IEC 62443-2-1

Edición 1.0 2010-11

NORMA
INTERNACIONAL

Redes de comunicación industrial. Seguridad de redes y sistemas. Parte 2-1: Establecimiento de un programa de seguridad del sistema de automatización y control industrial.

COMISIÓN
ELECTROTÉCNICA
INTERNACIONAL

CÓDIGO DE PRECIO

ICS 25.040.40; 33.040 ISBN 978-2-88912-206-6

CONTENIDO

COMISIÓN ELECTROTÉCNICA INTERNACIONAL

_____

REDES DE COMUNICACIÓN INDUSTRIAL - RED Y SEGURIDAD DEL SISTEMA - Parte 2-1: Establecimiento de un programa de seguridad del sistema de automatización y control industrial.

PREFACIO

1) La Comisión Electrotécnica Internacional (IEC) es una organización mundial de normalización que comprende todos los comités electrotécnicos nacionales (Comités Nacionales IEC). El objetivo de IEC es promover la cooperación internacional en todas las cuestiones relacionadas con la estandarización en los campos eléctrico y electrónico. Con este fin y además de otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, Especificaciones Públicas (PAS) y Guías (en adelante, "Publicaciones de IEC"). Su preparación se confía a los comités técnicos; cualquier comité nacional de IEC interesado en el tema tratado puede 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 consenso internacional de opinión sobre los temas relevantes ya que cada comité técnico tiene representación de todos los Comités Nacionales de IEC interesados.
3) Las publicaciones IEC tienen la forma de recomendaciones para uso internacional y son aceptadas por los Comités Nacionales IEC en ese sentido. Si bien se hacen todos los esfuerzos razonables para garantizar que el contenido técnico de las Publicaciones de IEC sea exacto, 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 correspondiente publicación nacional o regional se indicará claramente en esta última.
5) IEC en sí mismo no proporciona ningún certificado de conformidad. Los organismos de certificación independientes proporcionan servicios de evaluación de la conformidad y, en algunas áreas, acceso a las marcas de conformidad IEC. IEC no es responsable de ningún servicio realizado por organismos de certificación independientes.
6) Todos los usuarios deben asegurarse de tener la última edición de esta publicación.
7) No se impondrá responsabilidad a IEC o sus directores, empleados, servidores o agentes, incluidos expertos individuales y miembros de sus comités técnicos y Comités Nacionales de IEC por daños personales, daños a la propiedad u otros daños de cualquier naturaleza, ya sea directa o indirecta, o para los costos (incluidos los honorarios legales) y los gastos que surjan de la publicación, el uso o la dependencia de esta publicación de IEC o de cualquier otra publicación de IEC.
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 estar sujetos a derechos de patente. IEC no será responsable de identificar ninguno o todos los derechos de patente.

La Norma Internacional IEC 62443-2-1 ha sido preparada por el comité técnico 65 de IEC: Medición, control y automatización de procesos industriales.

El texto de esta norma se basa en los siguientes documentos:

FDIS	Informe sobre votación.
65/457 / FDIS	65/461 / RVD

La información completa sobre la votación para la aprobación de esta norma 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.

Se puede encontrar una lista de todas las partes existentes de la serie IEC 62443, publicada bajo el título general Redes de comunicación industrial: seguridad de redes y sistemas, en el sitio web de IEC.
La lista completa de partes existentes y previstas también se puede encontrar en la Bibliografía de esta norma. El comité decidió que el contenido de esta publicación permanecerá sin cambios hasta la fecha de estabilidad indicada en el sitio web de IEC bajo "http://webstore.iec.ch" en los datos relacionados con la publicación específica. En esta fecha, la publicación será:

· Reconfirmado,
· Retirado,
· Reemplazado por una edición revisada, o
· Modificado.

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

NOTA La revisión de esta norma internacional se iniciará poco después de la publicación de esta norma. La próxima revisión se alineará más estrechamente con ISO / IEC 27001, que aborda muchos de los mismos problemas, pero sin tener en cuenta los requisitos especializados para la operación continua y la seguridad que son comunes en el entorno de los sistemas de automatización y control industrial.

IMPORTANTE: el logotipo de "colour inside (color dentro)" en la portada de esta publicación indica que contiene colores que se consideran útiles para la correcta comprensión de su contenido. Por lo tanto, los usuarios deben imprimir este documento con una impresora a color.

0 INTRODUCCIÓN.

0.1 Descripción general.

La seguridad cibernética es un tema cada vez más importante en las organizaciones modernas. Muchas organizaciones involucradas en la tecnología de la información (TI) y las empresas se han preocupado por la seguridad cibernética durante muchos años y cuentan con sistemas de gestión de seguridad cibernética (CSMS) bien establecidos, tal como lo definen la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional. (IEC) (ver ISO / IEC 17799 [23] 1 e ISO / IEC 27001 [24]). Estos sistemas de gestión proporcionan a la organización un método bien establecido para proteger sus activos de ataques cibernéticos.

Las organizaciones de sistemas de automatización y control industrial (IACS) han comenzado a utilizar tecnología comercial normalizada desarrollada para sistemas comerciales en sus procesos cotidianos, lo que ha brindado una mayor oportunidad de ataque cibernético contra el equipo IACS. Estos sistemas no suelen ser tan robustos, en el entorno de IACS, por muchas razones, como los sistemas IACS diseñados específicamente para hacer frente al ciberataque. Esta debilidad puede tener consecuencias para la salud, la seguridad y el medio ambiente (HSE).

Las organizaciones pueden intentar usar las soluciones de seguridad cibernética de TI y empresariales preexistentes para abordar la seguridad de IACS sin comprender las consecuencias. Si bien muchas de estas soluciones se pueden aplicar a IACS, deben aplicarse de la manera correcta para eliminar las consecuencias involuntarias.

0.2 Sistema de gestión de seguridad cibernética para IACS.

Los sistemas de gestión típicos suelen proporcionar orientación sobre lo que debe incluirse en un sistema de gestión, pero no proporcionan orientación sobre cómo desarrollarlo. Esta norma aborda los aspectos de los elementos incluidos en un CSMS para IACS y también proporciona orientación sobre cómo desarrollar el CSMS para IACS.

Un enfoque de ingeniería muy común cuando se enfrenta a un problema desafiante es dividir el problema en partes más pequeñas y abordar cada pieza de manera disciplinada. Este enfoque es sólido para abordar los riesgos de seguridad cibernética con IACS. Sin embargo, un error frecuente al abordar la seguridad cibernética es tratar con la seguridad cibernética un sistema a la vez. La seguridad cibernética es un desafío mucho mayor que debe abordar el conjunto completo de IACS, así como las políticas, procedimientos, prácticas y personal que rodean y utilizan esos IACS. La implementación de un sistema de gestión tan amplio puede requerir un cambio cultural dentro de la organización.

Abordar la seguridad cibernética en toda la organización puede parecer una tarea desalentadora. Desafortunadamente no hay un libro con una receta simple para la seguridad. Hay una buena razón para esto. No existe un conjunto único de prácticas de seguridad para todos. Puede lograrse una seguridad absoluta, pero probablemente sea indeseable debido a la pérdida de funcionalidad que sería necesaria para lograr este estado casi perfecto. La seguridad es realmente un equilibrio de riesgo versus costo. Todas las situaciones serán diferentes. En algunas situaciones, el riesgo puede estar relacionado con factores de HSE más que con un impacto puramente económico. El riesgo puede tener una consecuencia irrecuperable en lugar de un revés financiero temporal. Por lo tanto, un conjunto de libros de recetas de prácticas de seguridad obligatorias será demasiado restrictivo y probablemente bastante costoso de seguir, o será insuficiente para abordar el riesgo.

0.3 Relación entre esta norma, ISO / IEC 17799 e ISO / IEC 27001.

ISO / IEC 17799 [23] e ISO / IEC 27001 [24] son normas excelentes que describen un sistema de gestión de seguridad cibernética para sistemas de tecnología de información / negocios. Gran parte del contenido de estas normas también es aplicable a IACS. Esta norma enfatiza la necesidad de coherencia entre las prácticas para administrar la seguridad cibernética de IACS con las prácticas para administrar la seguridad cibernética de los sistemas empresariales / de tecnología de la información. Las economías se realizarán haciendo que estos programas sean consistentes. Se recomienda a los usuarios de esta norma que lean ISO / IEC 17799 e ISO / IEC 27001 para obtener información de soporte adicional. Esta norma se basa en la guía de estas normas ISO / IEC. Aborda algunas de las diferencias importantes entre IACS y los sistemas generales de negocios / tecnología de la información. Introduce el importante concepto de que los riesgos de seguridad cibernética con IACS pueden tener implicaciones de HSE y deben integrarse con otras prácticas de gestión de riesgos existentes que aborden estos riesgos.

COMISIÓN ELECTROTÉCNICA INTERNACIONAL

REDES DE COMUNICACIÓN INDUSTRIAL -
RED Y SEGURIDAD DEL SISTEMA -
Parte 2-1: Establecimiento de un programa de seguridad del sistema de automatización y control industrial.

1. Alcance.

Esta parte de IEC 62443 define los elementos necesarios para establecer un sistema de gestión de seguridad cibernética (CSMS) para sistemas de control y automatización industrial (IACS) y proporciona orientación sobre cómo desarrollar esos elementos. Esta norma utiliza la definición amplia y el alcance de lo que constituye un IACS descrito en IEC / TS 62443-1-1.

Los elementos de un CSMS descritos en esta norma son en su mayoría relacionados con políticas, procedimientos, prácticas y personal, y describen lo que debe o debe incluirse en el CSMS final para la organización.

NOTA 1. Otros documentos en la serie IEC 62443 y en la Bibliografía discuten tecnologías y / o soluciones específicas para la seguridad cibernética con más detalle.

La orientación proporciona un ejemplo sobre cómo desarrollar un CSMS. Se representa la opinión del autor sobre cómo una organización podría desarrollar todos los elementos y no ser funciona en todas las situaciones. Los usuarios de esta norma tendrán que leer los requisitos cuidadosamente y aplicar la guía de manera apropiada para desarrollar un CSMS completamente funcional para una organización. Las políticas y procedimientos discutidos en esta norma deben adaptarse para ajustarse a la organización.

NOTA 2. Puede haber casos en los que exista un CSMS preexistente y se agregue la parte de IACS o puede haber algunas organizaciones que nunca hayan creado formalmente un CSMS. Los autores de esta norma no pueden anticipar todos los casos en que una organización establecerá un CSMS para el entorno IACS, por lo que esta norma no intenta crear una solución para todos los casos.

2 Referencias normativas.

Los siguientes documentos referenciados son indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

IEC / TS 62443-1-12 - Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 1-1: Terminología, conceptos y modelos

3 Términos, definiciones, términos abreviados, acrónimos y convenciones.

3.1 Términos y definiciones.

Para los propósitos de este documento, se aplican los términos y definiciones dados en IEC / TS 62443-1-1 y los siguientes.

2 Esta norma se deriva de ANSI / ISA 99.02.01: 2009 y lo reemplaza completamente para uso internacional. Se pretende que la segunda edición de IEC / TS 62443-1-1 sea una norma internacional, no una TS, después de la inclusión de algunos requisitos normativos con los que es posible la conformidad.

3.1.1
acceder a la cuenta.
función de control de acceso que permite al usuario acceder a un conjunto particular de datos o funciones para ciertos equipos.
NOTA. Muchas veces las cuentas están vinculadas a identificaciones de usuario (ID) y contraseñas. Estas identificaciones de usuario y contraseñas pueden estar vinculadas a un individuo o grupo de individuos, como un equipo de trabajo de la sala de control que realiza el mismo conjunto de tareas operativas.

3.1.2
prácticas administrativas.
prácticas / procedimientos definidos y documentados que las personas son personalmente responsables de seguir en todo momento.
NOTA: Por lo general, se encuentran en condiciones de empleo para la organización. En el entorno de IACS, a menudo tienen implicaciones de HSE.

3.1.3
activo.
Objeto físico o lógico propiedad de o bajo los deberes de custodia de una organización, que tiene un valor percibido o real para la organización.
[IEC / TS 62443-1-1, 3.2.6]
NOTA En este caso específico, un activo es cualquier elemento que debe protegerse como parte del CSMS.

3.1.4
autenticación.
medida de seguridad diseñada para establecer la validez de una transmisión, un mensaje o iniciador o un medio de verificar la autorización de un individuo para recibir determinadas categorías de información.
[IEC / TS 62443-1-1, 3.2.13]

3.1.5
sistema de gestión de quemadores.
sistema para el arranque, monitoreo y apagado seguro de los sistemas de quemadores asociados con calderas, antorchas, incineradores, turbinas de gas, oxidantes térmicos y otros equipos a fuego.

3.1.6
plan de negocios continuo.

documento con procedimientos identificados para recuperarse de una interrupción significativa y restaurar las operaciones comerciales.
NOTA 1 Este término general también se refiere a otros aspectos de la recuperación ante desastres, como la gestión de emergencias, los recursos humanos y los medios de comunicación o las relaciones con la prensa.
NOTA 2 Un plan de continuidad comercial también identifica procedimientos para mantener operaciones comerciales esenciales mientras se recupera de una interrupción significativa.

3.1.7
Planificación de la Continuidad del Negocio.
proceso para desarrollar un plan de continuidad comercial.

3.1.8
gestión del cambio.
proceso de controlar y documentar cualquier cambio en un sistema para mantener el funcionamiento adecuado del equipo bajo control.

3.1.9
conformidad.
adherencia a los requisitos en una norma por otra.
Adaptado de [ISO / IEC 10746-2, 15.1]
NOTA Esta es una relación entre dos especificaciones, A y B, que se cumple cuando la especificación A establece los requisitos que todos cumplen la especificación B (cuando B cumple con A).

3.1.10
conformidad.
relación entre una implementación y una norma donde cualquier proposición que sea verdadera en la norma debe ser verdadera en su implementación Adaptado de [ISO / IEC 10746-2, 15.1].
NOTA La relación de conformidad se mantiene cuando la implementación cumple los requisitos específicos de la especificación (los requisitos de conformidad). La evaluación de conformidad es el proceso a través del cual se determina esta relación.

3.1.11

consecuencia.

resultado de que se produce a partir de un incidente particular.

3.1.12

crítico.

dispositivo muy importante, sistema informático, proceso y similares que, si se ven comprometidos por un incidente, podrían tener un alto impacto financiero, de salud, seguridad o medioambiental (HSE) para una organización.

3.1.13

sistema de gestión de seguridad cibernética.

programa diseñado por una organización para mantener la seguridad cibernética de los activos de toda la organización a un nivel establecido de confidencialidad, integridad y disponibilidad, ya sea en el lado comercial o en el lado IACS de la organización.

3.1.14

requisitos del dispositivo.

características de contramedida necesarias para que los dispositivos dentro de una zona alcancen el nivel de seguridad objetivo deseado.

3.1.15

Especialista en información.

individuo de confianza que los gerentes superiores consultan para abordar y priorizar los problemas en que están más capacitados.

3.1.16
Salud, Seguridad y Entorno.
responsabilidad de proteger la salud y la seguridad de los trabajadores y la comunidad circundante y mantener una alta gestión ambiental.

3.1.17
Interfaz hombre-máquina.
conjunto de medios por los cuales las personas (los usuarios) interactúan con una máquina, dispositivo, programa de computadora u otra herramienta compleja (el sistema) en particular.
NOTA En muchos casos, estos incluyen pantallas de video o terminales de computadora, botones, retroalimentación auditiva, luces intermitentes y similares. La interfaz hombre-máquina proporciona medios para:

·Entrada, permitiendo a los usuarios controlar la máquina;

·Salida, permitiendo que la máquina informe a los usuarios.

3.1.18
incidente.
evento que no es parte de la operación esperada de un sistema o servicio que causa o puede causar, una interrupción o una reducción en la calidad del servicio provisto por el sistema.
3.1.19

auditoría independiente.
revisión de una organización (políticas, procedimientos, procesos, equipos, personal y similares) por un grupo externo no afiliado a la organización.
NOTA Esto puede ser requerido para las empresas públicas.

3.1.20
tecnologías de la información.
activos informáticos de una organización que representan activos no físicos, como aplicaciones de software, programas de proceso y archivos de personal.
NOTA 1 Este uso del término tecnología de la información no se abrevia en este documento.

NOTA 2 Otro uso del término tecnología de la información (TI) se refiere a la organización interna de la empresa (por ejemplo, el departamento de TI) o los elementos mantenidos tradicionalmente por este departamento (es decir, las computadoras administrativas, los servidores y la infraestructura de red). Este uso del término tecnología de la información se abrevia como TI en esta norma.

3.1.21
sistema heredado.
sistema de control y automatización industrial existente en una instalación que puede no estar disponible como artículo comercial.

NOTA Un sistema puede haber sido heredado con artículos comerciales a la vez, pero puede que ya no esté disponible y / o no sea compatible.

3.1.22
probabilidad.
estimación cuantitativa de que puede ocurrir una acción, evento o incidente.

3.1.23
usuario local.
usuario que se encuentra dentro del perímetro de la zona de seguridad a la que se dirige.
NOTA Una persona en el área de fabricación inmediata o en la sala de control es un ejemplo de usuario local.

3.1.24
sistema de ejecución de la fabricación.
El sistema de programación y seguimiento de producción se utiliza para analizar e informar la disponibilidad y el estado de los recursos, programar y actualizar pedidos, recopilar datos de ejecución detallados, como el uso de materiales, el uso de mano de obra, los parámetros operativos, el estado de los pedidos y equipos y

otra información crítica.
NOTA 1 Este sistema accede a listas de materiales, rutas y otros datos desde el sistema base de planificación de recursos empresariales y, por lo general, se usa para informes y monitoreo en planta en tiempo real que retroalimenta los datos de actividad al sistema base.
NOTA 2 Consulte IEC 62264-1 para obtener información adicional.

3.1.25.
MAC
dirección de hardware que diferencia un dispositivo en una red de otro.

3.1.26
operador
tipo particular de usuario que generalmente es responsable del correcto funcionamiento del equipo bajo control.

3.1.27
gestión de parches.
área de administración de sistemas que implica adquirir, probar e instalar múltiples parches (cambios de código) en un sistema informático administrado.
NOTA Las tareas de administración de parches incluyen: mantener el conocimiento actual de los parches disponibles, decidir qué parches son apropiados para sistemas particulares, garantizar que los parches se instalen correctamente, probar los sistemas después de la instalación y documentar todos los procedimientos asociados, como configuraciones específicas requeridas de forma remota en entornos heterogéneos de acuerdo reconocidas mejores prácticas.

3.1.28
ingeniero de procesos.
Persona típicamente responsable de los aspectos técnicos de la operación industrial y que utiliza el IACS y otras herramientas para supervisar y gestionar la automatización industrial en las instalaciones.

3.1.29
sistema de gestión de información de procesos.
Conjunto de sistemas que proporciona información de apoyo para ayudar con la operación de la instalación.

3.1.30
controlador lógico programable.
Dispositivo programable basado en microprocesador que se utiliza en la industria para controlar líneas de ensamblaje y maquinaria en el taller, así como muchos otros tipos de equipos mecánicos, eléctricos y electrónicos en una planta.
NOTA Típicamente programada como en [14], un PLC está diseñado para uso en tiempo real en entornos industriales difíciles. Conectados a sensores y actuadores, los PLC se clasifican por el número y tipo de puertos de E / S que proporcionan y por su velocidad de exploración de E / S.

3.1.31
Gestión de la seguridad de procesos.
Regulación destinada a prevenir un desastre en los sistemas químicos y biotecnológicos abordando la gestión racional y el diseño de ingeniería.

3.1.32
acceso remoto.
comunicación o uso de activos o sistemas dentro de un perímetro definido desde cualquier ubicación fuera de ese perímetro.

3.1.33
usuario remoto.
usuario que se encuentra fuera del perímetro de la zona de seguridad a la que se dirige
EJEMPLO Una persona en una oficina en el mismo edificio, una persona que se conecta a través de la red de área amplia corporativa (WAN) y una persona que se conecta a través de redes de infraestructura pública son todos usuarios remotos.

3.1.34
Evaluación de riesgos.
proceso de identificación y evaluación de riesgos para las operaciones de la organización (incluida la misión, funciones, imagen o reputación), los activos o individuos de la organización mediante la determinación de la probabilidad de ocurrencia, el impacto resultante y las contramedidas adicionales que mitigarían este impacto.

NOTA Sinónimo de análisis de riesgos e incorpora análisis de amenazas y vulnerabilidades.

3.1.35
mitigación de riesgos.
acciones para reducir la probabilidad y / o gravedad de un evento

3.1.36
tolerancia al riesgo.
riesgo que la organización está dispuesta a aceptar.

3.1.37
autoevaluación.
revisión de una organización (es decir, políticas, procedimientos, operaciones, equipos y personal) por un grupo dentro de la organización.
NOTA Este grupo puede estar directamente asociado con el proceso comercial de la organización o puede estar en otra parte de la organización, pero debe estar íntimamente familiarizado con los riesgos asociados con ese proceso comercial.

3.1.38
Six Sigma®.
Metodología centrada en procesos diseñada para mejorar el rendimiento del negocio mediante la mejora de áreas específicas de los procesos estratégicos del negocio.

3.1.39
ingeniería social.
práctica de obtener información confidencial mediante la manipulación de usuarios legítimos.

3.1.40
parte interesada.
Individuo o grupo interesado en el éxito de una organización para entregar los resultados esperados y mantener la viabilidad de los productos y servicios de la organización.
NOTA Las partes interesadas influyen en los programas, productos y servicios. En este caso particular, las partes interesadas son personal de una organización responsable de promover y supervisar el proceso de seguridad cibernética. Este personal incluye al gerente del programa de seguridad cibernética, así como al equipo multifuncional de personas de todos los departamentos afectados por el programa de seguridad cibernética.

3.1.41
administrador del sistema.
Persona (s) responsable (s) de administrar la seguridad del sistema informático.
NOTA Esto puede incluir el mantenimiento del sistema operativo, la administración de la red, la administración de cuentas y la administración de parches, de acuerdo con el proceso de administración de cambios.

3.1.42
requisitos del sistema.
atributos del nivel de seguridad objetivo deseado.

3.1.43
seguimiento de acceso marcado.
procedimiento para monitorear las acciones de un usuario conectado remotamente.

3.1.44
evaluación de vulnerabilidad.
Descripción formal y evaluación de las vulnerabilidades en un sistema.

3.2 Términos y acrónimos abreviados.

Esta subcláusula define los términos y acrónimos abreviados utilizados en este documento.

ANSI.	Instituto Americano de Normas Nacionales.
CFR.	Código de Regulaciones Federales de EE. UU.
ChemITC.	Tecnología de la información química. Centro del Consejo Americano de Química.
CPU.	Unidad Central de procesamiento.
CSCSP.	Programa de Seguridad Cibernética del Sector Químico.
CSMS	Sistema de gestión de ciberseguridad.
DCS.	Sistema de control distribuido.
DMZ.	Zona desmilitarizada.
DoS, DDoS.	Denegación de servicio, Denegación de servicio distribuida.
FDN.	Red de dispositivos de campo.
FTP.	Protocolo de transferencia de archivos.
HMI.	Interfaz hombre-máquina.
HSE.	Salud, seguridad y medio ambiente.
HVAC.	Calefacción, ventilación y aire acondicionado.
SCAI	Sistemas de control y Automatización industrial.
ID.	Identificación.
IEC.	Comisión Electrotécnica Internacional.
IEEE.	Instituto de Ingenieros Eléctricos y Electrónicos.
IP.	Protocolo de Internet.
ISA .	Sociedad Internacional de Automatización.
ISO.	Organización Internacional de Normalización.
TI	Tecnologías de la información.
KPI .	Indicadores clave de rendimiento.
LAN.	Red de área local.
MAC.	Control de acceso a medios.
MES.	Sistema de ejecución de fabricación.

NERC.	Consejo de Fiabilidad Eléctrica de América del Norte (se aplica a EE. UU. Y Canadá).
NIST.	Instituto Nacional de Normas y Tecnología de EE. UU.
SO	Sistema operativo.
PC.	Computadora personal.
PCN.	Red de control de procesos.
PIM.	Gestión de la información del proceso.
PIN.	Número de identificación personal.
PLC.	Controlador lógico programable.
GSP	Gestión de la seguridad de procesos.
RAID.	Matriz redundante de discos independientes.
RCN.	Red de control reguladora
SANS.	Instituto de Sistemas, Auditoría, Redes y Seguridad.
SCADA.	Control, supervisión y Adquisición de Datos.
SI.	Sistema Internacional de Unidades.
SIS.	Sistemas instrumentados de seguridad.
SoA.	Declaración de aplicabilidad.
SOC.	Condición de funcionamiento normalizado.
SOP.	Procedimiento Operativo Normalizado.
SP.	Publicación especial (por NIST) SSL Secure socket layer.
TCP.	Protocolo de Control de Transmisión.
TR.	Reporte técnico.
VLAN.	Red de área local virtual.
VPN.	Red privada virtual WAN Red de área amplia.

3.3 Convenios.

Los elementos de un CSMS (Sistema de gestión de ciberseguridad) son los siguientes:

· El objetivo del elemento,
· Una descripción básica del elemento,
· Una justificación para explicar por qué se incluye el elemento y
· los requisitos para ese elemento.

Se utiliza una presentación tabular para proporcionar una descripción y requisitos para cada elemento. Los requisitos están numerados de forma similar a las subcláusulas (pero no son en sí, las mismas subcláusulas), de modo que los requisitos pueden ser referenciados individual y selectivamente.

4 Elementos de un sistema de gestión de seguridad cibernética.

4.1 Descripción general.

Esta cláusula presenta los elementos que constituyen un CSMS para IACS. Estos elementos representan lo que debe incluirse en el CSMS para proteger a IACS contra ataques cibernéticos.
Los elementos se presentan en las siguientes tres categorías principales:
· Análisis de riesgo,

· Abordar el riesgo con el CSMS, y
· Seguimiento y mejora del CSMS.

Cada una de estas categorías se divide en grupos de elementos y / o elementos. La Figura 1 muestra la relación entre las categorías, grupos de elementos y elementos.

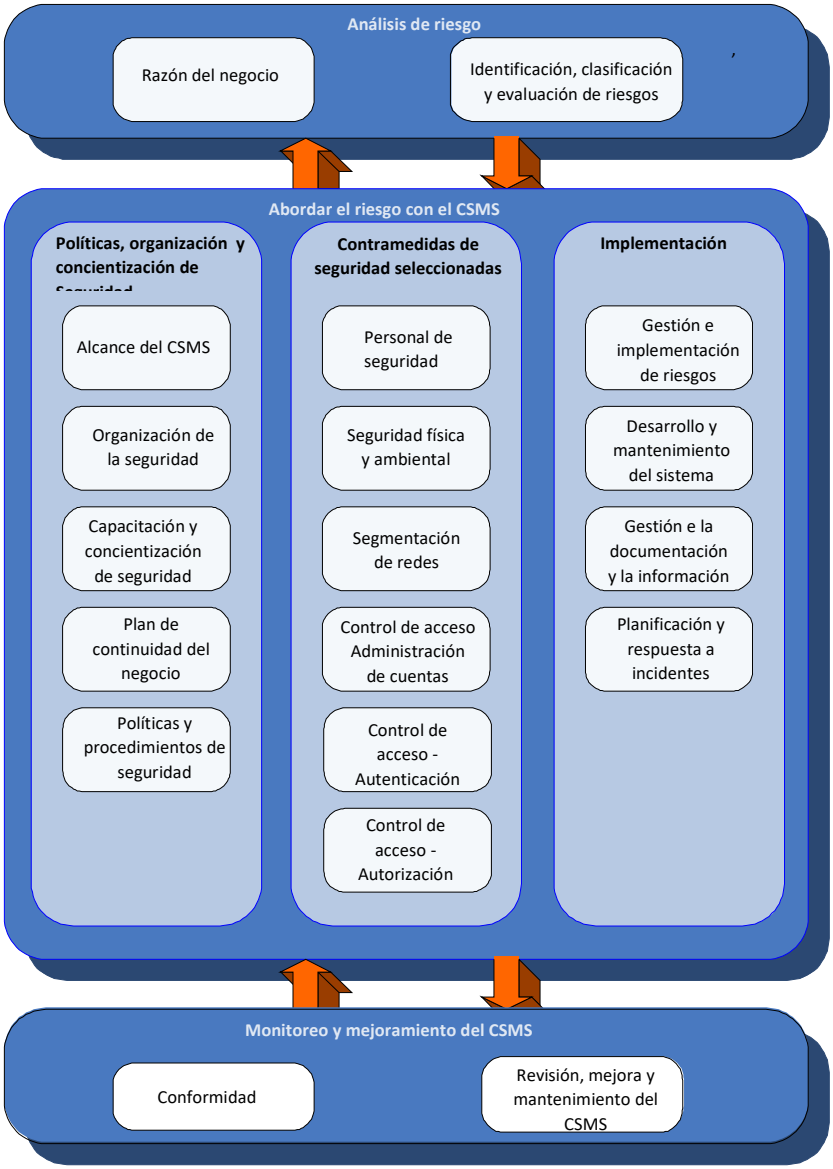

Figura 1 - Vista gráfica de elementos de un sistema de gestión de seguridad cibernética.

En esta cláusula se enumera el objetivo y se realiza una descripción básica de cada elemento, con una justificación para explicar por qué se incluye el elemento y los requisitos del mismo.

