
c) requisitos de acceso y controles;
d) amenazas y vulnerabilidades;
e) consecuencias de una violación de seguridad;
f) tecnologías autorizadas;
g) proceso de gestión del cambio;
h) zonas conectadas.

6.5.6.2 Políticas de seguridad

Cada conducto tiene un documento de control que describe los objetivos generales de seguridad y cómo garantizar que se cumpla el nivel de seguridad objetivo. Este documento incluye lo siguiente:

a) el alcance del conducto;
b) el nivel de seguridad del conducto;
c) la estructura organizacional y las responsabilidades para hacer cumplir la política de seguridad del conducto;
d) los riesgos asociados con el conducto;
e) la estrategia de seguridad para cumplir los objetivos requeridos;
f) las medidas de seguridad que se deben hacer cumplir;
g) los tipos de canales que están permitidos dentro del conducto;
h) documentación de los atributos del conducto.

Todo lo anterior está documentado y combinado en la política de seguridad del conducto, que se utiliza para guiar y medir la construcción y el mantenimiento de los activos contenidos dentro del conducto.

6.5.6.3 Inventario de activos

Al igual que con el inventario de zona, se requiere una lista precisa de los activos de comunicaciones.

6.5.6.4 Requisitos y controles de acceso

Por su naturaleza, un conducto implica que el acceso está restringido a un conjunto limitado de todas las entidades posibles que podrían tener acceso. Una política de seguridad para un conducto debe articular el acceso requerido para que el conducto cumpla con sus objetivos comerciales y cómo se controla este acceso.

6.5.6.5 Evaluación de amenazas y vulnerabilidades

Existen amenazas y vulnerabilidades correspondientes para un conducto dado. Las organizaciones deben identificar y evaluar estas amenazas y vulnerabilidades para determinar su riesgo de causar que los activos dentro del conducto no cumplan con sus objetivos comerciales. El proceso de

documentar las amenazas y vulnerabilidades ocurre en la valuación de amenazas y vulnerabilidades que forma parte de la política de seguridad de los conductos.
Existen muchas posibles contramedidas para reducir el riesgo de una amenaza que explota una vulnerabilidad dada dentro de un conducto. La política de seguridad debe describir qué tipos de contramedidas son apropiadas dentro de la compensación de costo versus riesgo.

6.5.6.6 Tecnología autorizada

A medida que los Sistemas de Control y Automatización Industrial evolucionan para satisfacer las cambiantes necesidades comerciales, la tecnología utilizada para implementar los cambios necesita ser controlada. Cada una de las tecnologías utilizadas en estos sistemas trae consigo un conjunto de vulnerabilidades y los riesgos correspondientes. Para minimizar los riesgos para un conducto dado, la política de seguridad del conducto debe tener una lista dinámica de tecnologías permitidas en el conducto.

6.5.6.7 Proceso de gestión de cambios

Se requiere un proceso formal y preciso para mantener la precisión de la política de un conducto determinado y cómo se realizan los cambios. Un proceso formal asegura que los cambios y adiciones al conducto no comprometan los objetivos de seguridad. Además, se requiere una forma de adaptarse a las cambiantes amenazas y objetivos de seguridad. Las amenazas y vulnerabilidades, con sus riesgos asociados, cambiarán con el tiempo.

6.5.6.8 Zonas conectadas

Un conducto también puede describirse en términos de las zonas a las que está conectado.

6.6 Relaciones modelo

Los modelos descritos en las páginas anteriores están relacionados entre sí y con las políticas, procedimientos y pautas que conforman un programa de seguridad. Estas relaciones se muestran en la Figura 23.