El Anexo A sigue la misma estructura básica de esta cláusula con categorías, grupos de elementos y elementos. Sin embargo, el anexo proporciona orientación sobre cómo desarrollar los elementos del CSMS.

El lector debe leer el Anexo A para comprender las necesidades especiales y los problemas relacionados con el desarrollo de un CSMS para IACS. La orientación discutida en el Anexo A debe adaptarse a los requisitos especiales de cada organización.

Esta norma especifica los elementos necesarios para un CSMS. La intención de la norma no es especificar un proceso secuencial particular para identificar y abordar el riesgo que incorpora estos elementos. Por lo tanto, una organización creará dicho proceso de acuerdo con su cultura, organización y el estado actual de sus actividades de seguridad cibernética. Para ayudar a las organizaciones con este aspecto de la aplicación de la norma, A.3.4.2 proporciona un ejemplo de un proceso para identificar y abordar el riesgo. Además, el Anexo B ofrece información sobre pedidos efectivos para actividades relacionadas con todos los elementos discutidos en esta norma.

Si bien un CSMS es una excelente herramienta para gestionar el riesgo dentro de una gran empresa, también es aplicable a las pequeñas empresas. El CSMS puede estar más formalizado en una gran empresa, por lo que puede utilizarse en muchas situaciones y geografías diferentes. En una empresa pequeña, se deben realizar actividades similares de CSMS, pero pueden no ser tan formales. La Cláusula 4 y el Anexo A proporcionan orientación para ayudar al usuario a comprender mejor los elementos y actividades de un CSMS.

4.2 Categoría: Análisis de riesgos.

4.2.1 Descripción de la categoría.

La primera categoría principal del CSMS es el análisis de riesgos. Esta categoría analiza gran parte de la información de fondo que se incorpora a muchos de los otros elementos del CSMS. La Figura 2 muestra los dos elementos que forman parte de la categoría:
· Justificación del negocio y
· Identificación, clasificación y evaluación de riesgos.

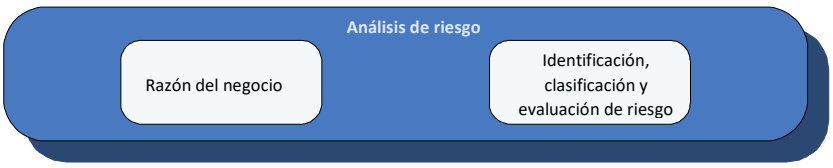

Figura 2 - Vista gráfica de la categoría: análisis de riesgos.

4.2.2 **Elemento: justificación del negocio.**

Objetivo:

Identifique y documente las necesidades únicas de una organización para abordar el riesgo cibernético de IACS.

Descripción:

Una justificación del negocio se basa en la naturaleza y magnitud de las consecuencias financieras, HSE y otras posibles consecuencias en caso de que ocurran incidentes cibernéticos de IACS.

Razón fundamental:

Establecer una justificación del negocio es esencial para que una organización mantenga la aceptación de la gerencia a un nivel apropiado de inversión para el programa de seguridad cibernética de IACS.

Requisitos:

Tabla 1 – Requisitos del negocio: Requerimientos.

Descripción		Requerimientos
4.2.2.1	**Desarrollar una justificación del negocio.**	La organización debe desarrollar una lógica comercial de alto nivel, como base para su esfuerzo por administrar la seguridad cibernética de IACS, que aborda la dependencia única de la organización con el IACS.

4.2.3 Elemento: identificación de riesgos, clasificación y evaluación.

Objetivo:

Identificar el conjunto de riesgos cibernéticos de IACS que enfrenta una organización y evaluar la probabilidad y la gravedad de estos riesgos.

Descripción:

Las organizaciones protegen su capacidad de realizar su misión identificando, priorizando y analizando sistemáticamente las posibles amenazas de seguridad, vulnerabilidades y consecuencias utilizando metodologías aceptadas. El primer conjunto de requisitos presenta las acciones que una organización toma para llevar a cabo una evaluación de riesgos detallada y de alto nivel que incorpora la evaluación de vulnerabilidad, en un orden cronológico típico. Entre estos requisitos, los relacionados con la preparación de evaluaciones de riesgo detalladas y de alto nivel son 4.2.3.1, 4.2.3.2 y 4.2.3.8 a continuación. Los últimos requisitos (4.2.3.10 a 4.2.3.14) son requisitos generales que se aplican al proceso general de evaluación de riesgos. La subcláusula 4.3.4.2 cubre el proceso de tomar medidas basadas en esta evaluación.

Razón fundamental:
Dado que el propósito de invertir en ciberseguridad es reducir el riesgo, se basa en la comprensión del nivel de riesgo y las posibles mitigaciones.

Requisitos:

Tabla 2 - Identificación, clasificación y evaluación de riesgos: requisitos.

Descripción		Requisitos
4.2.3.1	Seleccionar una metodología de evaluación de riesgos	La organización debe seleccionar un enfoque y metodología en particular de evaluación y análisis de riesgos que identifique y priorice los riesgos en función de las amenazas de seguridad, vulnerabilidades y consecuencias relacionadas con sus activos de IACS.

4.2.3.2	Proporcionar información básica sobre la evaluación de riesgos	La organización debe proporcionar a los participantes en la actividad de evaluación de riesgos la información adecuada, incluida la capacitación en metodología, antes de comenzar a identificar los riesgos.
4.2.3.3	Realizar una evaluación de riesgos de alto nivel	Se debe realizar una evaluación de riesgos del sistema de alto nivel para comprender las consecuencias financieras y de HSE en caso de que la disponibilidad, integridad o confidencialidad del IACS se vea comprometida.
4.2.3.4	Identificar los IACS	La organización debe identificar los diversos IACS, recopilar datos sobre los dispositivos para caracterizar la naturaleza del riesgo de seguridad y agrupar los dispositivos en sistemas lógicos.
4.2.3.5	Desarrollar diagramas de red simples	La organización debe desarrollar diagramas de red simples para cada uno de los sistemas integrados lógicamente que muestren los principales dispositivos, tipos de red y ubicaciones generales del equipo.
4.2.3.6	Priorizar sistemas	La organización debe desarrollar los criterios y asignar una calificación de prioridad para mitigar el riesgo de cada sistema de control lógico.
4.2.3.7	Realizar una evaluación detallada de la vulnerabilidad	La organización debe realizar una evaluación detallada de la vulnerabilidad de su IACS lógico individual, que se puede determinar en función de los resultados de la evaluación de riesgos de alto nivel y la priorización de IACS sujeto a estos riesgos.
4.2.3.8	Identificar una metodología detallada de evaluación de riesgos	La metodología detallada de evaluación de riesgos de la organización debe incluir métodos para priorizar vulnerabilidades detalladas e identificadas en la evaluación de vulnerabilidad.
4.2.3.9	Realizar una evaluación de riesgos detallada	La organización debe realizar una evaluación de riesgos detallada que incorpore las vulnerabilidades detalladas e identificadas en la evaluación de vulnerabilidad.
4.2.3.10	Identificar la frecuencia de reevaluación y los criterios de activación	La organización debe identificar la frecuencia de reevaluación de riesgos y vulnerabilidades, así como cualquier criterio de activación de reevaluación basado en tecnología, organización o cambios en la operación industrial
4.2.3.11	Integrar los resultados de la evaluación de riesgos de seguridad física, HSE y ciberseguridad	Los resultados de las evaluaciones de riesgos de seguridad física, HSE y ciberseguridad se integrarán para comprender el riesgo general de los activos.
4.2.3.12	Realizar evaluaciones de riesgos durante todo el ciclo de vida de IACS	Las evaluaciones de riesgos se realizarán en todas las etapas del ciclo de vida de la tecnología, incluidos el desarrollo, la implementación, los cambios y la descontinuación del sistema.

4.2.3.13	Documentar la evaluación de riesgos	Se documentará la metodología de evaluación de riesgos y los resultados de la evaluación de riesgos.
4.2.3.14	Mantener registros de evaluación de vulnerabilidad	Se mantendrán registros de evaluación de vulnerabilidad actualizados para todos los activos que comprenden el IACS.

4.3 Categoría: abordar el riesgo con el CSMS.

4.3.1 Descripción de la categoría.

La segunda categoría principal del CSMS es abordar el riesgo con el CSMS. Esta categoría contiene la mayor parte de los requisitos e información contenidos en el CSMS. Se divide en los siguientes tres grupos de elementos:

· Política de seguridad, organización y sensibilización.
· Contramedidas de seguridad seleccionadas e Implementación.

4.3.2 Grupo de elementos: política de seguridad, organización y concientización.

4.3.2.1 Descripción del grupo de elementos.

El primer grupo de elementos en esta categoría analiza el desarrollo de las políticas básicas de seguridad cibernética, las organizaciones responsables de la seguridad cibernética y la concientización dentro de la organización de los problemas de seguridad cibernética. La Figura 3 muestra una representación gráfica de los cinco elementos contenidos en este grupo de elementos:

· Alcance del CSMS,
· Organización para la seguridad,
· Capacitación del personal y concientización de seguridad,
· Plan de continuidad del negocio y
· Políticas y procedimientos de seguridad.

IEC 2314/10

Figura 3 - Vista gráfica del grupo de elementos: Políticas, organización y concientización de seguridad.

4.3.2.2 Elemento: alcance del CSMS. Objetivo:

Identifique, evalúe y documente los sistemas, procesos y organizaciones a los que se aplica el CSMS.

Descripción:

El alcance incluye todos los aspectos del IACS, puntos de integración con socios comerciales, clientes y proveedores.

Razón fundamental:

La gerencia debe comprender los límites en los que el CSMS se aplica a la organización, así como establecer una dirección y enfoque para el CSMS. Al desarrollar un alcance claramente definido, es más fácil para la gerencia transmitir sus objetivos y propósitos para el CSMS.

Requisitos:

Tabla 3 - Alcance del CSMS: requisitos.

Descripción		Requisitos
4.3.2.2.1	Definir el alcance del CSMS	La organización debe desarrollar un alcance escrito formal para el programa de seguridad cibernética.
4.3.2.2.2	Definir el contenido del alcance	El alcance debe explicar los objetivos estratégicos, el proceso y el momento para el CSMS.

4.3.2.3 Elemento: Organización para la seguridad. Objetivo:

Establecer las entidades responsables de administrar, conducir y evaluar la seguridad cibernética general de los activos IACS de la organización.

Descripción:

El liderazgo superior establece una organización, estructura o red de personas para proporcionar supervisión y dirección para administrar los riesgos de seguridad cibernética asociados con IACS. También proporcionan el personal necesario para llevar a cabo y evaluar los programas de seguridad cibernética en toda la organización durante la vida del CSMS. Una organización en cualquier nivel puede implementar esta norma, incluida una empresa u otra empresa, división, planta o subconjunto general de una planta.

Razón fundamental:

El compromiso con un programa de seguridad comienza en la parte superior de la organización. Debido a que la seguridad cibernética de IACS involucra varios conjuntos diferentes de habilidades que a menudo no se encuentran en una sección o departamento particular de una organización, es imperativo que los altos directivos formulen un enfoque responsable para administrar la seguridad, con una identificación clara de responsabilidades que haga un buen uso de las habilidades y recursos laborales. Esto puede adoptar varias formas diferentes, desde una sola organización hasta una red de personas que trabajan juntas para abordar

diferentes aspectos de seguridad. El enfoque particular depende en gran medida de la cultura operativa de una organización.

Requisitos:

Tabla 4 - Organización para la seguridad: requisitos.

Descripción		Requisitos
4.3.2.3.1	Obtener el apoyo de la alta dirección	La organización debe obtener el apoyo de la alta gerencia para un programa de seguridad cibernética.
4.3.2.3.2	Establecer las organizaciones de seguridad	Debe haber una organización, estructura o red de partes interesadas establecida (o elegida) bajo el liderazgo de la gerencia, con la responsabilidad de proporcionar una dirección y supervisión clara de los aspectos cibernéticos de la IACS.
4.3.2.3.3	Definir las responsabilidades organizacionales.	Las responsabilidades de la organización se definirán claramente para la seguridad cibernética y las actividades de seguridad física relacionadas.
4.3.2.3.4	Definir la composición del equipo de partes interesadas.	El equipo central de partes interesadas debe ser de naturaleza cruzada para reunir las habilidades necesarias para abordar la seguridad en todas las partes de la IACS.

4.3.2.4 Elemento: Capacitación del personal y concientización de seguridad. Objetivo:

Proporcione a todo el personal (incluidos los empleados, los empleados contratados y los contratistas externos) la información necesaria para identificar, revisar, abordar y, cuando corresponda, corregir las vulnerabilidades y amenazas a IACS y para ayudar a garantizar que sus propias prácticas laborales estén utilizando contramedidas efectivas.

Descripción:

Todo el personal debe recibir capacitación técnica adecuada asociada con las amenazas y vulnerabilidades conocidas de hardware, software e ingeniería social.

Razón fundamental:

En el área de IACS, se debe poner el mismo énfasis en la seguridad cibernética que en la seguridad y la integridad operativa, porque las consecuencias pueden ser igual de graves. La concientización de seguridad para todo el personal es una herramienta esencial para reducir los riesgos de seguridad cibernética. El personal bien informado y atento es una de las líneas de defensa más importantes para asegurar un sistema. Por lo tanto, es importante que todo el personal comprenda la importancia de la seguridad para mantener el funcionamiento seguro del sistema.

Requisitos:

Tabla 5 - Capacitación del personal y concientización de seguridad: requisitos.

Descripción		Requisitos
4.3.2.4.1	Desarrollar un programa de capacitación.	La organización debe diseñar e implementar un programa de capacitación en seguridad cibernética.
4.3.2.4.2	Proporcionar procedimientos y capacitación en las instalaciones.	Todo el personal (incluidos los empleados, los empleados contratados y los contratistas de terceros) deberá recibir capacitación inicial y periódica, en los procedimientos de seguridad, en el uso correcto de las instalaciones y procesamiento de información.
4.3.2.4.3	Proporcionar capacitación para el personal de apoyo.	Todo el personal que realiza la gestión de riesgos, la ingeniería de IACS, la administración / mantenimiento del sistema y otras tareas que afectan al CSMS debe recibir capacitación sobre los objetivos de seguridad y las operaciones industriales para estas tareas.
4.3.2.4.4	Validar el programa de capacitación.	El programa de capacitación debe validarse de manera continua para garantizar que el personal comprenda el programa de seguridad y que esté recibiendo la capacitación adecuada.
4.3.2.4.5	Revisar el programa de entrenamiento a lo largo del tiempo	El programa de capacitación en seguridad cibernética se revisará, según sea necesario, para tener en cuenta las amenazas y vulnerabilidades nuevas o cambiantes.
4.3.2.4.6	Mantener registros de capacitación de empleados	Los registros de la capacitación de los empleados y los periodos para las actualizaciones deben mantenerse y revisarse periódicamente.

4.3.2.5 Elemento: Plan de continuidad del negocio. Objetivo:

Identifique procedimientos para mantener y / o restablecer operaciones comerciales esenciales mientras se recupera de una interrupción significativa.

Descripción:

Un plan de continuidad del negocio debe abordar los objetivos de recuperación para los diversos sistemas y subsistemas involucrados en función de las necesidades comerciales típicas, una lista de posibles interrupciones y los procedimientos de recuperación para cada uno, así como un cronograma para probar parte o la totalidad de los procedimientos de recuperación. Uno de los principales objetivos de recuperación debería ser mantener la máxima disponibilidad del sistema de control.

Razón fundamental:

Ningún conjunto de defensas puede prevenir todas las interrupciones debidas a incidentes de seguridad

cibernética. Un plan detallado de continuidad del negocio asegura que la información de IACS pueda restaurarse y utilizarse lo antes posible después de que ocurra una interrupción significativa.

Requisitos:

Tabla 6 - Plan de continuidad del negocio: requisitos.

Descripción		Requisitos
4.3.2.5.1	Especificar objetivos de recuperación	Antes de crear un plan de continuidad del negocio, la organización debe especificar objetivos de recuperación para los sistemas involucrados en función de las necesidades del negocio.
4.3.2.5.2	Determinar el impacto y las consecuencias para cada sistema.	La organización debe determinar el impacto en cada sistema debido a una interrupción significativa y las consecuencias asociadas con la pérdida de uno o más de los sistemas.
4.3.2.5.3	Desarrollar e implementar planes de continuidad del negocio	Los planes de continuidad se desarrollarán e implementarán para garantizar que los procesos del negocio puedan restaurarse de acuerdo con los objetivos de recuperación.
4.3.2.5.4	Formar un equipo de continuidad del negocio	Se debe formar un equipo de continuidad del negocio que incluya IACS y otros propietarios de procesos. En caso de una interrupción significativa, este equipo debe determinar la prioridad de los IACS para sistemas críticos del negocios para restablecer las operaciones.
4.3.2.5.5	Definir y comunicar roles y responsabilidades específicos	El plan de continuidad del negocio debe definir y comunicar los roles y responsabilidades específicos para cada parte del plan.
4.3.2.5.6	Crear procedimientos de respaldo que aseguren el plan de continuidad del negocio	La organización debe crear procedimientos de respaldo y restauración (ver 4.3.4.3.9) que aseguren el plan de continuidad del negocio.
4.3.2.5.7	Probar y actualizar el plan de continuidad del negocio.	El plan de continuidad del negocio se probará periódicamente y se actualizará según sea necesario.

4.3.2.6 Elemento: Políticas y procedimientos de seguridad. Objetivo:

Abordar cómo una organización define la seguridad, opera su programa de seguridad, define y aborda su tolerancia al riesgo y revisa su programa para realizar mejoras adicionales.

Descripción:

Las políticas de seguridad cibernética para el entorno IACS deben desarrollarse en función de las políticas existentes de alto nivel, los riesgos caracterizados y los niveles de tolerancia al riesgo identificados por la administración. Los procedimientos de seguridad cibernética se desarrollan a partir de las políticas de seguridad cibernética e identifican cómo se implementarán las políticas.

Razón fundamental:

Estas políticas y procedimientos escritos permiten a los empleados, contratistas, terceros y similares comprender claramente la perspectiva de seguridad cibernética para la organización, sus roles y responsabilidades para asegurar los activos de la compañía.

Requisitos:

Tabla 7 - Políticas y procedimientos de seguridad: requisitos.

	Descripción	Requisitos
4.3.2.6.1	Desarrollar políticas de seguridad.	La organización debe desarrollar políticas de seguridad cibernética de alto nivel para el entorno IACS que sean aprobadas por la dirección.
4.3.2.6.2	Desarrollar procedimientos de seguridad.	La organización debe desarrollar y aprobar procedimientos de seguridad cibernética, basados en las políticas de seguridad cibernética y proporcionar orientación sobre cómo cumplir con las políticas.
4.3.2.6.3	Mantener la coherencia entre los sistemas de gestión de riesgos.	Las políticas y procedimientos de seguridad cibernética que se ocupan de los riesgos de IACS deben ser coherentes con las políticas creadas por otros sistemas de gestión de riesgos o con extensiones de las mismas.
4.3.2.6.4	Definir requisitos de cumplimiento de procedimientos y políticas de seguridad cibernética.	Las políticas y procedimientos de seguridad cibernética, para el entorno IACS, deben incluir requisitos de cumplimiento.
4.3.2.6.5	Determinar la tolerancia de la organización al riesgo.	La organización debe determinar y documentar su tolerancia al riesgo como base para la creación de políticas y actividades de gestión de riesgos.
4.3.2.6.6	Comunique las políticas y procedimientos a la organización	Las políticas y procedimientos de seguridad cibernética, para el entorno IACS, se comunicarán a todo el personal apropiado.
4.3.2.6.7	Revisar y actualizar las políticas y procedimientos de seguridad cibernética	Las políticas y procedimientos de seguridad cibernética se revisarán periódicamente, se validarán para confirmar que están actualizados y se seguirán y actualizarán según sea necesario para garantizar que sigan siendo apropiados.
4.3.2.6.8	Demostrar apoyo de liderazgo superior para la seguridad cibernética.	Los altos directivos deberán demostrar su compromiso con la seguridad cibernética al respaldar las políticas de seguridad cibernética.

4.3.3 Grupo de elementos: contramedidas de seguridad seleccionadas.

4.3.3.1 Descripción del grupo de elementos.

El segundo grupo de elementos dentro de esta categoría es Contramedidas de seguridad seleccionadas. Los elementos dentro de este grupo evalúan algunos de los principales tipos de controles de seguridad que forman parte de un CSMS bien diseñado. Este documento no intenta describir la implementación completa de ninguna de estas contramedidas de seguridad seleccionadas. Discute muchos de los problemas de política, procedimiento y práctica relacionados con estas contramedidas de seguridad particulares. La Figura 4 muestra una representación gráfica de los seis elementos en el grupo de elementos:

· Personal de Seguridad,
· Seguridad física y ambiental,
· Segmentación de la red,
· Control de acceso - Administración de cuentas,
· Control de acceso - Autenticación y · Control de acceso - Autorización.

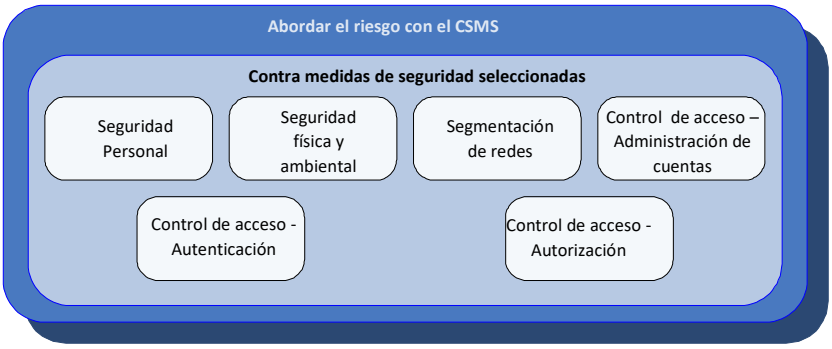

Figura 4 - Vista gráfica del grupo de elementos: contramedidas de seguridad seleccionadas.

Estas contramedidas particulares se seleccionaron para su inclusión porque su amplio impacto en las políticas y la arquitectura hace que sea esencial considerarlas por adelantado al construir cualquier CSMS. No es la intención de esta norma especificar una lista completa y suficiente de contramedidas, ya que la integridad se determina a través del proceso de evaluación y gestión de riesgos descrito en la norma.

4.3.3.2 Elemento: Seguridad del personal. Objetivo:

Establezca las políticas y procedimientos para determinar si el personal mantendrá la seguridad IACS de la organización durante todo el ciclo de vida de su empleo.

Descripción:

La seguridad del personal implica evaluar al personal tanto actual como nuevo para determinar si mantendrán la seguridad de IACS para la organización. Para el personal nuevo, los evalúa antes de su ingreso a la organización asegurándose de que demuestren comportamientos consistentes con su futura responsabilidad de seguridad. Para el personal actual, establece que continúan demostrando un comportamiento consistente con sus responsabilidades de seguridad actuales.

Razón fundamental:

En muchas organizaciones, los requisitos de seguridad del personal están motivados por las preocupaciones sobre las amenazas internas y la posibilidad de accidentes causados por la falta de atención a los detalles o por el personal no apto para un trabajo debido a la falta de antecedentes adecuados o el uso de sustancias que podrían nublar el juicio. Al implementar políticas de seguridad del personal, es posible reducir este tipo de problemas.

Requisitos:

Tabla 8 - Seguridad del personal: requisitos.

Descripción		Requisitos
4.3.3.2.1	Establecer una política de seguridad del personal	Deberá establecerse una política de seguridad del personal que constituya claramente el compromiso de la organización con la seguridad y las responsabilidades de seguridad del personal. (El personal incluye empleados, posibles empleados, empleados contratados y contratistas externos).
4.3.3.2.2	Personal de prueba inicialmente	A menos que la regulación gubernamental lo prohíba, todo el personal con acceso al IACS (tanto físico como cibernético), incluidas las nuevas contrataciones y las transferencias internas a puestos sensibles, se someterá a un examen, incluida la validación de su identidad y verificación de antecedentes, durante el proceso de solicitud de empleo.
4.3.3.2.3	Examinar al personal de manera continua	El personal también debe estar sujeto a un examen continuo de los cambios que puedan indicar un conflicto de intereses o inquietudes por realizar el trabajo de manera adecuada.
4.3.3.2.4	Abordar las responsabilidades de seguridad	La política de seguridad del personal debe abordar las responsabilidades de seguridad desde el reclutamiento hasta el final del empleo, especialmente para puestos sensibles.
4.3.3.2.5	Documentar y comunicar las expectativas y responsabilidades de seguridad	Las expectativas y responsabilidades de seguridad deben documentarse claramente y comunicarse regularmente al personal.
4.3.3.2.6	Términos y condiciones de empleo de seguridad cibernética	Los términos y condiciones de empleo deberán indicar claramente la responsabilidad del personal por la seguridad cibernética. Estas responsabilidades se extenderán por un período de tiempo razonable después de que cese el empleo.
4.3.3.2.7	Separar las obligaciones para mantener los controles y equilibrios adecuados	Las obligaciones se deben separar entre el personal para mantener los controles y equilibrios adecuados, de modo que ningún individuo tenga el control total sobre las acciones que cambian la operación funcional del IACS.

4.3.3.3 Elemento: Seguridad física y ambiental. Objetivo:

Cree un entorno seguro para la protección de los activos de IACS. Un activo es cualquier objeto físico o lógico

propiedad o bajo custodia de una organización, que tiene un valor percibido o real para la organización (ver IEC / TS 62443-1). Los activos de IACS son aquellos que forman parte de IACS, ya sean físicos o cibernéticos, o que pueden afectar el funcionamiento de IACS. Las medidas de seguridad física aseguran que todos los activos, específicamente aquellos relacionados con el IACS de una organización, estén protegidos físicamente del acceso no autorizado, pérdida, daño, mal uso y similares. Las medidas de seguridad ambiental aseguran que los activos de una organización estén protegidos contra las condiciones ambientales que los harían inutilizables o dañarían la información que contienen.

Descripción:

Las medidas de seguridad física y ambiental deben diseñarse para complementar las medidas de seguridad cibernética adoptadas para proteger los activos que forman parte del IACS y coordinarse con la seguridad física del resto de la planta. Al desarrollar un programa para la seguridad física de los activos, es importante incluir todos los sistemas en el alcance y no solo limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras. El juicio práctico de ingeniería debe usarse para equilibrar los riesgos al determinar los procedimientos de seguridad física. La segmentación física es una contramedida de seguridad clave diseñada para compartimentar dispositivos en zonas de seguridad donde se emplean prácticas de seguridad identificadas para lograr el nivel de seguridad objetivo deseado.

Razón fundamental:

Los activos físicos son un medio para un fin, así como el fin en sí mismo. En los sistemas de control modernos, los activos físicos proporcionan los medios por los cuales opera el sistema cibernético. Por lo tanto, el activo tiene valor en sí mismo, pero también tiene valor como parte integral del sistema de control. Dado que tanto el activo como el sistema de control se requieren mutuamente, ambos estarán protegidos para que el sistema sea seguro. La premisa de seguridad primordial es que el uso de contramedidas de seguridad debe ser acorde con el nivel de riesgo. Si bien la segmentación física es una contramedida de seguridad importante empleada junto con otras capas de defensa para reducir el riesgo que puede estar asociado con IACS, puede no ser necesario si los riesgos de seguridad están dentro de los límites aceptados.

Requisitos:

Tabla 9 - Seguridad física y ambiental: requisitos.

	Descripción	Requisitos
4.3.3.3.1	Establecer políticas complementarias de seguridad física y cibernética	Se establecerán políticas y procedimientos de seguridad que aborden la seguridad física y cibernética en la protección de los activos.
4.3.3.3.2	Establecer perímetro (s) de seguridad física	Se deben establecer uno o más perímetros de seguridad física para proporcionar barreras al acceso no autorizado a los activos protegidos
4.3.3.3.3	Proporcionar controles de entrada	Se deben proporcionar controles de entrada apropiados en cada barrera o límite.

4.3.3.3.4	Proteger los activos contra el daño ambiental	Los activos deben protegerse contra el daño ambiental de amenazas tales como incendios, agua, humo, polvo, radiación, corrosión e impacto.
4.3.3.3.5	Exigir a los empleados que sigan los procedimientos de seguridad	Los empleados deberán seguir y hacer cumplir los procedimientos de seguridad física que se hayan establecido.
4.3.3.3.6	Proteger las conexiones	Todas las conexiones bajo el control de la organización deben estar protegidas adecuadamente contra manipulaciones o daños.
4.3.3.3.7	Mantener los activos del sistema	Todos los activos del sistema, incluidos los equipos ambientales auxiliares, se deben mantener adecuadamente para garantizar un funcionamiento adecuado.
4.3.3.3.8	Establecer procedimientos para el monitoreo y las alarmas	Se deben establecer procedimientos para el monitoreo de las alarmas cuando se compromete la seguridad física o ambiental.
4.3.3.3.9	Establecer procedimientos para la adición, eliminación y eliminación de activos	Los procedimientos deben establecerse y auditarse con respecto a la adición y eliminación de todos los activos.
4.3.3.3.10	Establecer procedimientos para la protección provisional de activos críticos	Se deben establecer procedimientos para garantizar la protección de los componentes críticos durante la interrupción de las operaciones, por ejemplo, debido a incendio, ingreso de agua, violación de seguridad, interrupción, natural o cualquier otro tipo de desastre.

4.3.3.4 Elemento: segmentación de la red. Objetivo:

Agrupe y separe los dispositivos IACS claves en zonas con niveles de seguridad comunes para administrar los riesgos de seguridad y lograr el nivel de seguridad deseado para cada zona.

Descripción:

La segmentación de red es una contramedida de seguridad clave diseñada para compartimentar dispositivos en zonas de seguridad donde se emplean prácticas de seguridad identificadas para lograr el nivel de seguridad deseado. La zona puede ser un segmento de red autónomo aislado o un segmento de red separado de la red de la organización por algún tipo de dispositivo de barrera de red. IACS debe diseñarse de manera que filtre / evite que los paquetes de comunicación no esenciales lleguen a los dispositivos IACS.

Para las redes basadas en el Protocolo de control de transmisión / Protocolo de Internet (TCP / IP), los dispositivos de barrera más comunes en uso son los firewalls, enrutadores y conmutadores de capa 3. Para redes de tipo no TCP / IP, los dispositivos de barrera pueden ser puertas de enlace independientes o integradas en el módulo de interfaz de red de un dispositivo IACS.

Razón fundamental:

La premisa de seguridad primordial es que el uso de contramedidas de seguridad debe ser acorde con el nivel de riesgo. Si bien la segmentación de la red es una contramedida de seguridad importante empleada junto con otras capas de defensa para reducir el riesgo que puede estar asociado con IACS, puede no ser necesario si los riesgos de seguridad son bajos.

Requisitos:

Tabla 10 - Segmentación de red: requisitos

Descripción		Requisito
4.3.3.4.1	Desarrollar la arquitectura de segmentación de red.	Se desarrollará una estrategia de contramedida de segmentación de red que emplee zonas de seguridad para dispositivos IACS en función del nivel de riesgo de IACS.
4.3.3.4.2	Emplear aislamiento o segmentación en IACS de alto riesgo	Los IACS de alto riesgo deben aislarse o emplear un dispositivo de barrera para separarlo de otras zonas con diferentes niveles de seguridad o riesgos.
4.3.3.4.3	Bloquee las comunicaciones no esenciales con dispositivos de barrera.	Los dispositivos de barrera bloquearán todas las comunicaciones no esenciales dentro y fuera de la zona de seguridad que contiene equipos de control crítico.

4.3.3.5 Elemento: Control de acceso - Administración de la cuenta. Objetivo:

Asegúrese, de manera continua, de que solo las entidades apropiadas tengan cuentas que permitan el acceso y que estas cuentas ofrezcan los privilegios de acceso adecuados.

Descripción:

El control de acceso es el método para controlar quién o qué entidades pueden acceder a las instalaciones y sistemas y qué tipo de acceso está permitido. Hay tres aspectos clave asociados con el control de acceso: administración de cuentas, autenticación y autorización. Los tres aspectos trabajarán juntos para establecer una estrategia de control de acceso segura y sólida.

La administración de cuentas es el método asociado con la concesión y revocación de cuentas de acceso y el mantenimiento de los permisos y privilegios otorgados en virtud de estas cuentas para acceder a recursos y funciones específicos en las instalaciones físicas, la red o el sistema. Las cuentas de acceso deben estar basadas en funciones o roles y pueden definirse para individuos, grupos de individuos que funcionan como un equipo o para dispositivos que proporcionan una función.

Razón fundamental:

El mal uso de datos y sistemas puede tener serias consecuencias, incluyendo daños a la vida humana, daños ambientales, pérdidas financieras y reputación corporativa dañada. Estos riesgos aumentan cuando los empleados, contratistas o personal temporal tienen acceso innecesario a datos y sistemas.

Requisitos:

Tabla 11 - Control de acceso - Administración de cuentas: requisitos

Descripción		Requisito
4.3.3.5.1	Las cuentas de acceso implementan la política de seguridad de autorización	Los privilegios de acceso implementados para las cuentas de acceso deben establecerse de acuerdo con la política de seguridad de autorización de la organización (ver 4.3.3.7.1).
4.3.3.5.2	Identificar individuos	Como para todos los controles de seguridad cibernética, la realización de las cuentas de acceso a individuos, para que puedan acceder a un equipo del sistema de control se determinará considerando las amenazas, los riesgos y las vulnerabilidades. En este caso, las consideraciones incluyen los riesgos HSE de los controles individuales, la mitigación mediante controles de seguridad física complementarios, el requisito de responsabilidad y la necesidad administrativa / operativa.
4.3.3.5.3	Autorizar acceso a la cuenta	El acceso se otorgará, cambiará o terminará bajo la autoridad de un directivo apropiado.
4.3.3.5.4	Registrar cuentas de acceso	Se mantendrá un registro de todas las cuentas de acceso, incluidos los detalles de las personas y dispositivos autorizados para usar la cuenta, sus permisos y el administrador de autorización.
4.3.3.5.5	Suspender o eliminar cuentas innecesarias	Las cuentas de acceso se suspenderán o eliminarán tan pronto como ya no sean necesarias (por ejemplo, cambio de trabajo).
4.3.3.5.6	Revisar los permisos de la cuenta	Todas las cuentas de acceso establecidas se revisarán periódicamente para garantizar que las personas y los dispositivos tengan solo los permisos mínimos requeridos.
4.3.3.5.7	Cambiar contraseñas predeterminadas	Las contraseñas predeterminadas para las cuentas de acceso se cambiarán antes de que el IACS se ponga en servicio.
4.3.3.5.8	Administración de cuentas de auditoría	Se deben realizar revisiones periódicas del cumplimiento de la política de administración de cuentas.

4.3.3.6 Elemento: Control de acceso – Autenticación. Objetivo:

Identifique positivamente a los usuarios, hosts, aplicaciones, servicios y recursos de la red para transacciones computarizadas, de modo que se les puedan otorgar los derechos y responsabilidades asociados con las cuentas que se les han otorgado bajo la administración de la cuenta.

Descripción:

El control de acceso es el método para controlar quién o qué recursos pueden acceder a las instalaciones y sistemas y qué tipo de acceso está permitido. Hay tres aspectos clave asociados con el control de acceso: administración de cuentas, autenticación y autorización. Los tres aspectos trabajarán juntos para establecer una estrategia de control de acceso segura y sólida.
Existen varios tipos de estrategias de autenticación y cada uno tiene diferentes grados de fortaleza. Los métodos de autenticación sólidos son bastante precisos para identificar positivamente al usuario. Los

métodos de autenticación débiles son los que pueden ser fácilmente derrotados para proporcionar acceso no deseado a la información. La ubicación física del usuario puede tener un impacto significativo en el riesgo de acceder al IACS.

Razón fundamental:

Los requisitos de autenticación son más estrictos para los usuarios de administración / configuración y usuarios remotos, que para otros usuarios. Esto se debe a que los usuarios de administración / configuración tienen privilegios más amplios y sus acciones tienen potencialmente más impacto que otros usuarios; y los usuarios remotos generalmente no están sujetos a controles de acceso físico complementarios. El bloqueo automático de la cuenta debido a inicios de sesión fallidos o períodos de inactividad aumenta la intensidad de la autenticación, pero se considera cuidadosamente en el entorno IACS, ya que la falla de autenticar a un usuario válido podría tener implicaciones de HSE si el usuario no puede realizar tareas en una situación crítica. En el entorno IACS, hay un gran énfasis en combinar medidas de autenticación física con prácticas de autenticación electrónica.

Requisitos:

Tabla 12 - Control de acceso - Autenticación: requisitos.

Descripción		Requisito
4.3.3.6.1	Desarrollar un estrategia de autenticación	Las empresas deberán tener una estrategia o enfoque de autenticación que defina los métodos de autenticación que se utilizarán.
4.3.3.6.2	Autenticar a todos los usuarios antes de usar el sistema	Todos los usuarios deberán autenticarse antes de usar la aplicación solicitada, a menos que haya combinaciones compensatorias de tecnologías de control de entrada y prácticas administrativas.
4.3.3.6.3	Requerir métodos de autenticación fuertes para la administración del sistema y la configuración de la aplicación	Se deben utilizar prácticas de autenticación sólidas (como requerir contraseñas seguras) en todas las cuentas de acceso del administrador del sistema y las cuentas de acceso de configuración de la aplicación.
4.3.3.6.4	Registre y revise todos los intentos de acceso a sistemas críticos	Los archivos de registro deben registrar todos los intentos de acceso a sistemas críticos y deben revisarse para detectar intentos de acceso exitosos y fallidos.
4.3.3.6.5	Autenticar a todos los usuarios remotos en el nivel apropiado	La organización debe emplear un esquema de autenticación con un nivel adecuado de fortaleza para identificar positivamente a un usuario interactivo remoto.
4.3.3.6.6	Desarrolle una política para inicio de sesión remoto y conexiones	La organización debe desarrollar una política que aborde el inicio de sesión remoto por parte de un usuario y / o conexiones remotas (por ejemplo, conexiones de tarea a tarea) al sistema de control que define las respuestas apropiadas del sistema a intentos fallidos de inicio de sesión y períodos de inactividad.
4.3.3.6.7	Deshabilitar la cuenta de acceso después de intentos fallidos de inicio de sesión remoto	Después de cierto número de intentos fallidos de inicio de sesión por parte de un usuario remoto, el sistema debe deshabilitar la cuenta de acceso durante un cierto período de tiempo.

4.3.3.6.8	Requerir autenticación después de la inactividad del sistema remoto	Después de un período definido de inactividad, se debe requerir que un usuario remoto vuelva a autenticarse antes de que el usuario remoto pueda volver a acceder al sistema.
4.3.3.6.9	Emplear autenticación para la comunicación de tarea a tarea	Los sistemas deben emplear esquemas de autenticación apropiados para la comunicación de tarea a tarea entre aplicaciones y dispositivos.

4.3.3.7 Elemento: Control de acceso – Autorización. Objetivo:

Otorgue privilegios de acceso a los recursos tras la autenticación exitosa del usuario y la identificación de su cuenta de acceso asociada. Los privilegios otorgados están determinados por la configuración de la cuenta configurada durante el paso de administración de la cuenta en el proceso de negocio.

Descripción:

El control de acceso es el método para controlar quién o qué recursos pueden acceder a las instalaciones y sistemas y qué tipo de acceso está permitido. Hay tres aspectos clave asociados con el control de acceso: administración de cuentas, autenticación y autorización. Los tres aspectos trabajarán juntos para establecer una estrategia de control de acceso segura y sólida.
La autorización explora los controles destinados a proteger la información y los activos de la destrucción, cambio o divulgación deliberada e inadvertida. Se centra específicamente en medidas diseñadas para garantizar que los agentes autenticados tengan acceso a los activos de información requeridos.
Al igual que con la autenticación, la autorización depende de la ubicación del usuario.

Razón fundamental:

Es importante en el entorno de IACS asegurarse de que las personas adecuadas tengan acceso a la información y los sistemas correctos y que no se les impida hacer su trabajo debido a la falta de autorización. La aplicación proporciona la autorización para realizar funciones de trabajo específicas.
Es necesario considerar las implicaciones de seguridad al desarrollar la estrategia de autorización.

Requisitos:

Tabla 13 - Control de acceso - Autorización: Requisitos

Descripción		Requisito
4.3.3.7.1	Definir una política de seguridad de autorización.	Las reglas que definen los privilegios autorizados en las cuentas de acceso para el personal en diversas funciones laborales se definirán en una política de seguridad de autorización que esté claramente documentada y aplicada a todo el personal tras la autenticación.
4.3.3.7.2	Establecer métodos de permisos físicos y lógicos apropiados para acceder a dispositivos IACS	El permiso para acceder a los dispositivos IACS debe ser lógico (reglas que otorgan o niegan el acceso a usuarios conocidos en función de sus roles), físicos (bloqueos, cámaras y otros controles que restringen el acceso a una consola de computadora activa), o ambos.

4.3.3.7.3	Controle el acceso a la información o sistemas a través de cuentas de acceso basadas en roles	Las cuentas de acceso deben estar basadas en roles para administrar el acceso a información o sistemas apropiados para el rol de ese usuario. Las implicaciones de seguridad se deben considerar al definir roles.
4.3.3.7.4	Emplear múltiples métodos de autorización para IACS críticos	En entornos de control críticos, se deben emplear múltiples métodos de autorización para limitar el acceso al IACS.

4.3.4 Grupo de elementos: implementación.

4.3.4.1 Descripción del grupo de elementos.

El tercer grupo de elementos en esta categoría es Implementación. Este elemento dentro de este grupo trata temas relacionados con la implementación del CSMS. La Figura 5 muestra una representación gráfica de los cuatro elementos en el grupo de elementos:

· Gestión e implementación de riesgos.
· Desarrollo y mantenimiento del sistema.
· Gestión de información y documentos.
· Planificación y respuesta a incidentes.

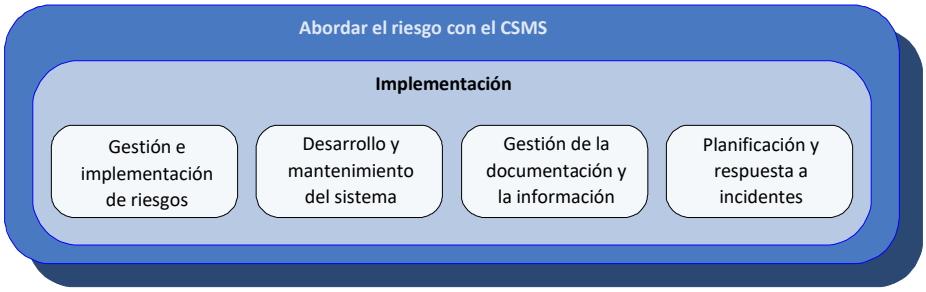

Figura 5 - Vista gráfica del grupo de elementos: implementación

4.3.4.2 Elemento: Gestión e implementación de riesgos. Objetivo:

Reduzca el riesgo y mantenga el riesgo a un nivel aceptable en el IACS basado en la tolerancia de la organización al riesgo.

Descripción:

La gestión e implementación de riesgos aborda la selección, desarrollo e implementa contramedidas que sean proporcionales a los riesgos. Las contramedidas pueden tener en cuenta el uso de productos con fuertes capacidades de seguridad inherentes, controles de seguridad manuales y de procedimiento y controles basados en tecnología para prevenir o reducir incidentes de seguridad.

Razón fundamental:

El elemento de gestión e implementación de riesgos se utiliza para convertir los resultados del elemento de clasificación y evaluación de identificación de riesgos de esta norma en acciones efectivas y concretas. Aunque nunca se puede eliminar por completo, el riesgo se puede gestionar de manera que equilibre el costo de evitarlo con el costo potencial del incidente.

Requisitos:

Tabla 14 - Gestión e implementación de riesgos: requisitos.

Descripción		Requisito
4.3.4.2.1	Gestionar el riesgo de IACS de forma continua	La organización debe adoptar un marco de gestión de riesgos que incluya la selección e implementación de dispositivos IACS y contramedidas para gestionar el riesgo a un nivel aceptable durante la vida útil de la instalación.
4.3.4.2.2	Emplear un conjunto común de contramedidas	Un conjunto definido común de contramedidas (técnicas y administrativas) para abordar los riesgos de seguridad física y cibernética debe definirse y aplicarse en toda la organización siempre que se identifique un riesgo específico.

4.3.4.3 Elemento: Desarrollo y mantenimiento del sistema. Objetivo:

Asegúrese de que el nivel de tolerancia al riesgo deseado de la organización se mantenga a medida que sus activos de IACS evolucionen mediante el mantenimiento de los sistemas existentes, así como el desarrollo y la adquisición de nuevos sistemas.

Descripción:

Este elemento aborda el diseño de ciberseguridad en sistemas desde las primeras etapas de desarrollo. También implica el mantenimiento de esas políticas y procedimientos de ciberseguridad a medida que el sistema cambia a lo largo de su ciclo de vida.

Razón fundamental:

Las organizaciones han descubierto que el mantenimiento del CSMS es más desafiante que establecerlo. Por esta razón, los procedimientos que abordan proactivamente la seguridad cibernética como parte de la evolución natural de los sistemas IACS son críticos.

Requisitos:

Tabla 15 - Desarrollo y mantenimiento del sistema: requisitos

Descripción		Requisito
4.3.4.3.1	Definir y probar funciones y capacidades de seguridad.	Las funciones y capacidades de seguridad de cada nuevo componente del IACS se definirán por adelantado, se desarrollarán o se lograrán mediante adquisiciones y se probarán junto con otros componentes para que todo el sistema cumpla con el perfil de seguridad deseado.

4.3.4.3.2	Desarrollar e implementar un sistema de gestión de cambios.	Se debe desarrollar e implementar un sistema de gestión de cambios para el entorno IACS. El proceso de gestión del cambio deberá seguir los principios de separación de funciones para evitar conflictos de intereses.
4.3.4.3.3	Evaluar todos los riesgos de cambiar el IACS	Usando criterios claramente definidos, los cambios propuestos a IACS serán revisados por su impacto potencial a los riesgos de HSE y los riesgos de seguridad cibernética por personas técnicamente conocedoras de la operación industrial y el sistema IACS.
4.3.4.3.4	Requerir políticas de seguridad para el desarrollo del sistema o cambios de mantenimiento	Los requisitos de seguridad de un nuevo sistema que se instala en el entorno IACS en una zona existente deberá cumplir con las políticas y procedimientos de seguridad requeridos para esa zona / entorno. Del mismo modo, las actualizaciones o cambios de mantenimiento deberán cumplir con los requisitos de seguridad de la zona.
4.3.4.3.5	Integre los procedimientos de gestión de cambios de ciberseguridad y gestión de seguridad de procesos (PSM)	Los procedimientos de gestión de cambios de seguridad cibernética deben integrarse con los procedimientos de PSM existentes .
4.3.4.3.6	Revisar y mantener políticas y procedimientos.	Las políticas y procedimientos de gestión de cambios y operaciones deberán revisarse y mantenerse actualizados para garantizar que los cambios de seguridad no aumenten los riesgos para la seguridad o la continuidad del negocio.
4.3.4.3.7	Establecer y documentar un procedimiento de gestión de parches.	Se debe establecer, documentar y seguir un procedimiento para el manejo de parches.
4.3.4.3.8	Establecer y documentar procedimientos de gestión de antivirus / malware	Se establecerá, documentará y seguirá un procedimiento para la gestión de antivirus / malware.
4.3.4.3.9	Establecer procedimientos de respaldo y restauración	Se establecerá, utilizará y verificará un procedimiento apropiado para realizar copias de seguridad y restaurar sistemas informáticos y proteger copias de seguridad.

4.3.4.4 Elemento: Gestión de información y documentos. Objetivo:

Clasifique, gestione, proteja y presente la información asociada con el IACS y el CSMS en el momento apropiado al personal autorizado.

Descripción:

Las organizaciones deben emplear políticas integrales de gestión de documentos e información para activos de información dentro del alcance de sus IACS y CSMS. Se debe tener cuidado para proteger esta información y verificar que se conserven las versiones apropiadas. Los sistemas de clasificación de información que permiten que los activos de información reciban el nivel adecuado de protección son la clave para alcanzar este objetivo.

Razón fundamental:

Gran parte de la información sobre IACS puede almacenarse electrónicamente o en papel fuera de IACS y no está protegida por los controles de autorización de IACS. El acceso y el uso no autorizados de esta información es una amenaza para la seguridad de IACS. Esta información debe controlarse y gestionarse adecuadamente.

Requisitos:

Tabla 16 - Gestión de información y documentos: requisitos.

Descripción		Requisito
4.3.4.4.1	Desarrollar procesos de gestión del ciclo de vida para la información de IACS	Se desarrollará y mantendrá un proceso de gestión de documentos del ciclo de vida para la información de IACS.
4.3.4.4.2	Definir niveles de clasificación de información	Los niveles de clasificación de la información (por ejemplo, confidencial de la empresa, restringida y pública) se definirán para el acceso y el control, incluido el intercambio, la copia, la transmisión y la distribución apropiadas para el nivel de protección requerido.
4.3.4.4.3	Clasificar todos los activos de información CSMS	Todos los activos lógicos dentro del alcance del CSMS (es decir, la información de diseño del sistema de control, las evaluaciones de vulnerabilidad, los diagramas de red y los programas de operaciones industriales) se clasificarán para indicar la protección requerida acorde con la consecuencia de su divulgación o modificación no autorizada.
4.3.4.4.4	Garantizar el control adecuado de los registros.	Deben desarrollarse políticas y procedimientos que detallen la retención, la protección física y de integridad, la destrucción y la eliminación de todos los activos en función de su clasificación, incluidos los registros escritos y electrónicos, el equipo y otros medios que contengan información, teniendo en cuenta los requisitos legales o reglamentarios.
4.3.4.4.5	Garantizar la recuperación de registros a largo plazo	Deben emplearse medidas apropiadas para garantizar que se puedan recuperar registros a largo plazo (es decir, convertir los datos a un formato más nuevo o retener equipos más antiguos que puedan leer los datos).
4.3.4.4.6	Mantener clasificaciones de información	La información que requiere un control o manejo especial debe revisarse periódicamente para validar que aún se requiere un manejo especial.
4.3.4.4.7	Auditar el proceso de gestión de información y documentos.	Se deben realizar revisiones periódicas del cumplimiento de la política de información y gestión de documentos.

4.3.4.5 Elemento: Planificación y respuesta a incidentes. Objetivo:

Predefina cómo la organización detectará y reaccionará ante incidentes de seguridad cibernética.

Descripción:

Al desarrollar un programa para la planificación y respuesta a incidentes, es importante incluir todos los sistemas en su alcance y no limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras. Parte del plan de respuesta a incidentes debe incluir procedimientos sobre cómo responderá la organización a los incidentes, incluidos métodos de notificación y documentación, investigaciones, recuperaciones y prácticas de seguimiento posteriores.

Razón fundamental:

Identificar un incidente temprano y responder adecuadamente puede limitar las consecuencias del evento. La planificación y respuesta a incidentes brinda a la organización la oportunidad de planificar incidentes de seguridad y luego responder de acuerdo con las prácticas establecidas de la compañía. No importa cuánto cuidado se tome al proteger un sistema, siempre es posible que intrusiones no deseadas puedan comprometer el sistema. Las vulnerabilidades tecnológicas continúan existiendo y las amenazas externas están aumentando en número y sofisticación, por lo que requieren una estrategia sólida para determinar la planificación y respuesta adecuadas. La información obtenida de los incidentes reales se captura porque es fundamental para evaluar y mejorar el CSMS.

Requisitos:

Tabla 17 - Planificación y respuesta a incidentes: requisitos

Descripción		Requisito
4.3.4.5.1	Implementar un plan de respuesta a incidentes.	La organización debe implementar un plan de respuesta a incidentes que identifique al personal responsable y defina las acciones que deben realizar las personas designadas.
4.3.4.5.2	Comunicar el plan de respuesta a incidentes.	El plan de respuesta a incidentes se comunicará a todas las organizaciones apropiadas.
4.3.4.5.3	Establecer un procedimiento de informe para actividades y eventos inusuales.	La organización debe establecer un procedimiento de informe para comunicar actividades y eventos inusuales que en realidad pueden ser incidentes de seguridad cibernética.
4.3.4.5.4	Educar a los empleados sobre cómo informar incidentes de seguridad cibernética.	Se debe educar a los empleados sobre su responsabilidad de reportar incidentes de seguridad cibernética y los métodos para reportar estos incidentes.
4.3.4.5.5	Informe los incidentes de seguridad cibernética de manera oportuna	La organización debe informar los incidentes de seguridad cibernética de manera oportuna.
4.3.4.5.6	Identificar y responder a incidentes.	Si se identifica un incidente, la organización debe responder de inmediato de acuerdo con los procedimientos establecidos.
4.3.4.5.7	Identificar infracciones de seguridad cibernética fallidas y exitosas	La organización debe tener procedimientos establecidos para identificar infracciones de seguridad cibernética fallidas y exitosas.
4.3.4.5.8	Documentar los detalles de los incidentes.	Los detalles de un incidente identificado se documentarán para registrar el incidente, la respuesta, las lecciones aprendidas y cualquier acción tomada para modificar el CSMS a la luz de este incidente.

4.3.4.5.9	Comunicar los detalles del incidente.	Los detalles documentados de un incidente se comunicarán a todas las organizaciones apropiadas (es decir, gestión, TI, seguridad de procesos, automatización y control de ingeniería, seguridad y fabricación) de manera oportuna.
4.3.4.5.10	Abordar los problemas y corregir los descubiertos	La organización debe contar con una metodología de negocios para abordar los problemas descubiertos y garantizar que se corrijan.
4.3.4.5.11	Realizar simulacros	Se deben realizar simulacros para evaluar el programa de respuesta a incidentes de manera rutinaria.

4.4 Categoría: Monitoreo y mejora del CSMS.

4.4.1 Descripción de la categoría.

La tercera categoría principal del CSMS se titula Supervisión y mejora del CSMS . Se trata de asegurar que tanto los CSMS se está utilizando y también la revisión de los CSMS sí mismo para la eficacia. La Figura 6 muestra una representación gráfica de los dos elementos en la categoría:

· Conformidad.
· Revisar, mejorar y mantener el CSMS.

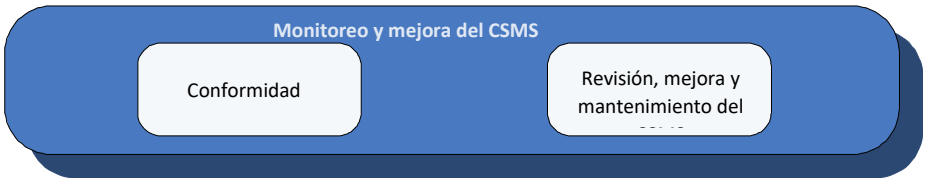

Figura 6 - Vista gráfica de la categoría: Monitoreo y mejora del CSMS

4.4.2 Elemento: Conformidad. Objetivo:

Asegúrese de que se siga el CSMS desarrollado para una organización.

Descripción:

La conformidad con un CSMS significa que la organización se adhiere a sus políticas establecidas, ejecuta los procedimientos en el momento correcto y produce los informes apropiados para permitir una revisión futura.

Razón fundamental:

Independientemente de la calidad de un CSMS, si no se usa, no agrega ningún valor a la organización y no ayuda a reducir el riesgo.

Requisitos:

Tabla 18 - Conformidad: requisitos.

Descripción		Requisito
4.4.2.1	Especificar la metodología del proceso de auditoría.	El programa de auditoría especificará la metodología del proceso de auditoría.
4.4.2.2	Realizar auditorías periódicas de IACS	Valide que el IACS se ajusta al CSMS. El CSMS incluirá auditorías periódicas del IACS, para validar que las políticas y procedimientos de seguridad estén funcionando según lo previsto y cumplan los objetivos de seguridad para la zona.
4.4.2.3	Establecer métricas de conformidad	La organización debe definir indicadores de desempeño y criterios de éxito, que se utilizan para monitorear la conformidad con el CSMS. Los resultados de cada auditoría periódica deben expresarse en forma de rendimiento frente a estas métricas para mostrar el rendimiento y las tendencias de seguridad.
4.4.2.4	Establecer una trazabilidad de documentos de auditorías	Se desarrollará una lista de documentos e informes necesarios para establecer una trazabilidad de auditoría.
4.4.2.5	Definir medidas disciplinarias por incumplimiento	La organización debe indicar qué significa la no conformidad con el CSMS, y también se deben definir las medidas disciplinarias relacionadas.
4.4.2.6	Garantizar la competencia de los auditores.	Se debe especificar la competencia requerida para auditar los sistemas específicos que están dentro del alcance. El nivel de independencia requerido debe determinarse como parte de la gestión del sistema.

4.4.3 Elemento: Revisar, mejorar y mantener el CSMS. Objetivo:

Asegúrese de que el CSMS continúe cumpliendo sus objetivos con el tiempo.

Descripción:

Revisar, mejorar y mantener el CSMS establece una supervisión continua del sistema de gestión para verificar que funcione de manera efectiva y gestionar los cambios requeridos en el CSMS a lo largo del tiempo.

Razón fundamental:

Se requiere una revisión y monitoreo para que el CSMS siga siendo efectivo, ya que el sistema responderá a los cambios en las amenazas, vulnerabilidades y consecuencias internas y externas, así como a los cambios en la tolerancia al riesgo, los requisitos legales y la evolución de los enfoques técnicos y no técnicos para la mitigación de riesgos.

Requisitos:

Tabla 19 - Revisar, mejorar y mantener el CSMS: requisitos.