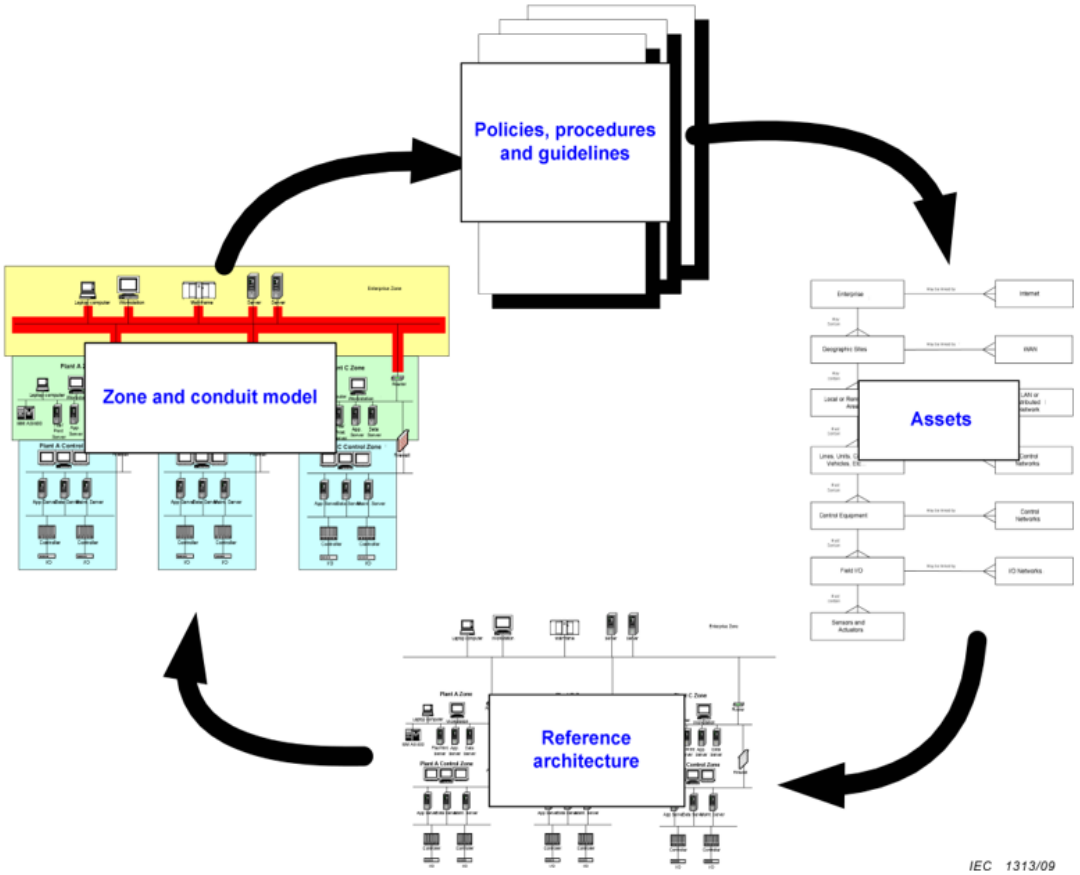

Figura 23 - Relaciones modelo

En IEC 62443-2-15 se aborda información más detallada sobre el proceso para desarrollar dicho programa.

Bibliografía

The following documents contain material referenced in this technical specification:

[1] IEC 60050, *International Electrotechnical Vocabulary*, available at <http://www.electropedia.org>

[2] IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 4: Definitions and abbreviations*

[3] IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

[4] IEC 61511-3, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

[5] IEC 61512-1, *Batch control – Part 1: Models and terminology*

[6] IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

[7] IEC 62264-3, *Enterprise-control system integration – Part 3: Activity models of manufacturing operations management*

[8] IEC 62443-2-1, *Industrial communication networks – Network and system security –Part 2-1: Establishing an industrial automation and control system security program6*

[9] *IEC Glossary,* available at <http://std.iec.ch/glossary>

[10] ISO 7498-2: *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

[11] RFC 2828, *Internet Security Glossary,* available at <http://www.faqs.org/rfcs/rfc2828.html>

[12] FIPS PUB 140-2, *Security requirements for cryptographic modules,* available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

[13] CNSS Instruction No. 4009, *National Information Assurance Glossary* (AI), available at <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>

[14] NASA/Science Office of Standards and Technology (NOST), *ISO Archiving Standards – Fourth US Workshop – Reference Model Definitions*, available at <http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html>

[15] SANS, *Glossary of Terms used in Security and Intrusion Detection*, available at <http://www.sans.org/resources/glossary.php>