Descripción	Requisito

4.4.3.1	Asignar una organización para administrar e implementar cambios en el CSMS	Se debe asignar una organización para administrar y coordinar el ajuste y la implementación de los cambios del CSMS y utilizar un método definido para realizar e implementar cambios.
4.4.3.2	Evaluar el CSMS periódicamente	La organización administradora evaluará periódicamente el CSMS, para garantizar que se cumplan los objetivos de seguridad.
4.4.3.3	Establecer desencadenantes para evaluar CSMS	La organización debería establecer una lista de desencadenantes con umbrales establecidos, lo que resultaría en una revisión de los elementos relacionados del CSMS y tal vez un cambio. Estos factores desencadenantes incluyen, como mínimo: la ocurrencia de incidentes de seguridad graves, cambios legales y reglamentarios, cambios en el riesgo y cambios importantes en el IACS. Los umbrales deben basarse en la tolerancia al riesgo de la organización.
4.4.3.4	Identificar e implementar acciones correctivas y preventivas.	La organización debe identificar e implementar acciones correctivas y preventivas apropiadas que modifiquen el CSMS para cumplir con los objetivos de seguridad.
4.4.3.5	Revisar la tolerancia al riesgo	Se debe iniciar una revisión de la tolerancia de la organización al riesgo cuando hay cambios importantes en la organización, la tecnología, los objetivos comerciales, los negocios internos y los eventos externos, incluidas las amenazas identificadas y los cambios en el clima social.
4.4.3.6	Monitorear y evaluar las estrategias de CSMS de la industria.	Los propietarios del sistema de gestión deben monitorear la industria para conocer las mejores prácticas de CSMS para la evaluación y mitigación de riesgos y evaluar su aplicabilidad.
4.4.3.7	Monitorear y evaluar la legislación aplicable relevante a la seguridad cibernética.	La organización debe identificar la legislación aplicable y cambiante relevante para la seguridad cibernética.
4.4.3.8	Solicite e informe los comentarios de los empleados sobre sugerencias de seguridad	Los comentarios de los empleados sobre las sugerencias de seguridad deben buscarse activamente e informarse a la alta gerencia, según corresponda, sobre las deficiencias y oportunidades de desempeño.

Anexo A
(informativo)
Orientación para desarrollar los elementos de un CSMS.

A.1 Descripción general.

Este anexo proporciona orientación informativa al lector sobre cómo desarrollar un CSMS que cumpla con los requisitos especificados en la Cláusula 4. La guía presentada aquí proporciona un marco de sistema de gestión general que permite a las organizaciones que adoptan el CSMS adaptarlo a sus propias necesidades específicas. Debe considerarse como un punto de partida o línea de base para un CSMS. No todas las pautas pueden ser aplicables y, dependiendo de la aplicación, la organización puede requerir más seguridad de la que se presenta. Tampoco está destinado a ser un proceso paso a paso, como se indicó anteriormente en 4.1.

Este anexo está organizado con las mismas categorías, grupos de elementos y elementos que los enumerados en la Cláusula 4 (ver Figura A.1). Cada elemento en este anexo usa la siguiente organización:

- Descripción del elemento: una descripción básica del tema.
- Información específica del elemento: una o más subcláusulas que proporcionan orientación detallada sobre este elemento. Su estructura y contenido es específico del elemento.
- Prácticas de apoyo:
    - Prácticas básicas: recomendaciones para que las organizaciones alcancen un nivel básico de seguridad cibernética. Estas prácticas se convierten en los componentes básicos de los requisitos para cada elemento.
    - Prácticas adicionales: prácticas de seguridad innovadoras utilizadas por algunas organizaciones para mejorar aún más la seguridad cibernética;
- Recursos utilizados: fuentes de información adicional, así como documentos referenciados (además del documento actual).

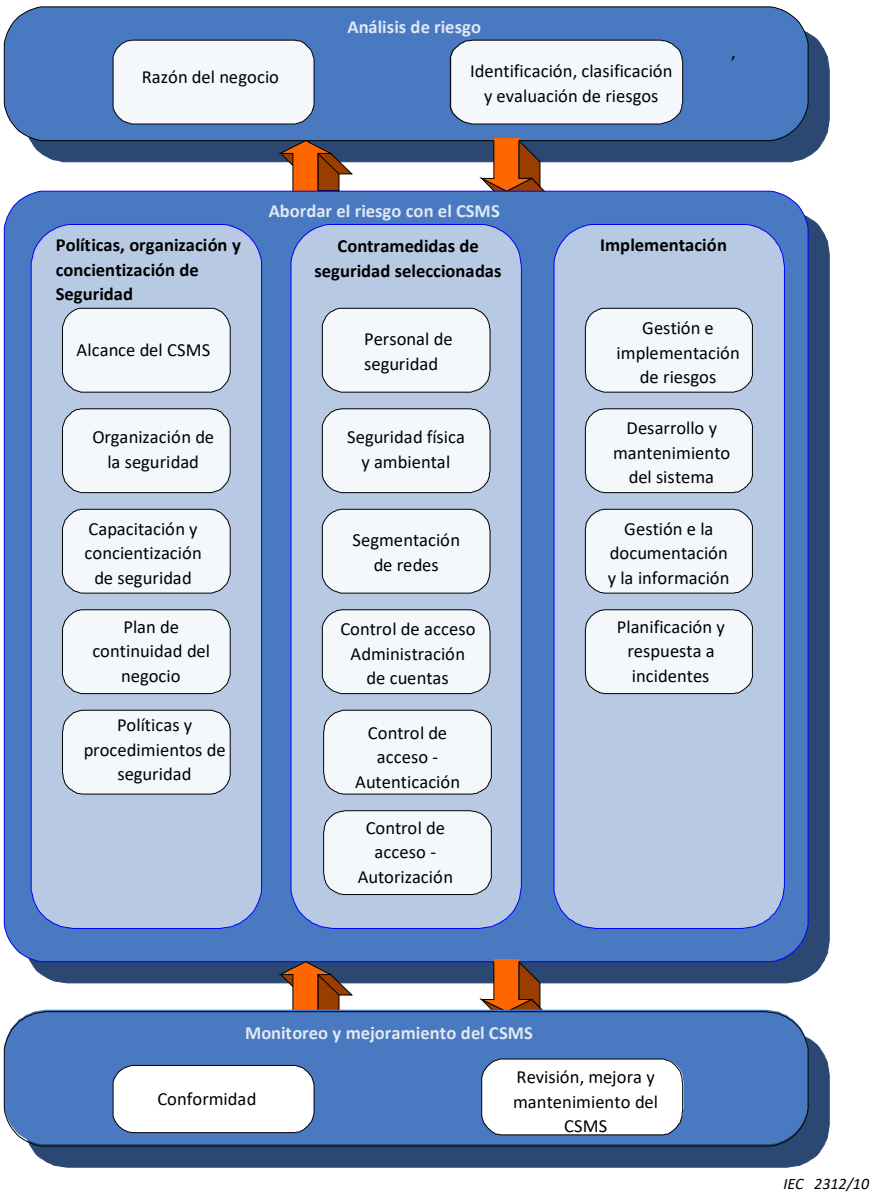

Figura A.1 - Vista gráfica de elementos de un sistema de gestión de seguridad cibernética

A.2 Categoría: Análisis de riesgos.

A.2.1 Descripción de la categoría.

La primera categoría principal del CSMS es el análisis de riesgos. Esta categoría analiza gran parte de la información de fondo que se incorpora a muchos de los otros elementos del CSMS. La Figura A.2 muestra los dos elementos que forman parte de la categoría:

- Justificación del negocio.

· Identificación, clasificación y evaluación de riesgos.

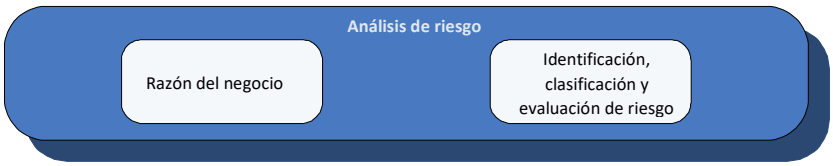

Figura A.2 - Vista gráfica de la categoría: Análisis de riesgos.

A.2.2 Elemento: justificación del negocio.

A.2.2.1 Descripción del elemento.

Este elemento establece que la organización conoce y comprende la importancia de la seguridad cibernética para la tecnología de la información tal como se utiliza en IACS. Esta comprensión se basa en la comprensión de los roles que desempeña la tecnología de la información en la misión de la organización, los riesgos asociados a esta misión y el costo y otros impactos comerciales de mitigar este riesgo.

A.2.2.2 Riesgo de seguridad cibernética, justificación y argumentos del negocio.

El primer paso para implementar un programa de seguridad cibernética para IACS es desarrollar una lógica del negocio convincente con las necesidades únicas de la organización para abordar el riesgo cibernético. Una organización puede derivar la justificación de su CSMS para IACS y proyectos individuales como resultado de las políticas existentes relacionadas con la seguridad, de la gestión general de riesgos o el cumplimiento de los requisitos reglamentarios. Otras organizaciones pueden exigir que la justificación del negocio tome la forma de un caso comercial formal o informal para actividades de gestión de seguridad cibernética a fin de establecer que el costo de mitigar el riesgo cibernético se justifica por su beneficio financiero. Una justificación del negocio o un caso comercial para dar los primeros pasos para construir un CSMS dependerá de una evaluación del riesgo, generalmente a un nivel alto. Una vez que se reconoce el riesgo, una organización está lista para tomar las medidas adecuadas para mitigarlo. Un esfuerzo por realizar una evaluación de riesgos más sistemática y detallada (como se describe más adelante en esta norma) y las decisiones individuales sobre contramedidas, pueden requerir una justificación del negocio, posiblemente en forma de un caso comercial.

Una fundamentación del negocio capta las preocupaciones empresariales de la alta gerencia utilizando la experiencia de aquellos que ya enfrentan muchos de los mismos riesgos. Esta subcláusula trata los componentes clave de la lógica del negocio resultante y los recursos clave para ayudar a identificar esos componentes. Una justificación del negocio puede tener como alcance la justificación de una evaluación de riesgo detallada o de alto nivel, otros aspectos específicos de un CSMS completo como se describe aquí, o la implementación de una sola contramedida.

La experiencia ha demostrado que embarcarse en un programa de seguridad cibernética sin una justificación del negocio acordada a menudo resulta en una eventual pérdida de recursos del programa en favor de otros requisitos del negocio. Por lo general, estos otros requisitos del negocio tienen un beneficio comercial más directo y una lógica fácil de entender.

A.2.2.3 Componentes claves de la lógica empresarial.

Hay cuatro componentes claves de una justificación del negocio: consecuencias del negocio prioritarias, amenazas priorizadas, impacto del negocio anual estimado y costo de las contramedidas.

a) Consecuencias del negocio priorizadas.

La lista de posibles consecuencias comerciales debe resumirse en las consecuencias del negocio particulares que la alta gerencia encontrará más convincentes. Por ejemplo, una compañía de alimentos y bebidas que no maneja materiales tóxicos o inflamables y típicamente procesa su producto a temperaturas y presiones relativamente bajas podría no estar preocupada por el daño del equipo o el impacto ambiental, pero podría estar más preocupada por la pérdida de disponibilidad de producción y la degradación del producto, la calidad. La información aquí se basa en los historiales de incidentes pasados, así como en el conocimiento de cómo se usan realmente los IACS en el negocio y el posible impacto comercial que podrían causar cambios técnicos no autorizados. El cumplimiento normativo también podría ser una preocupación.

b) Amenazas priorizadas.

La lista de amenazas potenciales necesita ser refinada, si es posible, a aquellas amenazas que se consideran creíbles. Por ejemplo, una compañía de alimentos y bebidas podría no considerar que el terrorismo es una amenaza creíble, pero podría estar más preocupado por los virus y gusanos y los empleados descontentos. La idea aquí se basa principalmente en historias de incidentes pasados.

c) Impacto empresarial anual estimado.

Los elementos de mayor prioridad que se muestran en la lista de consecuencias para el negocio priorizadas deben analizarse para obtener una estimación del impacto para el negocio anual preferiblemente, pero no necesariamente, en términos financieros. Para el ejemplo de la compañía de alimentos y bebidas, puede haber experimentado un incidente de virus dentro de su red interna que la organización de seguridad de la información calculó como resultado de un costo financiero específico. Debido a que la red interna y la red de controles están interconectadas, es concebible que un virus que se origina en la red de controles pueda causar el mismo impacto para el negocio. La idea aquí se basa principalmente en historias de incidentes pasados. El cumplimiento normativo puede implicar sanciones financieras o comerciales específicas por incumplimiento.

d) Costo.

El costo estimado del esfuerzo humano y las contramedidas técnicas que la justificación del negocio pretende evidenciar.

NOTA Se requiere una estimación del impacto para el negocio en términos financieros y estimaciones de costos de contramedidas para crear un caso comercial, pero una justificación para el negocio exitosa no siempre puede incluir esta información.

Existen varios recursos de información para ayudar a formar esta lógica comercial: recursos externos en organizaciones comerciales y recursos internos en programas de gestión de riesgos relacionados o ingeniería y operaciones.

Los recursos externos en las organizaciones comerciales a menudo proporcionan consejos útiles sobre los factores que más influyeron en su gestión para apoyar sus esfuerzos y qué recursos dentro de sus organizaciones resultaron más útiles. Para diferentes industrias, estos factores pueden ser diferentes, pero puede haber similitudes en los roles que pueden desempeñar otros especialistas en gestión de riesgos.

Los recursos internos asociados con los esfuerzos de gestión de riesgos relacionados (es decir, seguridad de la información, riesgo HSE, seguridad física y continuidad del negocio) pueden proporcionar una asistencia tremenda en función de su experiencia con incidentes relacionados en la organización. Esta información es útil desde el punto de vista de priorizar las amenazas y estimar el impacto para el negocio. Estos recursos también pueden proporcionar información sobre qué gerentes se centran en tratar con qué riesgos y, por lo tanto, qué gerentes podrían ser los más apropiados o receptivos para servir como líderes en el tema.

Los recursos internos asociados con la ingeniería y las operaciones de sistemas de control pueden proporcionar información sobre los detalles de cómo los sistemas de control se utilizan realmente dentro de la organización. ¿Cómo se segregan típicamente las redes? ¿Cómo se diseñan típicamente los sistemas de combustión de alto riesgo o los sistemas instrumentados de seguridad (SIS)? ¿Qué contramedidas de seguridad ya se usan comúnmente? Teniendo en cuenta la historia de la organización con fusiones y adquisiciones, también es importante comprender cuán representativo puede ser cualquier sitio en particular de toda la unidad de negocio, región u organización en general.

Recuerde que, en las primeras etapas de la operación industrial, el enfoque principal será identificar uno o dos temas de alta prioridad que justifiquen el esfuerzo continuo. A medida que el programa de seguridad cibernética de IACS se desarrolla más, pueden aparecer otros elementos en la lista y las prioridades pueden cambiar, ya que la organización aplica una metodología de análisis de riesgos más rigurosa. Sin embargo, estos cambios no deberían restar valor al resultado de este esfuerzo original para justificar el inicio del programa.

A.2.2.4 Sugerencias de contenido para la justificación comercial de IACS.

Dentro de cada organización, el viaje para desarrollar un programa de seguridad cibernética eficaz para IACS comienza con personas que reconocen los riesgos que la organización está tomando y comienzan a articular estos riesgos internamente, no solo en términos técnicos, sino en términos del negocio que resuenan con la alta gerencia. Una justificación comercial no es una evaluación detallada del riesgo; es más bien una descripción de alto nivel de riesgos suficiente para justificar los próximos pasos planeados en la construcción de un CSMS. Puede ser tan breve o detallado como sea necesario para respaldar los procesos de decisión en la organización en particular.

Las consecuencias comerciales negativas de los ataques cibernéticos contra IACS pueden incluir lo siguiente:

- Reducción o pérdida de producción en un sitio o en varios sitios simultáneamente;
- Lesiones o muerte de empleados;
- Lesiones o muerte de personas en la comunidad;
- Daño al equipo;
- Daño ambiental;
- Violación de los requisitos reglamentarios;
- Contaminación del producto;
- Responsabilidades legales, penales o civiles;
- Pérdida de información patentada o confidencial;
- Pérdida de imagen de marca o confianza del cliente;

- Pérdida económica.

Al priorizar el riesgo de que ocurran estas consecuencias, también es importante tener en cuenta la posible fuente o amenaza que inicia un ataque cibernético y la probabilidad de que tal evento ocurra. Las amenazas cibernéticas pueden surgir de fuentes dentro o fuera de una organización; las amenazas pueden ser el resultado de acciones intencionales o no intencionales; y las amenazas pueden ser dirigidas a un objetivo específico o no dirigidas. Los incidentes de seguridad cibernética pueden ser el resultado de muchos tipos diferentes de agentes de amenazas, como los siguientes:

- Personas que buscan emociones, aficionados o alienados que adquieren una sensación de poder, control, autoimportancia y placer a través de la penetración exitosa de los sistemas informáticos, ya sea a través de ataques no dirigidos (virus y gusanos) o ataques dirigidos (piratería) para robar o destruir información o interrumpir las actividades de una organización.
- Empleados o contratistas descontentos que dañan los sistemas o roban información para vengarse o obtener ganancias.
- Empleados bien intencionados que inadvertidamente realizan cambios en el controlador o equipo operativo incorrectos.
- Empleados que rompen las políticas o procedimientos de calidad, seguridad o protección para satisfacer otras necesidades urgentes (por ejemplo, objetivos de producción).
- Los terroristas generalmente están motivados por creencias políticas para las cuales los ataques cibernéticos ofrecen el potencial de ataques de bajo costo, bajo riesgo, pero de alta ganancia, especialmente cuando están vinculados con ataques físicos coordinados.
- Ladrones profesionales (incluido el crimen organizado) que roban información para la venta.
- Las naciones o grupos adversarios que usan Internet como arma militar para la guerra cibernética para interrumpir las capacidades de comando, control y comunicación de un enemigo.

Los casos documentados proporcionan información sobre cómo y con qué frecuencia uno de estos agentes de amenazas logra infligir consecuencias comerciales negativas. La rápida adopción de nuevas tecnologías de red ha llevado al desarrollo de nuevas herramientas para permitir ataques cibernéticos. Con la falta de un sistema reconocido de notificación de incidentes accesible al público, será extremadamente difícil en el futuro cercano determinar una probabilidad cuantitativa de que ocurra cualquier tipo específico de evento. La probabilidad deberá evaluarse cualitativamente en función del historial interno de incidentes de una organización y en los pocos casos que se hayan documentado públicamente. Varios ejemplos de estos casos son:

- EJEMPLO 1 En enero de 2003, el gusano SQL Slammer se extendió rápidamente de una computadora a otra a través de Internet y dentro de redes privadas. Penetró en una red informática en la planta de energía nuclear Davis-Besse de Ohio y desactivó un sistema de monitoreo durante casi cinco horas, a pesar de la creencia del personal de la planta de que la red estaba protegida por un firewall. Ocurrió debido a una interconexión desprotegida entre la planta y las redes corporativas. El gusano SQL Slammer derribó la red SCADA crítica de una empresa de servicios públicos después de pasar de una red corporativa a la red de área local (LAN) del centro de control. Otra utilidad perdió su red Frame Relay utilizada para las comunicaciones y algunas plantas petroquímicas perdieron interfaces hombre-máquina (HMI) e historiadores de datos. Se desconectó un centro de llamadas del 911, se retrasaron y cancelaron los vuelos de las aerolíneas y se deshabilitaron los cajeros automáticos.
- EJEMPLO 2 Durante varios meses en 2001, un contratista descontento en Queensland, Australia, llevó a cabo una serie de ataques cibernéticos en un sistema computarizado de tratamiento de aguas residuales. Uno de estos ataques provocó el desvío de millones de galones de aguas residuales sin tratar hacia un río y parque local. Hubo 46 intrusiones antes de que el autor fuera arrestado.
- EJEMPLO 3 En septiembre de 2001, un adolescente supuestamente pirateó un servidor de computadora en el Puerto de Houston para atacar a una usuaria de una sala de chat luego de una discusión. Se afirmó que el adolescente tenía la intención de desconectar la computadora de la mujer bombardeándola con una gran cantidad de datos inútiles y que necesitaba usar otros

servidores para poder hacerlo. El ataque bombardeó la programación de sistemas informáticos en el octavo puerto más grande del mundo con miles de mensajes electrónicos. El servicio web del puerto, que contenía datos cruciales para el envío de pilotos, compañías de amarre y empresas de apoyo responsables de ayudar a los barcos a navegar dentro y fuera del puerto, quedó inaccesible.

La organización CERT ha estado monitoreando y rastreando el número de ataques que ocurren en sistemas conectados a Internet desde 1988. Ninguno de los incidentes reportados fue para sistemas de control. A partir de 2004, dejaron de rastrear la cantidad de ataques, debido a que la prevalencia de las herramientas de ataque automatizadas ha hecho que los ataques sean tan comunes que la cantidad de incidentes reportados proporciona poca información con respecto a la evaluación del alcance y el impacto de los ataques. En la Figura A.3 se muestra un gráfico de sus datos de incidentes para demostrar el dramático aumento que se ha producido en los últimos 15 años.

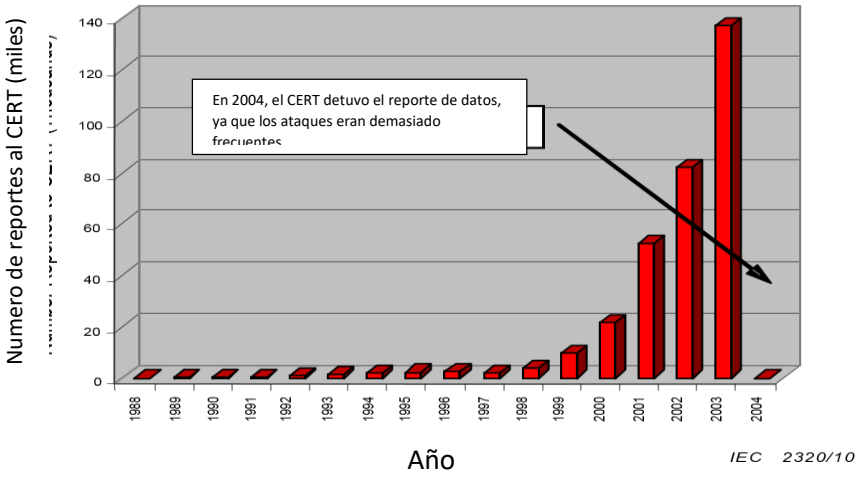

Figura A.3 - Ataques reportados en sistemas informáticos hasta 2004 (fuente: CERT)

A.2.2.5 Prácticas de apoyo.

A.2.2.5.1 Prácticas de referencia.

Las siguientes seis acciones son prácticas básicas:

a) Identificar y documentar los objetivos del negocio, los procesos comerciales críticos y los procesos críticos de tecnología de la información. Incluya IACS e interfaces con socios de la cadena de valor donde se transfiere, almacena o procesa información confidencial.

b) Identificar la dependencia del negocio de los sistemas de tecnología de la información. Clasifique la dependencia del negocio bajo, medio, alto o un sistema de clasificación alternativo.

c) Identificar varios escenarios de daños por la pérdida de confidencialidad, integridad o disponibilidad de información. Incluya la manipulación de IACS y las consecuencias de tales acciones para aquellas empresas que utilizan estos sistemas. Incluya HSE e integridad operacional y confiabilidad para los controladores de IACS. Capture los riesgos asociados con la cadena de valor y otros socios comerciales de terceros. Estos riesgos a menudo incluyen la pérdida o alteración de información sensible. Un ejemplo es la intercepción de información asociada con los envíos de productos de fabricación, incluidos los tipos de materiales, las cantidades, las rutas de envío, el modo de transporte y similares.
d) Desarrollar análisis de impacto empresarial para la seguridad de IACS.

e) Desarrollar análisis de impacto comercial para la cadena de valor u otro socio comercial externo.

f) Determinar el perfil de tolerancia al riesgo de la organización definido en términos de:

1) Seguridad del personal (lesiones graves o fatalidad);

2) Pérdida o impacto financiero, incluidas sanciones regulatorias;

3) Consecuencia ambiental / regulatoria;

4) Daño a la imagen de la empresa;

5) Impacto en la comunidad inversora;

6) Pérdida de base de clientes o confianza;

7) Impacto en la infraestructura.

NOTA La tolerancia al riesgo varía según el negocio. En pocas palabras, la tolerancia al riesgo de la organización es su umbral de dolor. La tolerancia al riesgo puede ser muy baja (por ejemplo, una sola lesión grave puede no ser aceptable y debe abordarse de inmediato) cuando se trata de la seguridad en la fabricación de la planta o puede ser muy alta (por ejemplo, en términos de pérdida de producción) si la organización tiene múltiples sitios de producción de un producto básico. El impacto financiero para una empresa puede no ser apropiado para otras empresas. Las organizaciones con múltiples negocios deben observar las interdependencias de un negocio sobre otro al determinar la tolerancia al riesgo.

Los gerentes de seguridad de TI generalmente estarán familiarizados con el perfil de tolerancia al riesgo de la organización para algunas, pero no todas, estas consecuencias. Otros gerentes responsables de administrar los riesgos asociados con las consecuencias de HSE estarán familiarizados con el perfil de tolerancia al riesgo de la organización en estas áreas. El perfil general de tolerancia al riesgo debe determinarse integrando la información de estas fuentes, así como las del entorno IACS.

A.2.2.5.2 Prácticas adicionales.

Las siguientes tres acciones son prácticas adicionales:

- Identificar y documentar los objetivos del negocio, los procesos comerciales críticos y los procesos críticos de TI. Este proceso se realiza mejor con una sección transversal de la organización que representa las áreas funcionales, así como las unidades de negocio de la empresa. Este grupo generalmente está constituido por un alto ejecutivo responsable de la organización de TI o por un equipo de liderazgo que incluye a otros altos ejecutivos de toda la organización. Esta carta incluye específicamente el riesgo asociado con IACS.

- Desarrollar un análisis de impacto empresarial que describa los problemas y las consecuencias de la inacción y los beneficios de la acción. En la medida de lo posible, estas acciones se cuantifican en términos de impactos financieros (es decir, pérdida de ventas o multas), impactos en el mercado (es decir, pérdida de confianza o imagen pública), así como impactos de HSE (es decir, liberación ambiental, daño al equipo y pérdida de vidas). Especialmente cuando se consideran consecuencias como la imagen pública, es importante comprender que un incidente debido a una unidad de negocios en particular puede afectar a la organización en su conjunto.

- Documentar y aprobar (por el nivel apropiado de gestión) los riesgos fuera del alcance del CSMS.

A.2.2.6 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [24], [26], [27], [30], [42].

A.2.3 Elemento: identificación de riesgos, clasificación y evaluación.

A.2.3.1 Descripción del elemento.

Las organizaciones protegen su capacidad de realizar su misión identificando, priorizando y analizando sistemáticamente las posibles amenazas de seguridad, vulnerabilidades y consecuencias utilizando metodologías aceptadas. El riesgo se define formalmente como una expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad particular con una consecuencia particular (ver IEC / TS 62443 - 1 - 1). Como se describe en el elemento relacionado Gestión e implementación de riesgos (ver A.3.4.2), una organización define su tolerancia al riesgo en términos de las características de las amenazas, vulnerabilidades y posibles consecuencias que identifica. Luego, la organización implementa esta decisión de tolerancia al riesgo tomando medidas, donde se indica reducir la probabilidad de que ocurra una amenaza de seguridad al mitigar las vulnerabilidades y / o reducir las consecuencias en caso de que la amenaza de seguridad se realice.

A.2.3.2 Riesgo cibernético para IACS.

El enfoque de gestión de riesgos descrito en A.2.2 se aplica en general a todos los tipos de riesgos cibernéticos, así como a otros tipos de riesgos. Esta discusión trata sobre los aspectos únicos del análisis del riesgo cibernético para IACS.

Aunque varias industrias pueden encontrar ciertos tipos de impacto sobre el negocio de mayor preocupación y pueden sentir que ciertos tipos de amenazas son más probables, todas las industrias que usan IACS deberían preocuparse de que estén entrando en un nuevo entorno de riesgo. Al mismo tiempo que IACS ha adoptado sistemas operativos de TI comerciales y tecnologías de red y los usuarios han interconectado sus redes privadas con sus redes IACS, la cantidad de amenazas también ha aumentado considerablemente. Existen riesgos asociados con la información tradicional (electrónica o en papel), aplicaciones y sistemas de TI clásicos, IACS, socios comerciales, empresas conjuntas, socios de subcontratación y similares.

Los riesgos para los activos de TI tradicionales se centran en la confidencialidad, integridad y disponibilidad de la información. Los riesgos en IACS son diferentes, ya que los controladores se centran más en los factores de HSE y la confiabilidad operativa, además de la protección tradicional de la confidencialidad, integridad y disponibilidad de la información. En IACS, las prioridades generalmente se invierten con un enfoque en la disponibilidad, integridad y confidencialidad en ese orden. Esto significa que la evaluación del riesgo cibernético para IACS debe coordinarse con la seguridad física y HSE, siempre que sea práctico. Algunas organizaciones integran plenamente los esfuerzos de evaluación de riesgos relacionados con todas estas áreas. Los riesgos de la contratación externa, contratistas externos u otros socios en la cadena de valor de fabricación incluyen información confidencial transmitida, almacenada o procesada. La integración de estos socios comerciales en las operaciones de una organización potencialmente permite el acceso involuntario a los sistemas de la compañía.

En prácticamente todos estos casos, las operaciones y tecnologías industriales relacionadas con la seguridad desarrolladas para aplicaciones de TI clásicas no se han implementado para IACS en parte debido a la ignorancia, pero en parte debido a restricciones válidas que no existen en las aplicaciones de TI clásicas. El objetivo de esta norma es abordar ambos problemas.

A.2.3.3 Proceso de evaluación de riesgos.

A.2.3.3.1 General.

Se requiere una descripción general de los riesgos para establecer las razones del negocio de un CSMS. Las prioridades más detalladas que aborda este sistema se determinan en función de una metodología que considera sistemáticamente el riesgo a un nivel de granularidad mayor que el que se evalúa habitualmente para establecer una justificación del negocio inicial.

A.2.3.3.2 Evaluación de riesgos y evaluación de vulnerabilidad.

En la literatura general, los términos evaluación de vulnerabilidad y evaluación de riesgo a veces se usan indistintamente. Estos dos tipos de análisis se pueden distinguir de acuerdo con las definiciones de vulnerabilidad y riesgo en esta norma. Recuerde que una vulnerabilidad se define como una falla o debilidad en el diseño, implementación u operación y gestión de un sistema que podría explotarse para violar la integridad del sistema o la política de seguridad (ver IEC / TS 62443 - 1 - 1). Como ejemplo, la observación de que las contraseñas en un centro de control rara vez cambian es un ejemplo de una vulnerabilidad que se identificaría en una evaluación de vulnerabilidad. Puede haber varios riesgos asociados con esta vulnerabilidad, por ejemplo:

- Una baja probabilidad de que la contraseña se conozca bien en la planta con el tiempo y que un empleado legítimo que no esté capacitado para las operaciones del sistema de control use la contraseña mientras se presenta para resolver un problema y causa una pérdida de producción durante varias horas debido a errores de entrada.

- Una baja probabilidad de que un ex empleado descontento rompa con éxito las defensas del firewall corporativo para acceder a la red del sistema de control de forma remota, inicie sesión en una HMI y tome medidas deliberadamente que pueden causar una pérdida de producción durante varios días.

Por lo tanto, como estos términos se usan en esta norma, la evaluación de riesgos tiene como resultado un conjunto de riesgos y una evaluación de vulnerabilidad tiene como resultado un conjunto de vulnerabilidades, que aún no se han analizado en términos de los riesgos que crean. De esta manera, una evaluación de vulnerabilidad es un insumo para una evaluación de riesgos. Tenga en cuenta que algunas metodologías existentes tituladas métodos de evaluación de vulnerabilidad incluyen conceptos de riesgo y otras no.

Volviendo al ejemplo anterior de la contraseña de la sala de control, está claro que también existen riesgos involucrados en cambiar periódicamente la contraseña del sistema de control, por ejemplo, una baja probabilidad de que un operador no recuerde una nueva contraseña en una situación de emergencia y será, no se puede iniciar sesión para resolver la situación, lo que resulta en daños ambientales colaterales graves. La compensación entre el riesgo abordado por una contramedida y el riesgo introducido por una contramedida como en este caso, se discute en el elemento de Gestión de Riesgos e Implementación de esta norma (ver A.3.4.2).

A.2.3.3.3 Evaluación de riesgo detallada y de alto nivel.

La evaluación de riesgos puede llevarse a cabo en varios niveles. Esta norma requiere una evaluación de riesgos en dos niveles de detalle, denominada evaluación de riesgos de alto nivel y evaluación detallada de riesgos.

La evaluación de riesgos de alto nivel examina cuál podría ser el impacto de los tipos generales de vulnerabilidades de seguridad cibernética y la probabilidad de que una amenaza pueda ejercer estas

vulnerabilidades, pero no considera casos particulares de estas vulnerabilidades o contramedidas. Así, los ejemplos de riesgos identificados en una evaluación de riesgos de alto nivel podrían ser:

- Una probabilidad media de que ocurra una infestación de malware y provoque una congestión de la red de control y, por lo tanto, una falta de visibilidad del estado del proceso industrial en la sala de control, lo que resulta en un posible cierre de emergencia y los costos resultantes.

- Una baja probabilidad de que un contratista con conexiones criminales y con acceso físico a los medios de la red del sistema de control toque estos medios y modifique con éxito los comandos de control de una manera que cause daños a la instalación.

Se requiere una evaluación de alto nivel porque la experiencia ha demostrado que, si las organizaciones comienzan observando vulnerabilidades detalladas, pierden el panorama general del riesgo cibernético y les resulta difícil determinar dónde enfocar sus esfuerzos de seguridad cibernética. El examen de los riesgos a un alto nivel puede ayudar a centrar el esfuerzo en evaluaciones detalladas de vulnerabilidad. La evaluación de alto nivel generalmente puede cubrir todas las redes de control de una organización, posiblemente dividiéndolas en grupos que comparten características comunes. Es posible que los recursos no estén disponibles para cubrir todos los IACS en el nivel detallado.

Una evaluación de riesgo detallada, como se define para esta norma, está respaldada por una evaluación detallada de vulnerabilidades que incluye el examen de las contramedidas técnicas existentes, el cumplimiento de los procedimientos de administración de cuentas, el parche y el estado del puerto abierto por host individual en una red de un sistema de control específico, características de conectividad como la separación y configuración del firewall. Por lo tanto, un resultado de ejemplo de una evaluación de riesgo detallada podría ser:

- La conexión directa de las estaciones de trabajo de ingeniería de procesos tanto a la red corporativa como a la red del sistema de control, evitando el firewall interno de la red de control, contribuye al riesgo de infección de malware en la red de control. En combinación con la falta de protección antivirus en el 50% de los hosts en la red de control, da como resultado una probabilidad media de un incidente de congestión de red provocada por virus que causa una falta de visibilidad del estado de la operación industrial en la sala de control y resultando en un posible cierre de emergencia y los costos resultantes.

- Todos los medios de red del sistema de control (por ejemplo, las direcciones 192.168.3.x) y las conexiones a otras redes están físicamente protegidas por paredes, techos o pisos, o en habitaciones cerradas accesibles para tres administradores de red autorizados del sistema de control. Por lo tanto, el riesgo de un intento exitoso de aprovechar este medio es bajo.

Estos resultados detallados de la evaluación de riesgos respaldan los resultados relacionados de una evaluación de alto nivel de acuerdo con los ejemplos relacionados anteriormente. Sin embargo, la evaluación detallada del riesgo puede en muchos casos determinar que los riesgos son más bajos o más altos de lo que se sospecha en la evaluación de alto nivel. La evaluación detallada de riesgos también puede descubrir riesgos no considerados en la evaluación de alto nivel. Finalmente, dado que la evaluación detallada identifica vulnerabilidades específicas, proporciona instrucciones sobre cómo una organización podría abordar los riesgos que se consideran inaceptables.

A.2.3.3.4 Tipos de metodologías de evaluación de riesgos.

A.2.3.3.4.1 General.

Hay una variedad de métodos de evaluación de riesgos que han sido desarrollados y comercializados por diferentes organizaciones. En general, estos pueden clasificarse de acuerdo con dos factores: cómo caracterizan los riesgos individuales (cualitativa versus cuantitativamente) y cómo estructuran el ejercicio de identificación de riesgos (basado en escenarios versus basado en activos).

A.2.3.3.4.2 Cualitativo versus cuantitativo.

La evaluación de riesgos cualitativa generalmente se basa en el aporte de empleados experimentados y / o expertos para proporcionar información sobre la probabilidad y la gravedad de las amenazas específicas que afectan a activos específicos. Además, los diferentes niveles de probabilidad y severidad se identifican por clases generales tales como probabilidades altas, medias y bajas en lugar de probabilidades específicas o impactos económicos. Se prefiere la evaluación cualitativa del riesgo cuando falta información confiable sobre la probabilidad de que amenazas específicas afecten a activos específicos o estimen el impacto general del daño a activos específicos.

La evaluación cuantitativa del riesgo generalmente se basa en conjuntos de datos extensos que documentan la velocidad a la que se produce el daño a los activos en función de la exposición a combinaciones definidas de amenazas y vulnerabilidades. Si esta información está disponible, puede proporcionar estimaciones de riesgo más precisas que los métodos de evaluación de riesgos cualitativos. Debido a la reciente exposición de IACS a las amenazas de seguridad cibernética, la poca frecuencia relativa en que ocurren los incidentes y la naturaleza de las amenazas que evoluciona rápidamente, todavía no existen conjuntos de datos extensos para ayudar en la evaluación de las amenazas de seguridad cibernética a IACS. En esta etapa, la evaluación cualitativa de riesgos es el método preferido para evaluar estos riesgos.

A.2.3.3.4.3 Basado en escenarios versus basado en activos.

Al realizar una evaluación de riesgos, generalmente es útil enfocar los pensamientos de los participantes en una de dos líneas: los escenarios por los cuales las amenazas aprovechan las vulnerabilidades para impactar los activos o los activos mismos. El enfoque basado en escenarios tiende a aprovechar la experiencia con incidentes reales o casi incidentes. Sin embargo, el enfoque puede no penetrar para descubrir amenazas o vulnerabilidades a activos sensibles que no han sido amenazados previamente. El enfoque basado en activos tiende a aprovechar el conocimiento de los sistemas y métodos de trabajo de una organización y activos particulares cuyo compromiso conduciría a un alto impacto económico. Sin embargo, este enfoque puede no penetrar para descubrir tipos de amenazas o vulnerabilidades que pondrían en peligro estos activos o escenarios que involucran a más de un activo. Cualquiera que sea el enfoque general utilizado, se recomienda incluir algún aspecto del otro enfoque para proporcionar una evaluación de riesgos más exhaustiva.

EJEMPLO Una organización que ha identificado activos como dispositivos, aplicaciones y datos se considera un ejemplo que integra escenarios y métodos basados en activos. En el siguiente paso, la organización enumera los posibles escenarios relacionados con estos activos y determina las consecuencias de la siguiente manera. Los escenarios de aplicación son muy similares a los escenarios de dispositivo que se muestran.

a) Escenarios de dispositivos.

   1) Escenario: usuario no autorizado que accede localmente a un dispositivo IACS.

      ¿Cuál es la consecuencia de que alguien se acerque al dispositivo y realice las tareas permitidas en este dispositivo?

   2) Escenario: acceso remoto de un dispositivo IACS por un usuario no autorizado

¿Cuál es la consecuencia de que un usuario no a

utorizado obtenga acceso remoto a este dispositivo y realice cualquiera de las tareas permitidas por este dispositivo?

3) Escenario: dispositivo IACS deshabilitado o destruido.

¿Cuál es la consecuencia de un incidente cibernético que impide que el dispositivo realice todas o un subconjunto de sus funciones normales?

b) escenarios de datos.

1) Escenario: robo de datos IACS.

¿Cuál es la consecuencia de que alguien robe este conjunto de datos?

· ¿El conjunto de datos tiene un alto valor de propiedad intelectual?

· ¿Es el conjunto de datos de valor comercial para un competidor?

· Si se publica, ¿el conjunto de datos sería una vergüenza para la organización?

· ¿Se requiere el conjunto de datos para el cumplimiento normativo?

· ¿Están los datos establecidos bajo una orden de retención por litigio?

2) Escenario: corrupción de datos IACS

¿Cuál es la consecuencia potencial si:

· ¿El conjunto de datos fue interceptado y cambiado entre el origen y el destino?

· ¿El conjunto de datos estaba dañado en la fuente?

· ¿Se requiere el conjunto de datos para el cumplimiento normativo?

· ¿Están los datos establecidos bajo una orden de retención por litigio?

3) Escenario: denegación de servicio de datos IACS

¿Cuál es la consecuencia si el usuario de los datos no pudo acceder al conjunto de datos IACS?

NOTA: Un grupo puede llevar a cabo una evaluación de riesgos basada en escenarios comenzando por descripciones de escenarios de incidentes y luego determinando las consecuencias del escenario, como se muestra en este ejemplo, o comenzar creando una lista de consecuencias no deseadas primero, y luego trabajar hacia atrás para desarrollar posibles escenarios de incidentes. eso podría crear estas consecuencias. También se puede usar una combinación de estos enfoques.

A.2.3.3.5 Seleccionar la metodología de evaluación de riesgos.

La selección de la metodología de evaluación de riesgos adecuada para una organización es muy subjetiva, basada en una serie de cuestiones. Muchas de estas metodologías están disponibles comercialmente. Algunos de estos están disponibles sin cargo; otros requieren una licencia para su uso. Evaluar estas metodologías para encontrar la más útil para una organización puede ser una tarea difícil. Común a la mayoría

de las metodologías es la premisa de que el riesgo es una combinación de la probabilidad de que ocurra un evento y las consecuencias de ese evento.

La complicación es cómo asignar números cuantitativos a la probabilidad, que generalmente se expresa de manera similar a una probabilidad. La experiencia de la industria con la seguridad de procesos y accidentes proporciona una gran cantidad de datos históricos cuantitativos sobre los cuales basar los valores de probabilidad. Pero identificar los números apropiados para la probabilidad de un incidente cibernético específico no es fácil, no solo por la falta de datos históricos, sino también porque el pasado puede no predecir el futuro una vez que los atacantes potenciales conocen una vulnerabilidad. Debido a esta complicación, muchas empresas y asociaciones comerciales han optado por desarrollar su propia metodología para abordar las preocupaciones de amenaza y vulnerabilidad de importancia específica para su empresa de una manera consistente con su cultura corporativa. También por esta razón, esta norma utiliza el término probabilidad, que tiene que ver con estimaciones de las capacidades e intenciones humanas, en lugar del término probabilidad esperada, que tiene que ver con la ocurrencia de eventos naturales imparciales por la interferencia humana.

Algunas metodologías apoyan bien la evaluación de riesgos de alto nivel. Algunos respaldan bien la evaluación detallada del riesgo, al permitir la entrada de los resultados de la evaluación de vulnerabilidad y también pueden proporcionar directamente orientación para la evaluación detallada de vulnerabilidad asociada. Una organización encontrará eficaz utilizar una metodología que respalde de manera coherente tanto la evaluación de riesgos detallada como la de alto nivel.

EJEMPLO Un ejemplo de una asociación comercial que ayuda con la tarea de seleccionar la metodología correcta, el Centro de Tecnología de la Información Química del Consejo Químico Americano (ChemITC) ha publicado un documento titulado "Informe sobre Metodologías de Evaluación de Vulnerabilidad de Seguridad Cibernética Versión 2.0" [27] Este documento examina varios elementos de once metodologías diferentes y los compara con un conjunto de criterios importantes en una metodología de riesgo de seguridad cibernética de propósito general para evaluar sistemas de TI de negocios, IACS y sistemas de cadena de valor. El informe ofrece algunos consejos sólidos para seleccionar una metodología. Una parte de la guía se incluye a continuación con el permiso de CSCSP.

a) Paso 1 – Filtro.

El primer paso es revisar la descripción general de las metodologías seleccionadas. El objetivo de este paso es filtrar las metodologías de interés en función de criterios como la facilidad de uso, la complejidad, el alcance, los requisitos de recursos y el tipo de metodología (véase [27], Apéndice IV).

b) **Paso 2 – Seleccione.**

Después de identificar las metodologías, seleccione las metodologías que se ajusten a las necesidades de la organización (ver [27], Anexo II). El Anexo II identifica los criterios particulares que se utilizaron para evaluar la metodología. Los criterios enumerados allí abordan un espacio de TI mucho más grande más allá de IACS. Puede ser que sea necesaria una metodología para abordar solo un subconjunto de los criterios utilizados en el estudio ChemITC. Entender la diferencia entre las necesidades de la organización y los criterios de evaluación será útil al revisar las sinopsis de las diferentes metodologías. Luego, revise las sinopsis correspondientes para obtener información más detallada para asistencia en la elección de una metodología informada (ver [27], Apéndice V).

La sinopsis de cada metodología aborda los siguientes temas:

- Metodología de evaluación de vulnerabilidad de seguridad cibernética,
- Revisores,

· Fecha,

· Dirección web,

· Observaciones generales,

· Puntos fuertes en comparación con los criterios de evaluación comunes,

· Brechas en comparación con los criterios comunes de evaluación,

· Cómo podría usarse esta metodología,

· Limitaciones en el uso de metodología, y

· revisiones sugeridas.

c) **Paso 3 - Validar (opcional)**

Si existe alguna incertidumbre o dificultad para elegir la metodología, revise las hojas de cálculo de criterios técnicos que se muestran en el documento de referencia para la metodología para validar las elecciones de la organización (ver [27] Anexo II). La hoja de cálculo de criterios técnicos existe para cada metodología. Este paso es opcional porque simplemente proporciona datos de evaluación aún más específicos.

d) **Paso 4 - Adquirir la metodología seleccionada.**

Después de reducir la selección de metodología a una, obtenga la metodología del proveedor. Las direcciones web proporcionadas en la bibliografía son un buen punto de partida.

A.2.3.3.6 Evaluación de riesgos de alto nivel: identificación de riesgos.

Una vez que se ha identificado un conjunto de partes interesadas y se les ha proporcionado capacitación sobre la naturaleza de IACS, realizarán una evaluación de riesgos de alto nivel siguiendo la metodología seleccionada por la organización. Este proceso de evaluación aclara la naturaleza de los riesgos individuales para la organización que surgen del uso de IACS. Esta claridad es necesaria para seleccionar en última instancia las contramedidas más rentables que se diseñarán o implementarán y para ayudar a justificar los costos de su implementación. Si bien esta tarea es el primer paso de una evaluación de riesgos, no es una evaluación detallada de vulnerabilidad o amenaza. Por lo general, implica una sesión de análisis de riesgos para recopilar información de todas las partes interesadas y aprovecha las consecuencias del negocio de alto nivel que pueden haberse identificado en la justificación del negocio.

El documento entregable de la sesión de análisis de riesgos es una lista de escenarios que describen cómo una amenaza en particular podría aprovechar un tipo particular de vulnerabilidad y dañar activos particulares, lo que resulta en identificar consecuencias negativas para el negocio. La misma sesión también puede abordar la apreciación del nivel de consecuencia y la priorización por nivel de tolerancia al riesgo.

Las partes interesadas, que tienen experiencia con las aplicaciones de IACS en las unidades de negocios y los responsables de la gestión de riesgos relacionados, deben participar en el esfuerzo de evaluación de riesgos para aprovechar su experiencia y conocimientos.

Para hacer el uso más eficiente del tiempo de los participantes, normalmente es necesario programar entre medio día y un día completo para llevar a cabo la sesión de análisis de riesgos con la asistencia de todos los participantes interesados. Hay dos fases de esta sesión de análisis de riesgos: información de antecedentes e identificación de riesgos.

Independientemente del método de evaluación de riesgos que se utilice, también es importante proporcionar a los participantes en la sesión de análisis de riesgos, la información de respaldo adecuada antes de comenzar a identificar los riesgos. La información de antecedentes típica incluye una descripción general de los fundamentos y el estatuto del negocio, una descripción general de las arquitecturas y funciones de IACS y una descripción general de tipos específicos de incidentes que ocurrieron dentro de la organización o incidentes publicitados que ocurrieron en otras organizaciones.

Para que la sesión sea exitosa, también es importante que los participantes comprendan las definiciones de trabajo para riesgos y vulnerabilidades; de lo contrario, es probable que la sesión identifique vulnerabilidades, pero puede que no logre identificar riesgos. Los ejemplos son útiles para este propósito. Por lo tanto, como ejemplo, la vulnerabilidad podría ser una autenticación débil en la HMI del sistema de control. La amenaza relacionada podría ser que un empleado con experiencia insuficiente pueda operar la HMI sin supervisión y establezca parámetros inseguros. La consecuencia podría ser una interrupción de la producción debido al ejercicio de controles de seguridad. Es un error común que una organización enumere las vulnerabilidades cibernéticas y luego proceda a mitigarlas.

A.2.3.3.7 Evaluación de riesgos de alto nivel: clasificación de riesgos.

A.2.3.3.7.1 General.

La lista de escenarios producidos como resultado de la sesión de análisis de riesgos describe una serie de riesgos diferentes que las amenazas a IACS plantean a las organizaciones. Una de las tareas de la gestión corporativa es gestionar todos los riesgos para sus organizaciones. Para facilitar este esfuerzo, los riesgos deben ser identificados y priorizados. Esta subcláusula describe los tres pasos necesarios para desarrollar un marco para priorizar los riesgos individuales de modo que las acciones correctivas apropiadas puedan justificarse.

A.2.3.3.7.2 La ecuación de riesgo.

Antes de describir el marco para la priorización y calibración de riesgos, es importante comprender un concepto básico de análisis de riesgos (por ejemplo, la ecuación de riesgos).

La probabilidad de que ocurra un evento tiene en cuenta tanto la probabilidad de que se produzca una amenaza que podría causar una acción como la probabilidad de que la vulnerabilidad explote permitiendo la acción. Por ejemplo, para que un virus paralice una red, primero necesita llegar a la red y luego vencer los controles antivirus en la red. Se expresa de manera similar a una probabilidad, entonces:

$$\textit{Probabilidad}_{\textit{Ocurrir Evento}} = \textit{Probabilidad}_{\textit{Amenaza Realizada}} \times \textit{Probabilidad}_{\textit{Vulnerabilidad Explotada}} \quad \text{(A.1)}$$

Como se discutió anteriormente, el riesgo se compone tanto de probabilidad como de consecuencia, donde la consecuencia es el impacto negativo que experimenta la organización debido al daño específico a los activos de la organización por la amenaza o vulnerabilidad específica.

$$\textit{Riesgo} = \textit{Probabilidad}_{\textit{Ocurrir Evento}} \times \textit{Consecuencia} \quad \text{(A.2)}$$

A.2.3.3.7.3 Calibración de escalas de probabilidad y consecuencia.

Los sistemas de gestión de riesgos se han desarrollado en la mayoría de las organizaciones para hacer frente a una amplia variedad de riesgos. En algunos casos, el uso de tales sistemas ha sido obligatorio por los requisitos reglamentarios. Estos sistemas de gestión de riesgos hacen uso de la misma ecuación de riesgo

para priorizar los riesgos para la organización por el mismo tipo de amenazas a diferentes activos (por ejemplo, seguridad de la información) o por diferentes amenazas a los mismos activos (es decir, continuidad del negocio, seguridad de operación, seguridad ambiental y seguridad física). En la mayoría de las organizaciones, estos sistemas de gestión de riesgos ya habrán desarrollado escalas de probabilidad y consecuencia.

Una escala de probabilidad típica se muestra en la Tabla A.1. Esta escala es solo un ejemplo; la organización necesitará determinar los valores reales utilizados en esta escala por sí mismos.

Tabla A.1 - Escala de probabilidad típica

Probabilidad.	
Categoría	**Descripción**
Alto	Una amenaza / vulnerabilidad cuya ocurrencia es probable en el próximo año.
Medio	Una amenaza / vulnerabilidad cuya ocurrencia es probable en los próximos 10 años.
Bajo	Una amenaza / vulnerabilidad para la cual no hay antecedentes de ocurrencia y para la cual la probabilidad de ocurrencia se considera improbable.

A la mayoría de las organizaciones les resulta difícil ponerse de acuerdo sobre la probabilidad, y actualmente hay poca información disponible para ayudar. Está claro que las opiniones diferentes sobre este factor pueden cambiar radicalmente las inversiones realizadas por el CSMS. Aunque es posible que no todos estén de acuerdo con la evaluación final sobre la probabilidad, el beneficio de usarla es que las suposiciones que se utilizan para impulsar la inversión en CSMS son claras para todos. Dado que la probabilidad es el principal factor de riesgo sobre el cual una organización tiene la menor información y control, es importante realizar un seguimiento de las mejoras en los datos de la industria disponibles para ayudar a que este factor sea más preciso.

Para abordar el problema de la falta de acuerdo, algunas organizaciones utilizan los siguientes métodos:

- Use una probabilidad del 100% y, por lo tanto, considere solo las consecuencias, o haga esto para ciertos tipos de consecuencias como HSE.

- Acuerde un rango de probabilidades o categorías de probabilidad y luego trabaje su proceso de priorización basado en rangos.

- Intente más precisión consultando los datos de la industria que están disponibles en ataques a IACS.

- Intente más precisión mediante la recopilación de datos internos de incidentes.

- Separe la probabilidad en dos factores: la probabilidad de que un adversario intente un ataque y la probabilidad de que tenga éxito. La separación de estos factores puede ayudar a aclarar la verdadera fuente de desacuerdo. Si todos pueden estar de acuerdo en que un intento tendrá éxito y el argumento de bajo riesgo se basa en esperar que no ocurra ningún intento, eso puede cambiar el tono de la discusión.

La consecuencia generalmente se mide en diferentes términos para diferentes tipos de riesgos. Una escala de consecuencia típica se muestra en la Tabla A.2. Este ejemplo ilustra cómo la evaluación del riesgo cibernético puede tener en cuenta la seguridad del proceso y otros riesgos organizacionales. Como se indicó anteriormente, esta escala es solo un ejemplo y deberá calibrarse para la organización.

Es importante seguir un alto nivel de honestidad intelectual al evaluar las consecuencias. Durante la evaluación, identifique los supuestos que afectan el nivel de consecuencia. Por ejemplo, uno podría suponer razonablemente que todos los enclavamientos de seguridad y los sistemas de apagado están en su lugar para minimizar el impacto de un evento, ya que la probabilidad de un evento cibernético junto con un accidente no relacionado que inhabilita los sistemas de seguridad es muy pequeña. Sin embargo, al hacer esta suposición, uno también debe considerar si existe el riesgo de un ataque cibernético intencional aprovechando un mal funcionamiento accidental de los sistemas de seguridad o un ataque físico o cibernético coordinado que causa dicho mal funcionamiento. Otros supuestos posibles que pueden mencionarse son, los que se siguen las prácticas operativas en la medida típica de la operación normal y se siguen los procedimientos fundamentales de bloqueo. Es importante que se evalúen honestamente los riesgos, teniendo en cuenta la sofisticación y el estado del sistema de control, las operaciones relacionadas y la dependencia de ese sistema para operar la instalación.

Las consecuencias se realizan necesariamente con respecto a los intereses y políticas de la organización que realiza la evaluación de riesgos. Aunque el riesgo del IACS puede verse muy afectado por los peligros asociados con las operaciones industriales controladas por el IACS, es importante no confundir el riesgo para la organización con el riesgo para la sociedad.

Las operaciones industriales pueden no emplear ningún material peligroso, pero producen un producto muy valioso en demanda que genera altos ingresos para la empresa. Un incidente de seguridad de IACS que resulte en un trastorno de las operaciones industriales, causando varios días de productos fuera de especificación que no se pueden vender, podría tener un impacto financiero muy alto para la compañía. Para esta empresa, el IACS tiene un nivel de alto riesgo a pesar de que la sociedad puede ver esto como de bajo riesgo porque no existe un impacto en la salud, la seguridad o el medio ambiente para el público en general. Del mismo modo, la misma organización también podría considerar una operación industrial alterada en una instalación de producción que utiliza materiales peligrosos como una consecuencia de alto riesgo, incluso si no impacta la producción, debido a políticas internas y / o regulaciones externas relacionadas con la seguridad pública.

Antes de convocar a un grupo para evaluar los riesgos individuales, aclare las escalas de probabilidad y consecuencia para proporcionar orientación al equipo que realiza la evaluación de riesgos.

Tabla A.2 - Escala de consecuencia típica

Consequence	Risk area											
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	> 5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community
C (low)	< 1 day	< 1 hour	< 5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits	Little to no impact to business sectors beyond the individual company. Little to no impact on community services

A.2.3.3.7.4 Nivel de riesgo.

El resultado de una evaluación de riesgo cualitativa consistirá en una lista de activos o escenarios con una clasificación general del nivel de riesgo. Esto normalmente se desarrolla en una matriz similar a la que se muestra en la Tabla A.3, que define tres niveles de riesgo basados en tres niveles de probabilidad y consecuencia. Por lo tanto, a cada riesgo identificado en la evaluación de riesgos se le asigna un nivel de riesgo. Nuevamente, esto se entiende como un ejemplo y requerirá una revisión adicional por parte de la organización.

Tabla A.3 - Matriz de nivel de riesgo típica

		Categoría de consecuencia		
		A	**B**	**C**
Probabilidad	**Alto**	Alto riesgo	Alto riesgo	Riesgo medio
	Medio	Alto riesgo	Riesgo medio	Riesgo bajo
	Bajo	Riesgo medio	Riesgo bajo	Riesgo bajo

Los niveles de riesgo en cada bloque (Alto, Medio y Bajo) corresponden a una combinación particular de probabilidad y consecuencia. Una organización definirá una política de tolerancia al riesgo relacionada con cada nivel de riesgo, que corresponderá a un nivel particular de respuesta corporativa. El enfoque real para resolver el riesgo puede ser mediante el uso de contramedidas identificadas. La administración corporativa responsable debe preparar una versión inicial de esta matriz antes del proceso de análisis de riesgos. Este es el método recomendado para garantizar que el esfuerzo de evaluación de riesgos proporcione resultados que ayuden directamente en la toma de decisiones y que la organización pueda actuar.

Consulte A.3.4.2 para obtener más información sobre cómo definir una política de tolerancia al riesgo y cómo se utilizan la política de tolerancia al riesgo y los resultados de la evaluación del riesgo para gestionar los riesgos.

A.2.3.3.8 Evaluación detallada de riesgos.

A.2.3.3.8.1 General.

Una evaluación detallada del riesgo se centra en las redes y dispositivos individuales de IACS, y tiene en cuenta una evaluación técnica detallada de la vulnerabilidad de estos activos y la efectividad de las contramedidas existentes. Es posible que no sea práctico para todas las organizaciones realizar una evaluación de riesgos detallada de todos sus activos de IACS a la vez; en este caso, una organización reunirá suficiente información sobre sus IACS para permitirles priorizar estos sistemas, determinando a los que primeros que se realizara el esfuerzo de evaluación de vulnerabilidad y riesgo.

Una evaluación de riesgos detallada identifica los riesgos y luego los prioriza. Se deben identificar los riesgos para cada IACS. Después de identificar los riesgos, una organización puede optar por priorizar todos los riesgos encontrados en todos estos sistemas, priorizar los riesgos individualmente para cada sistema o priorizar los riesgos encontrados en subconjuntos de los IACS estudiados, como todos los IACS en un sitio específico. Dado que la priorización en última instancia impulsa las decisiones sobre qué acciones se tomarán y las inversiones que se realizarán para mejorar la seguridad cibernética, el alcance de la priorización debe alinearse con el alcance del presupuesto y la autoridad de decisión en la organización para realizar estas

inversiones. Por ejemplo, si todos los IACS que respaldan una línea de productos específica se administran y presupuestan como un grupo, los riesgos entre esos IACS se priorizarían juntos para respaldar el proceso de decisión de ese gerente.

A.2.3.3.8.2 Caracterización de los IACS claves.

Identificar y priorizar los riesgos de IACS requiere que una organización localice e identifique los IACS clave y sus dispositivos y las características de estos sistemas que generan riesgos. Sin un inventario de los dispositivos y redes IACS, es difícil evaluar y priorizar dónde se requieren medidas de seguridad y dónde tendrán el mayor impacto.

El equipo se reunirá con el personal de IACS para identificar los diferentes IACS utilizados en todo el sitio y que controlan sitios remotos. La atención debe centrarse en los sistemas en lugar de solo dispositivos, incluidos, entre otros, los sistemas de control, los sistemas de medición y los sistemas de monitoreo que utilizan un panel de operador central. Incluya áreas de operaciones industriales, así como áreas de servicios públicos como centrales eléctricas e instalaciones de tratamiento de residuos.

Como se señaló anteriormente, el objetivo es identificar los principales dispositivos y tipos de dispositivos que están en uso y funcionan colectivamente para operar el equipo bajo control. En este punto del desarrollo del programa de seguridad, no es importante desarrollar un inventario completo de cada dispositivo en el IACS, porque el inventario se utilizará para tomar decisiones de juicio sobre el riesgo relativo que los dispositivos de control introducen en la operación industrial. Como ejemplos, es importante entender:

- Si la instrumentación de campo y su comunicación a los controladores es analógica o digital.
- Si los dispositivos / sistemas están conectados entre sí y los tipos de redes utilizados.
- Si los dispositivos están ubicados dentro de un área segura, como un edificio o instalación cercada, o si los dispositivos están ubicados de forma remota.
- Si los dispositivos de control están sujetos a control reglamentario.
- Si la pérdida o el mal funcionamiento del dispositivo / sistema es significativo en términos de su impacto en el equipo bajo control, tanto en términos comerciales / financieros como de HSE.

La identificación resultante de dispositivos / sistemas debe mostrar el alcance del impacto en el equipo bajo control, si los dispositivos pierden el control de las operaciones industriales a las que se aplican y su relativa vulnerabilidad de seguridad (por factores físicos, de red u otros). Este tipo de información se puede utilizar para comprender el riesgo relativo para la operación industrial. No es necesario realizar un inventario completo para identificar cantidades exactas de cada tipo de dispositivo en esta etapa.

A.2.3.3.8.3 Agrupar los dispositivos y sistemas y desarrollar un inventario.

A medida que el equipo identifica los dispositivos / sistemas individuales, puede ser útil colocar los elementos en una agrupación lógica de equipos. En las modernas instalaciones de IACS, esta colección de equipos funciona como un sistema integrado para controlar las diversas actividades de la operación industrial. El número de sistemas de control lógico en una empresa variará ampliamente. En una organización mediana a grande, puede haber varios cientos de IACS lógicos compuestos por miles de dispositivos individuales y sistemas de bajo nivel.

Para organizaciones medianas y grandes que abordan la seguridad cibernética en toda la empresa, puede ser muy útil registrar la lista de sistemas lógicos en una base de datos con capacidad de búsqueda. DCS puede organizarse por línea, unidad, área o grupo dentro de un sitio geográfico local o remoto. Los sistemas SCADA pueden organizarse por centro de control, sitio remoto y equipo de control asociado. La base de datos será más efectiva si los datos se recopilan en un formato normalizado para facilitar la comparación de un sistema con otro. La Figura 4 es un ejemplo de un formato normalizado que se puede crear fácilmente en forma de hoja de cálculo o base de datos. Se ha incluido para estimular el pensamiento sobre el tipo de información que puede ser útil más adelante en la priorización del sistema y las actividades detalladas de evaluación de riesgos.

Automatización industrial y sistema de control de caracterización de redes

Negocio. _____
Sitio. _____
Unidad Operativa. _____
Contacto de TI del sitio. _____ Teléfono #. _____
Contacto de control de proceso del sitio._____ Teléfono #._____
Última actualización. _____

POR FAVOR, CONTESTE A LAS SIGUIENTES PREGUNTAS:
_____ ¿Los sistemas de automatización están actualmente conectados a las LAN corporativas o del sitio?
_____ ¿Se accede a los sistemas de automatización de forma remota desde fuera del dominio IACS?

Dominio de control de procesos.
— Número total de nodos direccionables IP
— Número de nodos direccionables IP a los que se debe acceder desde un dominio de control de proceso externo
— Número de usuarios concurrentes dentro del dominio IACS
— Número de usuarios concurrentes dentro del dominio IACS que requieren acceso a recursos externos
— Número de usuarios totales fuera del dominio IACS que requieren acceso a recursos de control de procesos
— Número de usuarios concurrentes fuera del dominio IACS que requieren acceso a los recursos de control de proceso de direccionamiento IP (marque todos los que correspondan)

_____DHCP _____Direcciones públicas utilizadas (es decir, xxxxx)
_____ estáticas _____Direcciones privadas utilizadas (192.168.xx)

Plataformas de control.

_____Número de plataformas de control.
_____Tipo de plataforma de control (PLC, DCS, PC)
Proveedores de plataforma de control_____ _____
Modelos de plataforma de control. _____ _____

Consolas de operador y dispositivos HMI.

_____Número de consolas de operador
Proveedores de la consola del operador _____ _____
Modelo (s) de consola del operador _____ _____
Sistemas operativos de la consola del operador_____ _____

Nodos de aplicación (marque todos los que correspondan).

_____Servidor de control y gestión de procesos.
_____SCADA
_____Servidor OPC
_____Estación de trabajo de ingeniería
_____Servidor por lotes

_____Otro

Barreras de seguridad de red en uso.

Tipo (firewalls, routers, VLANS, etc.) _____

Soporte de seguridad de red (marque todo lo que corresponda)
Recursos del sitio_____
Externo (tercero) _____

sitio de la red (sí de respuesta / no)
¿Diagramas de topología de red del sitio actual disponibles y actualizados?
¿Están los nodos de control de proceso en el segmento LAN aislado?
¿Política de seguridad de la información del sitio en su lugar?
Auditoría de la oficina de seguridad completada (en caso afirmativo, fecha completada _____) ¿Utiliza el sitio la autenticación de dos factores?
Evaluación de riesgos de la oficina de seguridad completada (en caso afirmativo, fecha completada _____)

Requisitos de acceso remoto (marque todos los que correspondan)
Vía sitio / LAN corporativa
Mediante módem de acceso telefónico
Vía Internet
Mediante módem de acceso telefónico local directamente vinculado a los nodos de fabricación y control

Requisitos de salida local (marque todos los que correspondan)
Para ubicar aplicaciones y recursos (sistemas de gestión de documentos, sistemas de calidad, sistemas comerciales)
Para aplicaciones y recursos corporativos (sistemas de gestión de documentos, sistemas de calidad, sistemas comerciales)

IEC 2321/10

Figura A.4 - Ejemplo de hoja de recopilación de datos IACS lógica

Se debe tener cuidado al identificar los dispositivos / sistemas de control de automatización industrial y centrar la atención más allá de los dispositivos que realizan el control directo. El sistema o la red pueden ser más que el PLC o DCS. En una instalación integrada de fabricación o producción, la red IACS se compone de dispositivos que se utilizan directamente para fabricar, inspeccionar, administrar y enviar productos y puede incluir, además de otros, los siguientes componentes:

· DCS y dispositivos asociados;
· Sistemas SCADA y dispositivos asociados;
· PLC y dispositivos asociados;
· Estaciones HMI;
· SIS y dispositivos asociados;
· Computadoras de planta de trabajo (propósito especial);
· Sistemas de gestión de información de proceso (PIM) y sistemas de ejecución de fabricación (MES);
· Sistemas de modelado de control de automatización industrial;
· Sistemas expertos;
· Sistemas de inspección;
· Sistemas de manejo y seguimiento de materiales;
· Analizadores;
· Sistemas de medición;

· Sistemas de lotes;

· Monitoreo de energía eléctrica y / o sistemas de gestión;

· Sistemas de telemetría remota;

· Sistemas de comunicación utilizados para la comunicación con dispositivos remotos;

· Sistemas de condiciones de operación normalizados (SOC) y procedimientos de operación normalizados (SOP);

· Sistemas de gestión de documentos;

· Computadoras de desarrollo de programas;

· Sistemas de control de climatización;

· Puertas de enlace de comunicación de red (es decir, conmutadores, concentradores y enrutadores);

· Dispositivos de protección de red (es decir, firewalls y sistemas de detección de intrusos).

Considere incluir todos los dispositivos en red basados en CPU que son críticos para mantener la producción. El objetivo de este paso del inventario es descubrir dispositivos que sean vulnerables a los ataques basados en la red para que puedan incluirse en la evaluación detallada de riesgos.

NOTA: No es el momento para decidir qué dispositivos deben aislarse o separarse de la LAN. Errar por el lado de incluir más dispositivos en lugar de menos. Después de realizar la evaluación de riesgos y comprender mejor las vulnerabilidades generales, el equipo de evaluación debe decidir si las soluciones de mitigación de riesgos son realmente necesarias y dónde deben ubicarse los distintos dispositivos.

Existen varias herramientas de inventario para toda la empresa disponibles comercialmente que funcionarán en todas las redes para identificar y documentar todo el hardware, los sistemas y el software que residen en la red. Se debe tener cuidado antes de usar este tipo de aplicación para identificar IACS. Realice una evaluación de cómo funcionan estas herramientas y qué impacto podrían tener en el equipo de control conectado antes de usar cualquiera de ellas.

La evaluación de la herramienta puede incluir pruebas en entornos de sistemas de control similares, fuera de línea y sin producción para garantizar que la herramienta no afecte negativamente el funcionamiento del sistema de control e interrumpa la producción. Si bien los dispositivos que no son de producción pueden no tener impacto en los sistemas de producción, pueden enviar información que podría (y ha causado en el pasado) fallas o daños en los sistemas de control. El impacto podría deberse a la naturaleza de la información y / o el tráfico y la carga del sistema. Aunque este impacto puede ser aceptable en los sistemas de TI, no lo es en IACS.

A.2.3.3.8.4 Desarrollar diagramas de red simples.

Un diagrama de red simple será beneficioso al agrupar los diversos dispositivos y sistemas de automatización y control industrial en un sistema de control lógico identificable. Debe incluir los dispositivos identificados con la Hoja de recopilación de datos IACS lógica que se analiza en A.2.3.3.8.2. El diagrama debe intentar capturar la arquitectura de red lógica básica, como los enfoques de conectividad, combinados con algunos de los conceptos básicos de la arquitectura de red física, como la ubicación de los dispositivos.

Antes de realizar las prioridades de IACS o una evaluación de riesgos detallada, es importante que el equipo tenga una comprensión clara del alcance / límites del sistema a evaluar. Un diagrama de red es una herramienta para visualizar la red y ayudar a realizar la evaluación de riesgos. Puede ser un diagrama de

bloques muy simple que muestra dispositivos, sistemas y conexiones de interfaz o más detallado como el que se muestra en la Figura A.5. Cualquiera de los dos enfoques será beneficioso para cumplir los objetivos. Si se han establecido zonas y conductos, los diagramas de red simples deben representar estos elementos. (Puede encontrar más explicaciones sobre zonas y conductos en desarrollo en A.3.3.4.)

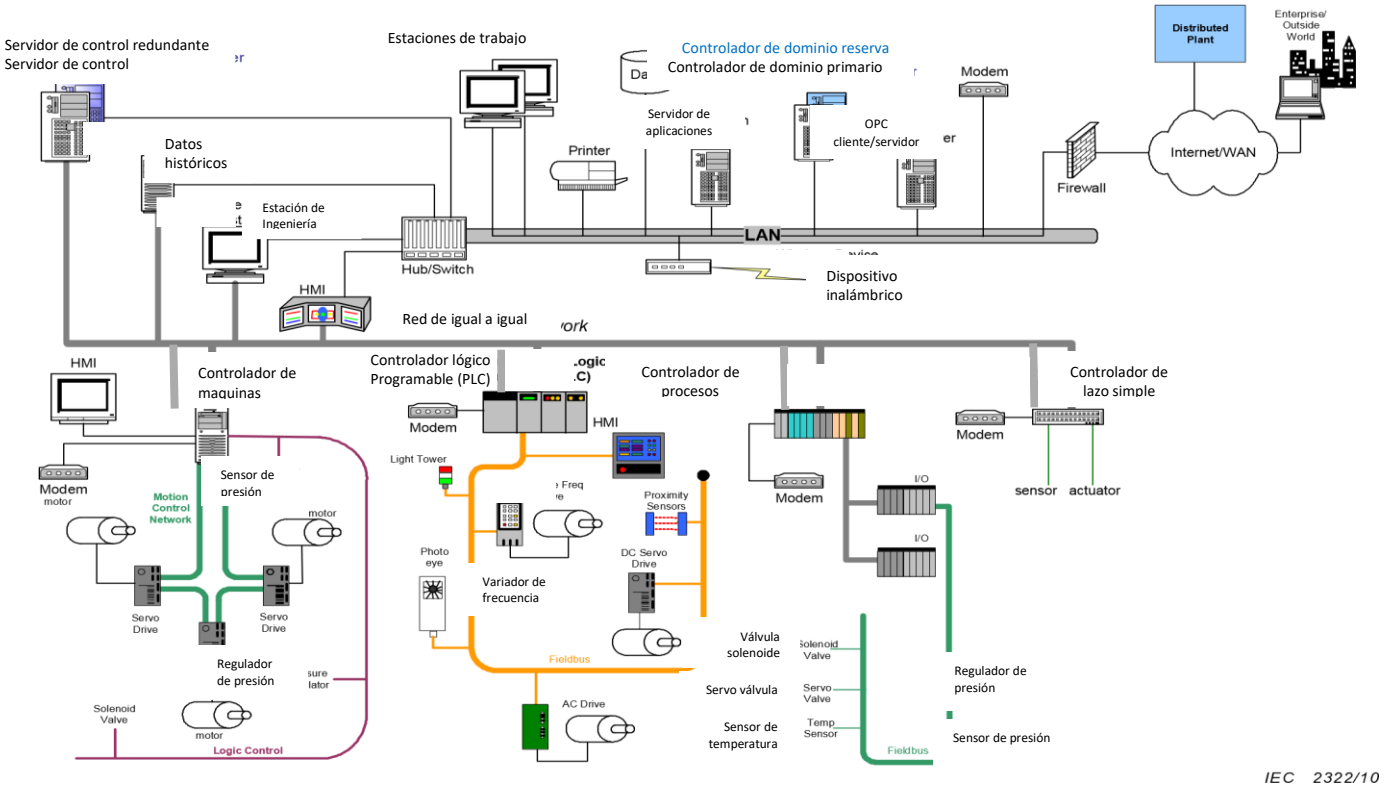

Figura A.5 - Ejemplo de un diagrama de red lógica gráficamente detallado.

Los diagramas de red simples son un punto de partida y representan una instantánea en un punto en el tiempo. La experiencia en la evaluación detallada de vulnerabilidades muestra que prácticamente todas las evaluaciones generan conexiones no identificadas en el proceso de diagramación inicial. Por lo tanto, estos diagramas no deberían constituir la única base para evaluar la conectividad sin una validación física más detallada. Son valiosos para determinar el esfuerzo de evaluación de riesgos y para definir zonas y conductos como se describe en IEC / TS 62443 - 1 - 1.

A.2.3.3.8.5 Evaluación preliminar del riesgo general para cada sistema identificado

Una vez que se ha completado la lista de dispositivos, activos y redes de IACS, se debe realizar una evaluación preliminar en cuanto al nivel relativo de riesgo asociado con los sistemas, de modo que puedan priorizarse para una evaluación detallada del riesgo. Si se va a realizar una evaluación de riesgos detallada en todos los IACS o si la evaluación de riesgos de alto nivel ha proporcionado información suficiente para priorizar los IACS individuales por riesgo, entonces este paso no será necesario.

Cada sistema individual se evaluará para comprender las consecuencias financieras y de HSE identificadas en la evaluación de riesgos de alto nivel, en caso de que la disponibilidad, integridad o confidencialidad del sistema se vea comprometida. Además, se debe asignar alguna medida de escala a la evaluación.

El personal familiarizado con el IACS llevará a cabo la actividad de evaluación de detección. El personal de IACS y TI generalmente brinda conocimiento de los dispositivos y sistemas en uso, mientras que el personal de operaciones generalmente comprende las consecuencias de un incidente de seguridad. Este equipo de recursos trabajará en conjunto para lograr la evaluación de detección.

El equipo desarrollará una escala de alto nivel para calificar cuantitativamente el riesgo general asociado con cada sistema. La escala podría ser tan simple como alta, media y baja o de 1 a 10 y establecerá los criterios para cada graduación en la escala de riesgo.

El equipo tomará una decisión de juicio sobre el nivel de riesgo asociado con cada sistema al examinar las consecuencias financieras y de HSE en caso de que la disponibilidad, integridad o confidencialidad del sistema se vea comprometida. El equipo debe registrar la evaluación de riesgos de alto nivel para el sistema lógico en la lista de inventario desarrollada anteriormente. Establecer niveles de tolerancia al riesgo ayuda a priorizar los activos reales en el entorno IACS.

Los resultados de esta evaluación preliminar serán un aporte importante a la decisión de realizar una evaluación de vulnerabilidad detallada para un IACS particular. Se planificará una evaluación completa de la vulnerabilidad si:

- Se determina que el IACS está actualmente conectado a la red corporativa o a redes externas (por ejemplo, Internet, módems). Una evaluación detallada del riesgo ayudará a comprender mejor las vulnerabilidades y la estrategia de mitigación adecuada para reducir el riesgo.
- Se determina que en el sistema se permite actuar de forma remota.
- Se anticipa que cualesquiera de los dos criterios anteriores se cumplirán en un futuro cercano. En ese caso, la evaluación de vulnerabilidad debe realizarse antes de tomar medidas que den como resultado esta posición de alto riesgo.

A.2.3.3.8.6 Priorización de los sistemas.

La subcláusula anterior sugería asignar una calificación de vulnerabilidad / riesgo a cada IACS lógico identificado. Esta escala de calificación es un buen punto para comenzar el proceso de priorización. Sin embargo, hay varios temas adicionales a considerar al decidir dónde comenzar a enfocar los esfuerzos detallados de evaluación de riesgos, tales como:

- Riesgo para la empresa (por ejemplo, HSE o financiera);
- Lugares donde el proceso de evaluación es más exitoso;
- Costo de las posibles contramedidas requeridas;
- Costos de capital versus no capital;
- Personal de apoyo calificado disponible para el sistema particular;
- Región geográfica;
- Directivas o sensibilidades de los miembros de asociaciones comerciales;

- Requisitos políticos locales o del país;
- Personal de apoyo externo o interno;
- Apoyo del sitio para emprender el esfuerzo;
- Historial de problemas conocidos de ciberseguridad.

No hay un enfoque correcto o incorrecto. Los valores serán diferentes para cada empresa. Lo importante es utilizar los mismos principios de priorización en todos los sitios. Registre las decisiones de priorización tomadas y la base para tomarlas.

A.2.3.3.8.7 Identificar vulnerabilidades y priorizar riesgos.

El siguiente paso en el proceso de evaluación de riesgos es llevar a cabo una evaluación de riesgos detallada en los sistemas priorizados. La mayoría de las metodologías emplean un enfoque para dividir el sistema en partes más pequeñas y examinar los riesgos asociados con estos elementos más pequeños que comprenden el sistema general.

Una evaluación de riesgos detallada debe abordar las amenazas de seguridad física y cibernética, las amenazas internas y externas y considerar el hardware, el software y la información como fuentes de vulnerabilidades.

Es imperativo que un equipo de personas realice la valoración para aportar una perspectiva completa a la evaluación. El equipo debe estar compuesto, como mínimo, por una persona líder de operaciones del sitio, una persona IACS del sitio, una persona de TI del sitio y una persona de la red del sitio. Otros a considerar incluyen expertos en seguridad física, seguridad del sistema de información, legal, comercial (operaciones, mantenimiento, ingeniería, etc.), recursos humanos, HSE y proveedores de hardware. Estas personas están en la mejor posición para reconocer las vulnerabilidades y la consecuencia del riesgo para sus áreas específicas.

Aunque el objetivo es comprender las amenazas y las consecuencias asociadas con un sistema en particular, es muy probable que un objetivo clave sea poder comparar los resultados de la evaluación de un sistema / sitio con otro en toda la organización. La capacidad de hacer esto dependerá de cuán consistentemente se aplique la metodología. Algunos enfoques probados incluyen:

- Uso de una persona clave para dirigir el proceso de evaluación en cada sitio;
- Utilizar un pequeño equipo de personas para dirigir las evaluaciones basadas en la geografía, la unidad de negocios y similares, que han participado entre sí en otras evaluaciones;
- Utilizar buenos materiales de capacitación con procedimientos y ejercicios para nivelar el equipo de personas que realizarán las evaluaciones en cada sitio;
- Utilizando un formulario o base de datos común para registrar los resultados de la evaluación;
- Revisar centralmente todos los resultados de la evaluación para verificar si los resultados parecen realistas y comparables a otros sistemas similares.

Al realizar la evaluación, tenga en cuenta todos los aspectos del IACS, incluidos los cambios involuntarios en la configuración del sistema provocados por el mantenimiento, las conexiones temporales del proveedor al sistema para obtener asistencia e incluso cambios sutiles en el diseño del proveedor que podrían introducir nuevas vulnerabilidades a través de repuestos o actualizaciones, que debe considerarse y / o probarse de la misma manera que los componentes del sistema original.

La evaluación también debe abordar los sistemas que interactúan con el IACS para garantizar que no puedan comprometer la seguridad del IACS o viceversa. Los ejemplos incluyen sistemas de desarrollo que proporcionan capacidades de perfeccionamiento en línea y sistemas ambientales y de energía cuyo compromiso podría crear riesgos inaceptables.

En algunos casos, la vulnerabilidad puede recaer en el proveedor. El aseguramiento de la calidad del proveedor y el control del diseño pueden requerir una evaluación de vulnerabilidad. Este paso es particularmente importante al ordenar repuestos o actualizaciones.

En este punto del proceso de evaluación, se debe realizar un examen detallado de la red desde un punto de vista físico y operativo para descubrir cualquier conexión que no se muestre en los diagramas iniciales simples de la red. Muchas evaluaciones encontrarán tales conexiones.

Las siguientes fuentes potenciales de vulnerabilidades relacionadas con la conectividad de red han sido identificadas previamente como debilidades en ciertos sistemas y deben identificarse y examinarse:

- Puntos de acceso inalámbrico, particularmente tecnologías mal aseguradas, como las primeras versiones de IEEE 802.11;
- Conexiones de módem, particularmente aquellas que no vuelven a marcar y no proporcionan cifrado;
- Programas de software de acceso remoto (por ejemplo, pcAnywhere®[3] y Timbuktu®) que los expertos suelen utilizar para acceder a sistemas u operaciones para el acceso de expertos dentro o fuera de la entidad. Estas aplicaciones pueden proporcionar un control significativo y acceso de configuración a un individuo no autorizado;
- Tecnologías de ventanas remotas como X Windows®;
- Conexiones de intranet;
- Conexiones a Internet;
- Redes de telemetría;
- Cualquier conexión de red a sistemas que no son parte directa de IACS;
- Cualquier conexión de red utilizada para acoplar partes del SCADA o el sistema de control que no formen parte de una red IACS dedicada físicamente segura. En otras palabras, cualquier red que se extienda más allá del límite de una sola zona de seguridad o a través de zonas inseguras o se use tanto para IACS como para otras funciones al mismo tiempo. El equipo incluido en las conexiones de red incluye telemetría de radio y servicios subcontratados, como el frame relay utilizado para comunicarse entre áreas separadas geográficamente.

Varios recursos de la industria cubren la seguridad del sistema de control y proporcionan listas de vulnerabilidades típicas para buscar en una evaluación detallada de vulnerabilidad (ver [27] y [29]).

El resultado final del equipo es una lista de vulnerabilidades priorizadas por su impacto en el riesgo. Una vez que se han identificado las vulnerabilidades, el equipo asocia estas vulnerabilidades con amenazas, consecuencias y probabilidades asociadas para la realización de la amenaza y el ejercicio de la vulnerabilidad. Este análisis tiene en cuenta la mitigación potencial debido a las medidas de seguridad física. Esas vulnerabilidades que contribuyen a los riesgos de más alto nivel son generalmente fáciles de acordar. Para completar el proceso de evaluación de vulnerabilidad, la metodología del equipo debe incluir un método acordado para determinar cómo priorizar las vulnerabilidades que contribuyen a una gran cantidad de riesgos de nivel medio y bajo.

Se deben documentar los resultados detallados de la evaluación de riesgos y se deben tomar medidas sobre las recomendaciones derivadas de ellos (ver A.3.4.2).

La documentación de las vulnerabilidades encontradas durante la evaluación de riesgos detallada generalmente incluye para cada vulnerabilidad encontrada, la fecha de la evaluación, la identificación de los activos involucrados, la descripción de la vulnerabilidad, el nombre de una persona que observó la vulnerabilidad y las herramientas o métodos que utilizaron para para hacerlo. Además de las vulnerabilidades encontradas, la documentación de la evaluación detallada de vulnerabilidades debe incluir vulnerabilidades comprobadas, pero no encontradas como presentes y cómo se verificó esto para cada activo evaluado. Esto puede tomar la forma de una simple lista de verificación. La documentación de vulnerabilidades proporciona un gran apalancamiento al actualizar la evaluación de riesgos y cuando se plantean preguntas específicas sobre los activos. Las listas de verificación de vulnerabilidad anteriores y los resultados forman una línea de base a partir de la cual mejorar las evaluaciones de vulnerabilidad en el futuro y una base para la coherencia en toda la organización. Una organización debería verlos desde esta perspectiva y evitar verlos como una definición estática de los contenidos de dicha evaluación.

[3] pcAnywhere®, Timbuktu® y X Windows® son ejemplos de productos adecuados disponibles comercialmente. Esta información se proporciona para la comodidad de los usuarios de esta norma y no constituye un respaldo por parte de ISA de estos productos.

Las tareas y la documentación relacionadas con los procesos de evaluación de riesgos detallados y de alto nivel descritos en esta subcláusula y el proceso de gestión de riesgos en A.3.4.2 pueden integrarse para que la eficiencia se adapte a las necesidades de una organización en particular.

Los resultados detallados de la evaluación de riesgos deben actualizarse y revalidarse periódicamente. Además, dado que una evaluación de riesgos detallada puede quedar desactualizada debido a cambios en el entorno de un sistema de control, los factores desencadenantes para un esfuerzo de evaluación de riesgos actualizado deben incorporarse en el programa de gestión del cambio. Este es un punto crítico, ya que a la mayoría de las organizaciones les resulta más fácil establecer una línea de base de seguridad cibernética que mantenerla en el tiempo (ver A.4.3).

A.2.3.3.8.8 Errores a evitar.

Durante la evaluación, se deben evitar las dificultades comunes que pueden descarrilar el proceso de evaluación de riesgos mediante las siguientes acciones:

a) Diseñar la solución durante la evaluación.

El propósito de la evaluación es aprender qué riesgos existen, no diseñar la solución en equipo. Se puede perder mucho tiempo tratando de resolver el problema y debatiendo un enfoque versus otro mientras se evalúa un activo en particular. El enfoque debe estar en comprender los riesgos y las consecuencias que existen actualmente o que pueden ocurrir en el futuro previsible, como un proyecto actualmente en curso para agregar un nuevo modelo de dispositivo con una interfaz de red.

b) Minimizando o exagerando la consecuencia.

Se debe proporcionar una evaluación honesta de la consecuencia de un incidente que afecte un hardware, software o activo de información en particular. Las consecuencias no deben minimizarse con el fin de evitar tomar acciones adecuadas de mitigación de riesgos de seguridad para reducir el riesgo. Lo que puede ser muy importante para una persona en particular porque afecta directamente su trabajo, puede tener un nivel muy diferente de consecuencias para la organización en su conjunto.

c) No lograr consenso sobre los resultados de la evaluación de riesgos.

Llegar a un acuerdo sobre los riesgos y las consecuencias es extremadamente importante. Será mucho más difícil llegar a un acuerdo sobre las contramedidas si el equipo no tiene una comprensión común del riesgo y un acuerdo sobre la importancia.

d) Evaluar el sistema sin considerar los resultados de la evaluación de otros sistemas similares.

Es importante validar que los resultados son apropiados y consistentes con los de procesos de evaluación similares en otros sitios. Las conclusiones de evaluaciones de sistemas similares anteriores y las vulnerabilidades identificadas pueden ser muy beneficiosas para la evaluación del sistema en cuestión.

A.2.3.3.8.9 Interrelación con medidas de seguridad física.

La seguridad cibernética y la seguridad física pueden estar estrechamente relacionadas. En algunas situaciones, pueden funcionar como capas independientes de protección y en otras situaciones dependen mucho el uno del otro. La pérdida de uno puede representar una pérdida de ambas capas de protección. Durante la evaluación detallada de riesgos para un sistema, se debe tener en cuenta la interacción potencial y cómo puede afectar las consecuencias.

En algunas industrias, es una práctica común tener un SIS además del IACS. Si el SIS se basa en retransmisión, la probabilidad de que se vea afectada por un evento cibernético que afecte al IACS es pequeña. Se puede contar con el SIS para realizar su función de seguridad y se puede contener y reducir la consecuencia de un evento cibernético. Sin embargo, si el SIS se basa electrónicamente y está vinculado a la misma red que el IACS (algunas industrias no recomiendan esta práctica), la probabilidad de un incidente cibernético que afecte a ambos sistemas es mucho mayor y la consecuencia podría ser mayor.

Otro ejemplo podría ser un sistema de acceso de credenciales a una sala de control cerrada. En situaciones normales, el sistema de control de acceso proporciona seguridad adicional a los sistemas de control.

Sin embargo, en el caso de una inundación de la red por denegación de servicio (DoS), el sistema de control de acceso a la puerta podría no funcionar e impedir la capacidad del operador de acceder a la consola del operador de la sala de control. La misma sobrecarga de red DoS podría estar afectando también a la consola del operador. En esta situación, el único incidente cibernético sirve como un doble impedimento para responder al dispositivo de control y podría aumentar la consecuencia del incidente.

Finalmente, las metodologías de evaluación de riesgos de seguridad cibernética deberían incorporarse a las metodologías de evaluación de riesgos físicos y del sitio.

A.2.3.3.8.10 Evaluación de riesgos y el ciclo de vida de IACS.

Las subcláusulas anteriores describen cómo se puede llevar a cabo el proceso de evaluación de riesgos en los IACS existentes cuando se establece un CSMS por primera vez y luego se aplica periódicamente. La evaluación de riesgos es más efectiva y menos perjudicial cuando se aplica de manera similar durante las diversas etapas del ciclo de vida del IACS, antes de que se ejecute en modo de producción:

a) Durante el desarrollo de un IACS nuevo o actualizado.

El riesgo cibernético debe considerarse de antemano antes de implementar un IACS nuevo o modificado, ya que la experiencia ha demostrado que siempre será más fácil y menos costoso considerar la seguridad durante la fase de diseño que agregarla más tarde. El proceso para la evaluación de riesgos de alto nivel continúa de la misma manera para un sistema futuro como se describió anteriormente para un sistema existente. La evaluación se realiza idealmente en paralelo con el diseño de alto nivel y los resultados del diseño propuesto y la evaluación de riesgos se revisan juntos. También se puede llevar a cabo una evaluación de riesgos detallada en paralelo con el diseño detallado, aunque las vulnerabilidades identificadas son hipotéticas y en todos los casos no serán tan específicas como para un sistema ya implementado. De esta manera, la evaluación de riesgos durante el desarrollo puede conducir decisiones sobre qué contramedidas deben implementarse junto con las mejoras deseadas de IACS, para minimizar las sorpresas después de la implementación.

b) Durante la implementación de un IACS nuevo o actualizado

Incluso con atención al riesgo durante la fase de desarrollo, los detalles de implementación pueden introducir vulnerabilidades inesperadas. En el mejor de los casos, parte del proceso de aceptación de un IACS nuevo o actualizado incluye no solo pruebas, sino también un análisis detallado de vulnerabilidad como se describió anteriormente. Así, por ejemplo, una organización puede necesitar determinar si activar un sistema nuevo o actualizado antes de que un parche a una vulnerabilidad descubierta recientemente esté disponible para el sistema operativo subyacente.

c) Durante la desactivación de un IACS

La decisión de retirar o retener un IACS o componentes de un IACS se basa en muchos factores, incluidos el costo, el deseo de una nueva funcionalidad o capacidad, la confiabilidad continua y la disponibilidad de soporte del proveedor. El impacto en la seguridad cibernética también es un factor a tener en cuenta en esta decisión. Los nuevos componentes y arquitecturas pueden mejorar la funcionalidad de seguridad y / o introducir nuevas vulnerabilidades que deben abordarse. Por lo tanto, una evaluación de riesgo cibernético que analiza una decisión de desactivación examina tanto el escenario en el que se reemplaza el sistema antiguo como el escenario en el que el sistema antiguo se retiene durante un período de tiempo.

Las evaluaciones de riesgo de alto nivel y detalladas se actualizan al retirar un IACS por dos razones: 1) la eliminación del IACS puede afectar la vulnerabilidad de otros que permanecen en su lugar y 2) si el IACS se reemplaza por un nuevo sistema, se pueden introducir nuevas vulnerabilidades como se discutió anteriormente. Un ejemplo de esto es que la conectividad de red a un IACS que permanece en su lugar, puede haber tenido lugar siempre a través de un IACS que ha sido eliminado. Esto significa que se implementa un nuevo diseño de conectividad para el IACS restante y esta configuración debe evaluarse para detectar vulnerabilidades y riesgos asociados.

A.2.3.4 Prácticas de apoyo.

A.2.3.4.1 Prácticas de referencia.

Las siguientes diez acciones son prácticas básicas:

a) Establecer los criterios para identificar qué dispositivos comprenden el IACS.

b) Identificar dispositivos IACS que admitan procesos del negocio críticos y operaciones, incluidos los sistemas de TI que admiten estos procesos.

c) Clasificar los activos y componentes lógicos en función de la disponibilidad, integridad y confidencialidad, así como el impacto de HSE.

d) Priorizar las actividades de evaluación de riesgos en función de las consecuencias (por ejemplo, las operaciones industriales con altos riesgos conocidos se abordan con alta prioridad).

e) Determinar los límites del sistema a evaluar, identificando todos los activos y componentes críticos.

f) Desarrollar un diagrama de red del IACS (ver A.2.3.3.8.4).

g) Comprender que los riesgos, la tolerancia al riesgo y la aceptabilidad de las contramedidas pueden variar según la región geográfica u organización empresarial.

h) Mantener un registro actualizado de todos los dispositivos que comprenden el IACS para evaluaciones futuras.

i) Realizar una evaluación de riesgos en todas las etapas del ciclo de vida de la tecnología (desarrollo, implementación, actualización y retiro).

j) Identificar la frecuencia de reevaluación o los criterios de activación basados en cambios de tecnología, organización u operación industrial.

A.2.3.4.2 Prácticas adicionales.

Las siguientes cuatro acciones son prácticas adicionales:

a) Identificar y clasificar activos para ayudar a definir el riesgo de la empresa. Las áreas de enfoque importantes deben ser las personas involucradas y las tecnologías utilizadas. La creación de una lista de verificación ayuda a agrupar los activos en categorías (ver A.2.3.3.8.3).

b) Clasificación de los activos individuales en función de las implicaciones de seguridad de la disponibilidad, integridad y confidencialidad. Un activo podría tener diferentes niveles de clasificación para cada una de las categorías.

EJEMPLO Clasificación para un tipo específico de datos:

- Disponibilidad: baja: el sistema no requiere un funcionamiento continuo. El sistema no es parte de una operación peligrosa. Un retraso de hasta uno o dos días sería aceptable.
- Integridad: medio: los datos se verifican en varias etapas y se detectarían cambios en ellos.
- Confidencialidad: muy alta: los datos críticos del negocio deben mantenerse al más alto nivel confidencial.

c) Establecer la probabilidad (es decir, probabilidad o frecuencia estimada) de que una amenaza particular sea exitosa, en vista del nivel actual de controles. Es importante tener en cuenta otros controles típicos que pueden existir en la fabricación / operaciones que complementarían los controles de seguridad cibernética para reducir la probabilidad de que ocurra la consecuencia. Estos incluyen SIS independiente y otras técnicas de PSM, como dispositivos de respaldo pasivos, auxiliares e independientes. La frecuencia estimada está directamente relacionada con la vulnerabilidad y las amenazas generales y podría expresarse cuantitativamente como un porcentaje o más subjetivamente como alta, media o baja.

d) Definir las consecuencias o el impacto de un intento de amenaza exitoso sobre el negocio o la evaluación de riesgos de IACS.

A.2.3.5 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [24], [26], [27], [28], [29], [30], [33] [42]

A.3 Categoría: abordar el riesgo con el CSMS.

A.3.1 Descripción de la categoría.

La segunda categoría principal del CSMS es abordar el riesgo. Esta categoría contiene la mayor parte de los requisitos e información contenidos en el CSMS. Se divide en tres grupos de elementos:

· Política de seguridad, organización y sensibilización.

· Contramedidas de seguridad seleccionadas.

· Implementación.

A.3.2 Grupo de elementos: política de seguridad, organización y concientización.

A.3.2.1 Descripción del grupo de elementos.

El primer grupo de elementos en esta categoría analiza el desarrollo de las políticas básicas de seguridad cibernética, las organizaciones responsables de la seguridad cibernética y la concientización dentro de la organización de los problemas de seguridad cibernética. La figura A.6 muestra una representación gráfica de los cinco elementos contenidos en el grupo de elementos:

· Alcance del CSMS,

· Organización para la seguridad,

· Capacitación del personal y concientización de seguridad,

· Plan de continuidad del negocio.

· Políticas y procedimientos de seguridad.

Figura A.6 - Vista gráfica del grupo de elementos: política de seguridad, organización y concientización

A.3.2.2 Elemento: alcance del CSMS.

A.3.2.2.1 Descripción del elemento.

Una vez establecida la justificación del negocio y obtenido el apoyo administrativo, el siguiente paso es desarrollar un alcance formal o una carta para el esfuerzo. Este alcance debe explicar qué se debe lograr (en términos comerciales) y cuándo. Define el enfoque específico para la entidad.

Esta declaración de alcance debe ser propiedad del líder ejecutivo del programa o de un equipo de gestión que será responsable de guiar al equipo durante el desarrollo del programa. En última instancia, el líder será responsable de asegurarse de que el programa se ejecute, incluidas las comunicaciones, la financiación, la aplicación y la auditoría.

Finalmente, el CSMS debe abarcar todas las unidades de negocios y todas las partes geográficas de la organización. Si el compromiso de liderazgo no se puede obtener inicialmente para este alcance de trabajo, defina un alcance de trabajo más pequeño y utilícelo como una oportunidad para generar credibilidad y demostrar el valor del CSMS.

A.3.2.2.2 Desarrollo del alcance del CSMS.

La gerencia necesita comprender los límites donde el CSMS se aplica a la organización, así como establecer una dirección y enfoque para el CSMS. Al desarrollar un alcance claramente definido, es más fácil para la gerencia transmitir sus objetivos y propósitos para el CSMS.

El alcance debe incluir todos los aspectos del IACS, puntos de integración con socios comerciales, clientes y proveedores. Se debe establecer un marco de gestión (por ejemplo, organización) para iniciar y controlar la implementación y las operaciones continuas de seguridad cibernética dentro de la empresa.

Una organización responsable de determinar y comunicar las políticas corporativas en relación con la seguridad cibernética es importante para proteger los activos corporativos desde una perspectiva de seguridad cibernética. Las empresas deben reconocer que, en el mundo empresarial actual impulsado por Internet, la conectividad de información electrónica es una parte integral de los negocios y, por lo tanto, la seguridad cibernética es esencial. Las transacciones comerciales no solo están contenidas en el firewall de Internet de la organización, sino que también se extienden a clientes, proveedores, contratistas externos y socios externos.

El alcance general del trabajo se debe precisar desde tres perspectivas diferentes: comercial, arquitectónica y funcional.

Desde una perspectiva empresarial, el alcance del trabajo debe responder preguntas similares a:

· ¿Qué corporaciones están incluidas?

· ¿Qué unidades de negocio están incluidas?

· ¿Qué regiones geográficas están incluidas?

· ¿Qué sitios específicos están incluidos?

Desde un punto de vista arquitectónico, el alcance del trabajo debe responder preguntas similares a:

· ¿Qué sistemas informáticos y redes se abordarán?

· ¿Se incluirán SCADA y los sistemas de monitoreo de distribución?

· ¿Se incluirán los sistemas informáticos no relacionados con la producción (tanto los admitidos como los no admitidos por la organización de TI)?

· ¿Se incluirán los sistemas de ejecución de fabricación (MES)?

· ¿Se incluirán los sistemas de gestión del quemador y el SIS?

· ¿Se incluirán los sistemas robóticos?

· ¿Se incluirán las conexiones con proveedores o clientes?

Desde el punto de vista funcional, el alcance del trabajo se puede dividir en las siguientes dos categorías:

a) Actividades de gestión directa de riesgos.

Estas son actividades que implican la evaluación, comunicación y priorización de riesgos. Los ejemplos incluyen la designación de propietarios locales de seguridad cibernética, la recopilación y el mantenimiento de un inventario de activos, el desarrollo y el mantenimiento de la arquitectura de la red, la realización de auditorías internas o externas y el informe de estos resultados en una unidad comercial o corporativa.

b) Proyectos relacionados con la gestión de riesgos.

Estas son actividades financiadas sobre la base de reducir los riesgos identificados por las actividades de gestión de riesgos. Estas soluciones de gestión de riesgos indirectos toman la forma de proyectos que están limitados en el tiempo y el desarrollo y despliegue de servicios en curso.

Al aclarar el alcance funcional, se deben considerar preguntas similares a las siguientes:

· ¿Cómo se relaciona el alcance de este trabajo con los sistemas de gestión de riesgos existentes?

· ¿Cómo se relaciona el alcance de este trabajo con las políticas de seguridad de la información que ya se aplican a estos sistemas y organizaciones?

· ¿Cómo se relaciona el alcance de este trabajo con las normas y procedimientos técnicos que ya se aplican a componentes arquitectónicos específicos (es decir, sistemas básicos de control de procesos, sistemas SCADA, SIS, sistemas de gestión de quemadores y sistemas robóticos)?

· ¿Cómo se relaciona el alcance de este trabajo con los proyectos que ya están financiados?

· ¿Cómo se relaciona el alcance de este trabajo con los servicios existentes?

El apoyo de los directivos proporciona el respaldo del esfuerzo por parte de los gerentes responsables de asignar recursos para administrar e implementar las tareas para reducir los riesgos para el IACS.

El alcance debe ser propiedad del líder ejecutivo del programa, que será responsable de guiar al equipo durante el desarrollo del programa. En última instancia, el líder será responsable de asegurarse de que el programa se ejecute, incluidas las comunicaciones, la financiación, la aplicación y la auditoría.

Con el apoyo y el compromiso de la dirección superior, se deben identificar las partes interesadas y se debe asignar su tiempo para trabajar en la mejora de la seguridad. Los interesados son responsables de hacer avanzar la iniciativa de seguridad. Con el apoyo de la dirección superior, las partes interesadas inician las próximas actividades y contratan los recursos adecuados para realizar las tareas. Forme un equipo integrado que involucre sistemas de computación convencionales y empresariales tradicionales, IACS y sistemas que

interactúen con clientes, distribuidores y proveedores de transporte. La carta y el alcance mencionados anteriormente se centran en quién debe participar para cumplir los objetivos de la iniciativa.

Es probable que los altos directivos puedan identificar a un líder de proyecto cuyo trabajo es reunir a las personas adecuadas para trabajar en el esfuerzo de seguridad. Esta persona deberá tener un conocimiento de alto nivel del estado actual de los procedimientos de seguridad cibernética en la empresa. Asumiendo que el objetivo es mejorar las políticas y procedimientos de seguridad cibernética para IACS, el líder del proyecto debe buscar las áreas que podrían verse afectadas por los incidentes de seguridad cibernética de IACS e identificar a las personas clave que son reconocidas como responsables / responsables de estas áreas. El enfoque debe estar en identificar a las personas en el rol correcto, independientemente de la organización a la que están asignadas.

Es importante tener en cuenta que las diferentes estructuras organizativas de la empresa pueden tener estas personas en diferentes organizaciones. El objetivo es desarrollar un CSMS rentable que aproveche los procesos y organizaciones comerciales existentes en lugar de crear una organización completamente nueva. Las personas que ya están en el papel correcto y con la experiencia adecuada deben seleccionarse cuando sea posible. Desglosar los problemas de campo puede ser una actividad importante de este equipo de partes interesadas.

El equipo central de partes interesadas debe ser de naturaleza cruzada y reunir habilidades que normalmente no se encuentran en una sola persona. El equipo debe incluir personas con los siguientes roles:

· Persona (s) IACS que pueden estar implementando y apoyando los dispositivos IACS;

· Persona (s) de operaciones responsables de hacer el producto y cumplir con los pedidos del cliente;

· Procesar a las personas de gestión de seguridad cuyo trabajo es garantizar que no ocurran incidentes de HSE;

· Persona (s) de TI que pueden ser responsables del diseño y operación de la red, soporte de escritorios y servidores, y similares;

· Personas de seguridad asociadas con la seguridad física y de TI en el sitio;

· Recursos adicionales que pueden estar en las funciones legales, de recursos humanos y de atención al cliente o cumplimiento de pedidos.

El conjunto de partes interesadas puede cambiar con el tiempo o las personas específicas pueden asumir roles de perfil más alto durante diferentes fases o actividades mientras desarrollan el CSMS. No es importante qué la organización lidere el esfuerzo, sino que el líder exhiba el correcto comportamiento fomentando el trabajo en conjunto, como un equipo con un propósito unificado. Las organizaciones principales con las cuales se alinean las personas mencionadas tienen algo que ofrecer y tienen interés en las decisiones y los resultados del CSMS.

A.3.2.2.3 Prácticas sugeridas.

A.3.2.2.3.1 Prácticas de referencia.

Las siguientes tres acciones son prácticas básicas:

a) Describir las organizaciones responsables de establecer, comunicar y monitorear la seguridad cibernética dentro de la empresa.

b) Establecer el alcance del CSMS, incluyendo:

- Sistemas de información: incluidos todos los sistemas operativos, bases de datos, aplicaciones, empresas conjuntas y actividades comerciales de terceros;
- IACS: incluye todos los sistemas de control de procesos, sistemas SCADA, PLC, DCS, estaciones de trabajo de configuración y sistemas de información de planta o laboratorio para datos históricos y en tiempo real;
- Redes, redes de área local (LAN), redes de área amplia (WAN) - incluyendo hardware, aplicaciones, firewalls, sistemas de detección de intrusos y similares;
- Puntos de integración con proveedores de soporte y servicios;
- Responsabilidades del usuario: incluidas políticas para abordar la autenticación y la auditabilidad;
- Protección de la información, incluidos los requisitos de acceso y la responsabilidad individual;
- Gestión de riesgos: incluidos los procesos para identificar y mitigar riesgos y documentar el riesgo residual;
- Recuperación ante desastres: incluida la identificación de software / servicios críticos;
- Requisitos de entrenamiento;
- Conformidad, cumplimiento y auditoría;
- Identificación de activos.

c) Caracterizar la organización responsable del CSMS, incluyendo:

- Estructura de la organización;
- Ubicación;
- Presupuesto;
- Roles y responsabilidades asociadas con los procesos CSMS.

A.3.2.2.3.2 Prácticas adicionales.

Las siguientes cinco acciones son prácticas adicionales:

a) Que la gerencia respalde el alcance y las responsabilidades del CSMS.

b) Tener una comprensión clara de las funciones y responsabilidades asociadas con la organización u organizaciones responsables de algún aspecto del CSMS.

c) Documentar el alcance del CSMS con subcláusulas separadas que aborden componentes específicos.

d) Abordar los requisitos y responsabilidades comerciales, legales (por ejemplo, privacidad de datos) y reglamentarios.

e) Identificar y documentar la dependencia de la seguridad del proceso de las prácticas y procedimientos de seguridad física y ciberseguridad, incluido un marco para la interacción organizacional.

A.3.2.2.4 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [24], [26].

A.3.2.3 Elemento: organización para la seguridad.

A.3.2.3.1 Descripción del elemento.

Las empresas deben establecer una organización, estructura o red de personas con la responsabilidad de la seguridad general, reconociendo que hay componentes físicos y cibernéticos que deben abordarse.

Es importante establecer la responsabilidad para proporcionar dirección y supervisión a la seguridad cibernética de una organización. La seguridad cibernética en el sentido más amplio cubre no solo los datos, sino también los sistemas (hardware y software) que generan o almacenan esta información e incluye también elementos de seguridad física. IACS, socios de la cadena de valor, contratistas externos, socios de empresas conjuntas, socios de subcontratación y especialistas en seguridad física deben ser considerados por la organización como parte de la estructura de seguridad general y, por lo tanto, incluidos en el alcance de la responsabilidad.

A.3.2.3.2 Construir un marco organizacional para la seguridad.

El compromiso con un programa de seguridad comienza en la parte superior. La alta gerencia deberá demostrar un claro compromiso con la seguridad cibernética. La seguridad cibernética es una responsabilidad comercial compartida por todos los miembros de la empresa y especialmente por los principales miembros de los equipos de negocios, fabricación, TI y gestión de riesgos. Los programas de seguridad cibernética con soporte visible de alto nivel y aceptación de los líderes de la organización tienen más probabilidades de obtener conformidad, funcionar de manera más efectiva y tener un éxito anterior.

Se debe establecer un marco de gestión para iniciar y controlar la implementación de un programa de seguridad general. El alcance y las responsabilidades de la seguridad cibernética para las organizaciones deben incluir la seguridad física y la seguridad cibernética para los sistemas de TI, proveedores de IACS, contratistas externos, socios de subcontratación y los componentes de la cadena de valor de la organización. Se debe extender un programa de seguridad general para incluir las operaciones de empresas conjuntas.

Las organizaciones deben establecer un marco con el liderazgo de la administración para aprobar la política de seguridad cibernética, asignar roles de seguridad y coordinar la implementación de la seguridad cibernética en toda la organización. El marco puede enfrentar algunos desafíos organizacionales interesantes. Muchas empresas están organizadas en una matriz tridimensional donde una dimensión es por línea de negocio, una segunda dimensión es por función o disciplina y una tercera dimensión es por región geográfica. Los gerentes individuales generalmente tienen responsabilidades para alguna parte de esta organización general. Debido a que un sistema es tan seguro como su eslabón más débil, en última instancia será necesario desarrollar un sistema de seguridad cibernética que abarque todo el alcance geográfico de la organización.

La seguridad cibernética aborda una serie de riesgos diferentes que generalmente se pueden clasificar en preocupaciones sobre disponibilidad, integridad o confidencialidad. Las inquietudes sobre la disponibilidad generalmente se gestionarían mediante un programa de planificación de continuidad del negocio o un programa de seguridad de red. Las inquietudes sobre la integridad en un contexto de fabricación generalmente se gestionan mediante un programa de seguridad de proceso o garantía de calidad. Las inquietudes sobre la confidencialidad generalmente son gestionadas por un programa de seguridad de la información. Debido a que la seguridad cibernética afecta tantas áreas de riesgo diferentes, es probable que ningún administrador tenga la responsabilidad necesaria de autorizar un programa de seguridad cibernética

para todos los IACS. A menudo será necesario convocar y convencer a un pequeño grupo de altos directivos que, posiblemente, nunca antes hayan tenido que trabajar juntos para tomar una decisión consensuada.

Una empresa en general (por ejemplo, una corporación) o suborganizaciones individuales dentro de la empresa pueden trabajar para cumplir con esta norma. Si la empresa en general debe cumplir, el riesgo se evalúa en toda la empresa. En este caso, por ejemplo, las plantas individuales dentro de la corporación pueden llevar a cabo evaluaciones de riesgos, pero utilizarán una metodología común de evaluación de riesgos que permite la recopilación de estas evaluaciones a nivel corporativo. Por lo tanto, si una empresa en general tiene el objetivo de lograr la conformidad, será necesario establecer pautas para respaldar esto, incluso si las suborganizaciones individuales, como las plantas, hacen gran parte del trabajo.

Otras posibilidades son que la empresa en general no intente cumplir con la norma, sino que solicite a sus suborganizaciones en algún nivel que lo hagan individualmente o que algunas suborganizaciones intenten cumplir la norma por su propia iniciativa. En cualquiera de estos casos, la empresa aún necesitará apoyar a estas suborganizaciones para cumplir con los requisitos específicos en la nrma que se manejan a nivel de la empresa, tales como asegurar arquitecturas proporcionadas por la empresa, selección de empleados y redacción de contratos con proveedores de servicios. Bajo estos escenarios, por ejemplo, un sitio de planta individual podría tener su propia metodología de evaluación de riesgos, determinar sus propias prioridades de mitigación y tener una alta gerencia a nivel de planta que respalde el esfuerzo. Y en estos casos, la empresa no está evaluando su propia conformidad general con la norma, aunque potencialmente podría evaluar la conformidad de las plantas individuales. Esta estrategia tendría más sentido para una corporación diversa altamente descentralizada u otra empresa.

A.3.2.3.3 Comenzar y obtener soporte.

Para que los gerentes superiores defiendan efectivamente un programa de seguridad cibernética, deben estar convencidos de que los costos del programa que pagarán con sus presupuestos serán menores que el impacto de la amenaza en sus áreas de responsabilidad. Puede ser necesario desarrollar una justificación comercial o un caso comercial para administrar los riesgos de seguridad cibernética para convencer al liderazgo de que respalde el programa. Las responsabilidades presupuestarias y los ámbitos de responsabilidad deberán aclararse entre los altos directivos.

Debido a las limitaciones de tiempo, muchos gerentes superiores tienen asesores de confianza que utilizan para filtrar los problemas importantes que necesitan abordar de los problemas que otros están más capacitados para afrontar. Estas personas son especialistas en información. En las organizaciones grandes, con frecuencia hay organizaciones de personal que los gerentes superiores utilizan para generar recomendaciones para problemas técnicamente complejos. Puede ser necesario trabajar con estas organizaciones de personal inicialmente para recopilar información suficiente para hacer el caso comercial. Estas organizaciones también pueden proporcionar información sobre qué gerentes suelen manejar tipos específicos de riesgos.

Es probable que los altos directivos puedan identificar a un líder de proyecto cuyo trabajo es reunir a las personas adecuadas para trabajar en el esfuerzo de seguridad. Esta persona deberá tener un conocimiento de alto nivel del estado actual de los procedimientos de seguridad cibernética en la empresa. Es importante reconocer que un CSMS verdaderamente integrado involucra sistemas de computación tradicionales y empresariales tradicionales, IACS y sistemas de cadena de valor que interactúan con clientes, proveedores y proveedores de transporte. La carta y el alcance mencionados anteriormente se centran en quién debe participar para cumplir los objetivos de la iniciativa.

El líder del proyecto debe buscar las áreas que podrían verse afectadas por los incidentes de seguridad cibernética de IACS e identificar a las personas clave que se reconocen como responsables / responsables de estas áreas. El enfoque debe estar en identificar a las personas en el rol correcto, independientemente de la organización a la que están asignadas.

Es importante tener en cuenta que las diferentes estructuras organizativas de la empresa pueden tener estas personas en diferentes organizaciones. El objetivo es desarrollar un CSMS rentable que aproveche los procesos y organizaciones comerciales existentes en lugar de crear una organización completamente nueva. Las personas que ya están en el papel correcto y con la experiencia adecuada deben seleccionarse siempre que sea posible. Desglosar los problemas de campo puede ser una actividad importante de este equipo de partes interesadas.

El equipo central de partes interesadas debe ser de naturaleza cruzada y reunir habilidades que normalmente no se encuentran en una sola persona. El equipo debe incluir personas con los siguientes roles:

· Persona (s) IACS que pueden estar implementando y apoyando los dispositivos IACS;

· Persona (s) de operaciones responsables de hacer el producto y cumplir con los pedidos del cliente;

· Procesar a la (s) persona (s) de gestión de seguridad cuyo trabajo es asegurar que no ocurran incidentes ambientales, de salud y seguridad;

· Persona (s) de TI que pueden ser responsables del diseño y operación de la red, soporte de escritorios y servidores, y similares;

· Personas de seguridad asociadas con la seguridad física y de TI en el sitio;

· Recursos adicionales que pueden estar en las funciones legales, de recursos humanos y de atención al cliente o cumplimiento de pedidos.

El conjunto de partes interesadas puede cambiar con el tiempo o las personas específicas pueden asumir roles de perfil más alto durante diferentes fases o actividades mientras desarrollan el CSMS. No es importante qué la organización lidere el esfuerzo, sino que el líder exhiba el correcto comportamiento fomentando el trabajo en conjunto, como un equipo con un propósito unificado. Las organizaciones principales con las cuales se alinean las personas mencionadas tienen algo que ofrecer y tienen interés en las decisiones y los resultados del CSMS.

Una práctica común para convencer al gerente superior es probar nuevos programas en una pequeña región geográfica o en un sitio en particular para demostrar que los nuevos procedimientos / programas funcionan antes de dedicar una gran cantidad de recursos. Este puede ser otro enfoque efectivo para obtener acceso a los gerentes senior o realmente hacer el caso de negocios a los gerentes senior.

Una vez que los gerentes superiores apropiados han sido identificados, es importante decidir si presentar el CSMS a todos ellos como un grupo o acercarse a ellos secuencialmente. Es más eficiente convencerlos a todos simultáneamente, pero puede que no todos sean receptivos a la discusión simultáneamente. Si es necesario persuadir a un equipo de liderazgo, es útil identificar un aliado en el equipo de liderazgo para revisar la presentación y ofrecer comentarios antes de hacer la presentación a todo el equipo. Debido a la cantidad de áreas de riesgo diferentes que se ven afectadas por la seguridad cibernética, no es raro exigir la persuasión de más de un equipo de liderazgo.

Si los costos del programa de seguridad cibernética no se pueden determinar inicialmente debido a la falta de un inventario de computadoras o la falta de contramedidas normalizadas, se puede requerir una segunda ronda de presentaciones una vez que estos costos se determinen con mayor precisión. El énfasis en esta etapa inicial debe estar en establecer un sistema para equilibrar los costos de las contramedidas con los costos de los riesgos. Por lo general, hay información inadecuada en esta etapa para solicitar un presupuesto específico para implementar contramedidas.

A.3.2.3.4 Prácticas de apoyo.

A.3.2.3.4.1 Prácticas de referencia.

Las siguientes cinco acciones son prácticas básicas:

a) Obtener el compromiso de la dirección ejecutiva para establecer un marco organizacional para abordar la seguridad.

b) Asignar la responsabilidad de la seguridad física y cibernética al personal con un nivel adecuado de financiación para implementar políticas de seguridad.

c) Iniciar un equipo (u organización) de seguridad en toda la empresa para proporcionar una dirección, compromiso y supervisión eficiente. El equipo puede ser una red informal, estructura organizativa o jerárquica que abarca diferentes departamentos u organizaciones de la empresa. Este equipo asigna responsabilidades y confirma que existen procesos comerciales para proteger los activos y la información de la empresa.

d) Establecer o modificar contratos para abordar las políticas y procedimientos de seguridad física y cibernética de socios comerciales, contratistas externos, socios de subcontratación y similares, donde las políticas y procedimientos de seguridad de esos socios externos afectan la seguridad de la IACS.

e) Coordinar o integrar la organización de seguridad donde exista una superposición y / o sinergia entre los riesgos de seguridad física y cibernética.

A.3.2.3.4.2 Prácticas adicionales.

Las siguientes cuatro acciones son prácticas adicionales:

a) Establecer la responsabilidad de la seguridad cibernética de IACS:

· Un solo individuo es responsable de la seguridad cibernética de toda la organización. Este individuo preside un equipo multifuncional que representa las diversas unidades de negocios y departamentos funcionales. El equipo demuestra un compromiso con la seguridad cibernética y establece una dirección clara para la organización. Esto incluye la propiedad de activos y operaciones industriales, así como proporcionar los recursos apropiados para abordar los problemas de seguridad.

· Un equipo separado es responsable de la seguridad de IACS bajo una organización de fabricación o ingeniería. Si bien este enfoque tiene la ventaja de tener un liderazgo conocedor de los riesgos asociados con IACS, los beneficios de dicho enfoque se pueden perder si este equipo no se coordina estrechamente con los responsables de los activos de TI tradicionales y la seguridad física.

· Un equipo de seguridad general es responsable de los activos físicos y lógicos. En esta estructura jerárquica, la seguridad está bajo una única organización con equipos separados responsables de los sistemas físicos y de información. Este enfoque es útil en organizaciones más pequeñas donde los recursos pueden ser limitados.

b) Coordinar los esfuerzos con los organismos encargados de hacer cumplir la ley, los reguladores y los proveedores de servicios de Internet junto con otras organizaciones relevantes, en lo que se refiere a terroristas u otras amenazas externas. Las organizaciones que han establecido relaciones con el personal local de respuesta a emergencias amplían estas relaciones para incluir el intercambio de información y la respuesta a incidentes de seguridad cibernética.

c) Mantener a los proveedores externos que tienen un impacto en la seguridad de la organización con las mismas políticas y procedimientos de seguridad para mantener el nivel general de seguridad de IACS. Las políticas y procedimientos de seguridad de los proveedores de segundo y tercer nivel también deben cumplir con las políticas y procedimientos corporativos de seguridad cibernética si impactan la seguridad de IACS:

· Las empresas deberían considerar el aumento del riesgo de seguridad asociado con la contratación externa como parte del proceso de toma de decisiones para determinar qué externalizar y externalizar la selección de socios.

· Contratos con proveedores externos que rigen el acceso físico y lógico;

· Las expectativas de confidencialidad o no divulgación y los derechos de propiedad intelectual deben estar claramente definidos;

· Los procedimientos de gestión del cambio deben estar claramente definidos.

d) Eliminar el acceso de proveedores externos al finalizar / rescindir el contrato. La puntualidad de esto es crítica y se detalla claramente en el contrato.

A.3.2.3.5 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [23], [26], [30], [43].

A.3.2.4 Elemento: capacitación del personal y concientización de seguridad.

A.3.2.4.1 Descripción del elemento.

La concientización de seguridad para todo el personal es una herramienta esencial para reducir los riesgos de seguridad cibernética. El personal experto y atento es una de las líneas de defensa más importantes para asegurar cualquier sistema. En el área de IACS, se pondrá el mismo énfasis en la seguridad cibernética que en la seguridad y la integridad operativa, porque las consecuencias pueden ser igual de graves. Por lo tanto, es importante que todo el personal (empleado, contrato o tercero) comprenda la importancia de la seguridad para mantener el funcionamiento del sistema. Los programas de capacitación del personal y de concientización de seguridad brindan a todo el personal (empleados, contratistas y similares) la información necesaria para identificar, revisar, abordar y, cuando corresponda, remediar vulnerabilidades y amenazas a IACS y ayudar a garantizar que sus propias prácticas laborales incluyan contramedidas efectivas. Todo el personal debe recibir capacitación técnica adecuada asociada con las amenazas y vulnerabilidades conocidas de hardware, software e ingeniería social. Los programas de capacitación en seguridad cibernética y concientización de seguridad son más efectivos si se adaptan a la audiencia, son consistentes con la política de la compañía y se comunican regularmente. La capacitación proporciona un medio para comunicar mensajes clave al personal de manera oportuna. Un programa de capacitación eficaz puede ayudar a los empleados a comprender por qué se requieren controles de seguridad nuevos o actualizados y generar ideas que puedan usar para reducir los riesgos y el impacto en la organización si no se incorporan métodos de control.

A.3.2.4.2 Desarrollar un programa de capacitación del personal y crear concientización sobre la seguridad.

La capacitación de un tipo u otro es una actividad que abarca casi todo el período durante el cual se desarrolla e implementa un CSMS. Comienza después de que se aclara el alcance del esfuerzo y se identifica el equipo de partes interesadas. El objetivo del programa de capacitación es proporcionar a todo el personal la información que necesitan para que estén al tanto de cualquier posible amenaza para el sistema y sus responsabilidades para la operación segura de las instalaciones de producción.

La organización debe diseñar y desarrollar un programa de capacitación en seguridad cibernética junto con el programa de capacitación general de la organización. La capacitación debe ser en dos fases: 1) capacitación general para todo el personal y 2) capacitación basada en roles dirigida a tareas y responsabilidades específicas. Antes de comenzar el desarrollo del programa de capacitación, es importante identificar el alcance y los límites de la capacitación e identificar y definir los diversos roles dentro de la organización.

El programa de capacitación general debe desarrollarse para todo el personal. Los usuarios deben estar capacitados en los procedimientos de seguridad correctos, el uso correcto de las instalaciones de procesamiento de información y el manejo correcto de la información para minimizar los riesgos. La capacitación también debe incluir responsabilidades legales, controles comerciales y responsabilidades de seguridad individuales.

La capacitación basada en roles debe enfocarse en los riesgos y responsabilidades de seguridad asociados con el rol específico que una persona desempeña dentro de la organización. Estas personas necesitarán una capacitación más específica e intensiva. Se deben emplear expertos en la materia para contribuir a esta capacitación. La capacitación basada en roles puede llevarse a cabo en el aula, puede ser basada en la web o práctica. Esta capacitación también puede aprovechar la capacitación brindada por los proveedores para una discusión en profundidad de las herramientas y exposiciones asociadas.

El programa debe incluir un medio para su revisión, según sea necesario, y un medio para evaluar la efectividad del programa. Además, debe haber un tiempo definido para el reentrenamiento periódico.

El compromiso de la gerencia con la capacitación y garantizar una concientización de seguridad cibernética adecuada es fundamental para proporcionar un entorno informático estable y seguro tanto para TI como para IACS. En particular para el entorno IACS, un entorno informático estable y seguro ayuda a mantener el funcionamiento seguro del equipo bajo control y a reducir los incidentes de HSE. Esto debería ser en forma de recursos para desarrollar y organizar la capacitación y hacer que el personal esté disponible para asistir.

Tras el desarrollo de un programa de capacitación en seguridad cibernética, la organización debe proporcionar la capacitación adecuada para todo el personal. Los programas de capacitación deben proporcionarse en un lugar y en momentos que permitan capacitar al personal sin afectar negativamente sus otras responsabilidades.

Se debe proporcionar capacitación general como parte de la orientación de un nuevo empleado y como parte de la orientación para el personal contratado, temporal o de terceros. La capacitación requerida debe ser apropiada para el nivel de contacto que tendrán con la organización. Se puede proporcionar capacitación especializada de la siguiente manera:

a) Capacitación para los interesados.

La capacitación es apropiada para el equipo de partes interesadas, así como para la comunidad de personas del IACS que finalmente se verán afectadas. El equipo de partes interesadas necesitará capacitación específica sobre el tipo de riesgos que se están considerando, el alcance y la carta de trabajo que la gerencia ha aprobado, cualquier información de antecedentes sobre incidentes que hayan ocurrido a estos sistemas, ya sea dentro de la organización o dentro de la industria en general. y sobre los tipos de arquitecturas y sistemas que están en uso dentro de la organización. La capacitación formal en el aula no es necesaria para compartir esta información. Las presentaciones en reuniones de negocios, sesiones de comunicación y anuncios por correo electrónico son ejemplos de formas de compartir la información.

b) Capacitar a los empleados que se preparan para nuevos roles.

Se necesitará capacitación para los empleados mientras se preparan para asumir nuevas funciones dentro del sistema de gestión de riesgos directos o dentro de los proyectos relacionados con la gestión de riesgos. Prácticamente todos los miembros de la comunidad IACS recibirán una cierta cantidad de capacitación durante esta fase. Algunos de los roles de gestión de riesgos directos incluirán responsabilidades para autoevaluaciones o auditorías internas.

c) Formación de auditores.

Se necesitará capacitación para que los auditores comprendan la naturaleza de los sistemas y redes que auditarán, así como las políticas específicas que se han creado.

d) Entrenamiento continuo.

Habrá una necesidad continua de capacitación en todos los niveles debido a la incorporación de nuevos empleados y personal de terceros, la necesidad de proporcionar actualizaciones a medida que las políticas y servicios se modifiquen con el tiempo y proporcionar capacitación de actualización para garantizar que el personal siga siendo competente en sus funciones y responsabilidades.

Es importante validar que el personal conozca sus roles y responsabilidades como parte del programa de capacitación. La validación de la concientización de seguridad proporciona dos funciones: 1) ayuda a identificar qué tan bien comprende el personal el programa de seguridad cibernética de la organización y 2) ayuda a evaluar la efectividad del programa de capacitación. La validación puede venir a través de varios medios, incluidas las pruebas escritas sobre el contenido de la capacitación, las evaluaciones del curso, el desempeño laboral monitoreado o los cambios documentados en el comportamiento de seguridad. Se debe acordar un método de validación durante el desarrollo del programa de capacitación y comunicarlo al personal.

Los registros de la capacitación de los empleados y los horarios para las actualizaciones de capacitación deben mantenerse y revisarse periódicamente. Documentar la capacitación puede ayudar a la organización a garantizar que todo el personal tenga la capacitación requerida para sus roles y responsabilidades particulares. También puede ayudar a identificar si se necesita capacitación adicional y cuándo se requiere capacitación periódica.

Con el tiempo, las vulnerabilidades, las amenazas y las medidas de seguridad asociadas cambiarán. Estos cambios requerirán cambios en el contenido del programa de capacitación. El programa de capacitación debe revisarse periódicamente (por ejemplo, anualmente) para determinar su efectividad, aplicabilidad, contenido y coherencia con las herramientas que se utilizan actualmente y las prácticas y leyes corporativas, y revisarse según sea necesario. Las suscripciones a servicios de alerta de seguridad pueden ayudar a garantizar un conocimiento actualizado de las vulnerabilidades y exposiciones recientemente identificadas.

A.3.2.4.3 Prácticas de apoyo.

A.3.2.4.3.1 Prácticas de referencia

Las siguientes siete acciones son prácticas básicas:

a) Abordar los diversos roles asociados con el mantenimiento de un entorno de sistemas seguros dentro de los currículos de capacitación en seguridad cibernética.

b) Tener cursos en el aula o capacitación en el trabajo para abordar los requisitos para cada función.

c) Validar la comprensión de un usuario a través de evaluaciones y / o exámenes del curso.

d) Tener expertos en la materia para cada curso que puedan proporcionar información adicional y consultoría.

e) Revisar y validar el currículo de capacitación periódicamente y evaluar su efectividad.

f) Comunicar mensajes clave a todo el personal de manera oportuna a través de un programa de comunicación de concientización de seguridad.

g) Capacitar a todo el personal inicialmente y periódicamente después (por ejemplo, anualmente).

Si bien ninguna de estas prácticas de línea de base es específica para la capacitación en seguridad de IACS, el énfasis y el contenido de los programas de capacitación deben mostrar la relación entre la seguridad de IACS y las consecuencias de HSE.

A.3.2.4.3.2 Prácticas adicionales

Las siguientes siete acciones son prácticas adicionales:

a) Establecer la capacitación en seguridad cibernética como un componente de la organización de capacitación general de la compañía para todos los empleados.

b) Adaptar los currículos de capacitación en seguridad cibernética con una progresión de material para un rol determinado en la organización.

c) Mantener y revisar los registros de capacitación de los empleados y los horarios para las actualizaciones de capacitación de forma regular, dependiendo de su puesto / función.

d) Aprovechar la capacitación en seguridad cibernética proporcionada por los proveedores.

e) Establecer el momento, la frecuencia y el contenido del programa de comunicación de concientización de seguridad en un documento para mejorar la comprensión de las organizaciones sobre los controles de seguridad cibernética.

f) Incluyendo una visión general del programa de comunicación y concientización de seguridad para todo el personal para garantizar que conozcan las prácticas de seguridad en su primer día.

g) Revisar anualmente la capacitación y el programa de concientización de seguridad por su efectividad, aplicabilidad, contenido y consistencia con las herramientas actualmente utilizadas y las prácticas corporativas.

A.3.2.4.4 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [2], [23], [24], [26].

A.3.2.5 Elemento: Plan de continuidad del negocio.

A.3.2.5.1 Descripción del elemento.

Un plan de continuidad del negocio identifica procedimientos para mantener o restablecer operaciones comerciales esenciales mientras se recupera de una interrupción significativa. El propósito del plan de continuidad del negocio es proporcionar un curso de acción para responder a las consecuencias de desastres, fallas de seguridad y pérdida de servicio a un negocio. Un plan detallado de continuidad del negocio asegura que los sistemas IACS críticos del negocio puedan restaurarse y utilizarse lo antes posible después de que ocurra una interrupción significativa.

A.3.2.5.2 Alcance del plan de continuidad del negocio.

Antes de desarrollar el plan de continuidad del negocio, es importante comprender cuándo se debe usar el plan y qué tipo de situaciones se aplican. Las interrupciones no planificadas pueden tomar la forma de un desastre natural (es decir, huracán, tornado, terremoto o inundación), un evento no intencional provocado por el hombre (es decir, daño accidental del equipo, incendio o explosión o error del operador), un evento intencional provocado por el hombre (es decir, ataque por bomba, arma de fuego, vandalismo, pirata informático o virus) o una falla del equipo. Desde una perspectiva de interrupción potencial, esto puede implicar intervalos de tiempos típicos de minutos u horas para recuperarse de muchas fallas mecánicas, a días y semanas o meses para recuperarse de un desastre natural. Debido a que a menudo existe una disciplina separada que se ocupa de la confiabilidad y el mantenimiento eléctrico / mecánico, algunas organizaciones eligen definir la continuidad del negocio de una manera que excluya estas fuentes de falla. Dado que la continuidad del negocio también se ocupa principalmente de las implicaciones a largo plazo de los cortes de producción, algunas organizaciones también optan por establecer un límite mínimo de interrupción en los riesgos a considerar. A los efectos de la seguridad cibernética de IACS, se recomienda que no se imponga ninguna de estas restricciones. Las interrupciones a largo plazo (recuperación ante desastres) y las interrupciones a corto plazo (recuperación operativa) deben considerarse. El plan también incluye otros aspectos de la recuperación ante desastres, como la gestión de emergencias, los recursos humanos y las relaciones con los medios o la prensa.

Debido a que algunas de estas interrupciones potenciales involucran eventos provocados por el hombre, también es importante trabajar en colaboración con la organización de seguridad física para comprender los riesgos relativos de estos eventos y las contramedidas de seguridad física para prevenirlos. También es importante que la organización de seguridad física comprenda qué áreas de un sitio de producción acogen IACS que podrían presentar riesgos de mayor nivel.

A.3.2.5.3 El proceso de planificación de continuidad del negocio.

Antes de crear un plan para hacer frente a posibles interrupciones, es importante especificar los objetivos de recuperación para los diversos sistemas y subsistemas involucrados en función de las necesidades del negocio típicas. La recuperación del sistema implica la restauración de todos los enlaces de comunicación y las capacidades de IACS y generalmente se especifica en términos de un objetivo de tiempo de recuperación o el tiempo para recuperar estos enlaces y capacidades. La recuperación de datos implica la restauración de información que describen la producción o las condiciones del producto en el pasado y generalmente se especifica en términos de un objetivo de punto de recuperación o el período de tiempo más largo durante el cual se puede tolerar la ausencia de datos.

Una vez que se definen los objetivos de recuperación, se debe crear una lista de posibles interrupciones y desarrollar y documentar el procedimiento de recuperación. Para la mayoría de las interrupciones a menor escala, las actividades de reparación y reemplazo basadas en un inventario de repuestos críticos pueden resultar adecuadas para cumplir con los objetivos de recuperación. En otros casos, se deben desarrollar planes de contingencia. Debido al costo potencial de estos planes de contingencia, estos deben revisarse con los gerentes responsables de la planificación de la continuidad del negocio para verificar que estén justificados.

Se deben identificar los requisitos para un equipo de continuidad del negocio y se debe formar un equipo. El equipo debe incluir IACS y otros propietarios de operaciones industriales. En caso de una interrupción significativa, este equipo debe determinar la prioridad de los sistemas críticos de negocios y IACS para restablecer las operaciones.

Se debe desarrollar un cronograma para evaluar todo o parte de los procedimientos de recuperación. A menudo, los procedimientos para un subsistema específico se prueban anualmente y el subsistema específico se rota para que los procedimientos generales del sistema finalmente se prueben durante un período de 5-10 años. Estas frecuencias son solo ejemplos y serán determinadas por la organización como parte del proceso de planificación.

Se debe prestar especial atención a la verificación de las copias de seguridad para los datos de configuración del sistema y los datos del producto o producción. No solo deben probarse en la implemntacion, los procedimientos de almacenamiento también deben revisarse con cierta frecuencia para verificar que las copias de seguridad y los datos de respaldo sean utilizables y precisos. Estas copias de seguridad deben mantenerse en condiciones ambientales que no las vuelvan inutilizables y en un lugar seguro donde puedan ser obtenidas rápidamente por personas autorizadas cuando sea necesario.

En el caso de que ocurra un incidente, se le puede solicitar a la organización que brinde datos forenses sobre el incidente a los investigadores, ya sea dentro o fuera de la organización.

Con el tiempo, el plan de continuidad del negocio deberá revisarse y examinarse para reflejar los cambios en la estructura de gestión, organización, modelo de negocio, industria y similares.

A.3.2.5.4 Prácticas de apoyo.

A.3.2.5.4.1 Prácticas de referencia.

Las siguientes diecinueve acciones son prácticas básicas:

a) Formar un equipo de continuidad del negocio que involucre a las partes claves interesadas de la organización (es decir, dueños de negocios, personal de TI y personal de IACS) para desarrollar el plan.

b) Determinar la prioridad de los negocios críticos y los IACS en función de la naturaleza del sistema y el tiempo requerido para la restauración. Esto depende de la tolerancia al riesgo y los objetivos de recuperación de la organización.

c) Determinar la cantidad de tiempo / recursos necesarios para la restauración del sistema, la ubicación de los archivos de copia de seguridad, el hardware, la frecuencia de las copias de seguridad, la necesidad de repuestos dinámicos y similares, para garantizar que los sistemas críticos puedan restaurarse en caso de una situación de desastre.

d) Requerir que los registros relacionados con la gestión de documentos y los procedimientos de copia de seguridad / recuperación estén fácilmente disponibles en múltiples formas desde múltiples ubicaciones (es decir, copias electrónicas almacenadas en una bóveda y copias en papel en el sitio y en una instalación protegida) para que no haya un solo punto de falla.

e) Considerar el posible impacto en terceros, como empresas conjuntas y cadenas de suministro.

f) Determinar la necesidad de un seguro comercial adicional.

g) Definir los roles y responsabilidades específicos para cada parte del plan. Algunas organizaciones dividen al equipo en sub-equipos que informan a un comité coordinador. Ejemplos de sub-equipos incluyen evaluación de daños, restauración y recuperación, comunicaciones (internas y externas) y respuesta a emergencias.

h) Asignar la responsabilidad de iniciar el plan de continuidad del negocio y definir claramente las circunstancias bajo las cuales activar el plan.

i) Detallar bajo qué circunstancias tomar medidas específicas de emergencia. La elección de las medidas varía según el escenario específico. Considere las consecuencias de un desastre de TI o IACS que tenga un impacto físico en las instalaciones de producción.

j) Definir el tipo, número e identidad de los recursos necesarios y sus asignaciones.

k) Detallar los métodos de comunicación para los miembros del equipo junto con las contingencias por pérdida de correo electrónico, interrupción del teléfono y similares en caso de un desastre a gran escala.

l) Definir la frecuencia y el método para probar, validar y evaluar el plan de continuidad y usar estos resultados para mejorar y actualizar el plan para una mayor efectividad.

m) Detallar los riesgos asociados con la operación bajo el plan de continuidad y cómo se abordarán y / o mitigarán.

n) Identificar datos que requieren un manejo y protección especiales, así como la información que es crítica para la operación continua.

o) Establecer procedimientos provisionales para continuar con las operaciones comerciales mínimas. Una lista reducida de productos puede ser apropiada durante este período intermedio.

p) Identificar y almacenar sistemas de respaldo (hardware, software y documentación) en un lugar seguro.

q) Probar sistemas de respaldo en un horario predefinido para la operación adecuada del sistema y la restauración correcta de los datos.

r) Identificar y / o almacenar suministros para apoyar al equipo de respuesta a emergencias y ayudar a restaurar las operaciones comerciales (por ejemplo, agua embotellada, duchas de desintoxicación y paquetes de aire o respiradores de emergencia).

s) Definir el proceso para reanudar las operaciones normales.

A.3.2.5.4.2 Prácticas adicionales.

Las siguientes nueve acciones son prácticas adicionales:

a) Priorizar los sistemas de TI y los IACS por sus consecuencias para el negocio u operación en función de la tolerancia al riesgo de la organización. El IACS puede tener un impacto en los sistemas de TI empresariales que podrían pasarse por alto sin examinar y priorizar colectivamente los sistemas en su conjunto. La planificación de desastres y los planes de recuperación deben abordar la interrelación de estos sistemas.

b) Localizar copias de seguridad críticas del sistema en diferentes áreas geográficas. Si esto no es factible, almacenar datos y equipos de respaldo en un área no sujeta al mismo desastre físico que el sistema primario (es decir, terreno elevado para inundaciones o búnker de concreto para tornados).

c) Probar y actualizar los planes de continuidad del negocio periódicamente o según sea necesario.

d) Vincular los planes de continuidad del negocio con un sistema de gestión de cambio que garantice una actualización del plan de continuidad del negocio en caso de cambios significativos en el sistema o consecuencia del negocio.

e) Probar los planes de comunicación periódicamente o según sea necesario y asignar la responsabilidad de mantener las listas de llamadas actualizadas.

f) Proporcionar información de contacto crítica al equipo central (una tarjeta que lleva cada miembro del equipo).

g) Hacer que cada persona del equipo guarde copias escritas del plan en casa.

h) Tener procedimientos y / o contratos para comprar hardware, software y suministros adicionales si es necesario. Es importante que el plan de continuidad equilibre los tiempos de reemplazo para IACS con los tiempos de reemplazo para el equipo que se controla. En algunos casos, este equipo puede tener largos plazos de reparación / reemplazo que exceden en gran medida el tiempo de reemplazo de los sistemas de control.

i) Establecer acuerdos de nivel de servicio avanzado con proveedores de un servicio de recuperación de desastres.

A.3.2.5.5 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [23], [37], [48], [51].

A.3.2.6 Elemento: políticas y procedimientos de seguridad.

A.3.2.6.1 Descripción del elemento.

Dentro de cada sistema de gestión, hay un conjunto de requisitos generales que debe cumplir el sistema y listas de las organizaciones que están sujetas a estos requisitos. En esta norma, esos requisitos se denominan políticas. También hay descripciones de cómo los individuos y las organizaciones cumplen con los requisitos del sistema de gestión. En esta norma, estas descripciones se denominan procedimientos.

Para un CSMS, las políticas proporcionan una guía de alto nivel sobre los requisitos de seguridad cibernética dentro de la organización. Contienen directivas que abordan cómo una organización define la seguridad cibernética, opera su programa de seguridad cibernética y aborda su tolerancia al riesgo. Las políticas para el CSMS se crean a partir de políticas corporativas de nivel superior de las cuales derivan su autoridad. Las políticas conllevan consecuencias negativas por falta de cumplimiento, posiblemente incluyendo la terminación del empleo o incluso el enjuiciamiento penal.

Los procedimientos proporcionan detalles sobre cómo se implementan las políticas CSMS dentro de la organización. Puede que no sean tan estrictos como las políticas y pueden incluir disposiciones para obtener excepciones, ya que es muy difícil elaborar procedimientos para abordar adecuadamente cada situación o contingencia posible.

Las políticas y procedimientos del CSMS redactados por la organización deben brindar al personal una comprensión clara de sus roles y responsabilidades para asegurar los activos de la organización.

A.3.2.6.2 Desarrollo de políticas de seguridad.

El desarrollo de políticas de seguridad para la organización no debe abordarse como una tarea lineal. Una vez que se han completado las etapas iniciales del desarrollo de políticas, es necesario que la organización revise y analice la efectividad de esas políticas y luego las refine según sea necesario. Estas políticas no deben desarrollarse de manera aislada de otros sistemas de gestión de riesgos en la organización.

El desarrollo e implementación de políticas de seguridad implica un compromiso de liderazgo superior de todas las áreas de la organización con responsabilidad para este tipo de sistemas. Al definir y respaldar una política de seguridad, los altos directivos pueden demostrar un compromiso con la mejora continua. El compromiso de liderazgo relacionado con las políticas de seguridad implica que la organización reconoce la política de seguridad como una responsabilidad comercial compartida por todos los miembros del equipo de gestión y como una política que incluye componentes físicos y cibernéticos. Los procedimientos de seguridad deben incorporarse a las estrategias del negocio generales y contar con soporte administrativo.

Muchas organizaciones de IACS tienen políticas existentes para sistemas como seguridad, seguridad física, TI y comportamiento de los empleados. Al comenzar el proceso de desarrollo de un CSMS, es importante intentar integrar las políticas de seguridad cibernética en ese sistema con las políticas y procedimientos existentes. Esto puede y a menudo requiere, la modificación de políticas dentro de esos otros sistemas de gestión de riesgos. Por ejemplo, los sistemas de gestión de riesgos existentes pueden haber caracterizado los riesgos o establecer niveles de tolerancia al riesgo que deben entenderse al desarrollar el nuevo CSMS. Se puede encontrar una explicación de la combinación de políticas y sistemas de gestión de riesgos en IEC / TS 62443 - 1 - 1, 5.6. Las políticas de seguridad que abordan los riesgos de IACS también abordarán una amplia gama de problemas, desde los requisitos de liderazgo de la organización hasta los requisitos de configuración del sistema técnicamente detallados. Se recomienda que estas políticas se separen en subgrupos apropiados para que sean más accesibles para los lectores que solo estén interesados en temas específicos.

En muchas circunstancias, las políticas y procedimientos de seguridad pueden considerarse contramedidas para abordar el riesgo. Estos pueden tomar varias formas, desde procedimientos administrativos hasta herramientas de seguridad automatizadas. El objetivo es hacer que el costo general de las contramedidas sea menor que el impacto general del riesgo. Reducir el costo para implementar las contramedidas mientras se logra el mismo nivel de reducción de riesgos proporciona más valor a la organización. En los casos en que la economía de escala existe, la disciplina de TI administrará las tecnologías en las que se puede aprovechar la escala. Por lo tanto, las políticas de seguridad detalladas de la disciplina de TI deben ser examinadas en busca de una potencial aplicación en el espacio IACS.

Al desarrollar políticas de seguridad cibernética, es importante tener en cuenta los requisitos de conformidad y cumplimiento y el proceso de auditoría también. Dado que el IACS deberá ser evaluado por su cumplimiento con las políticas de seguridad, es necesario asegurarse de que las políticas definidas no entren en conflicto con otras políticas de gestión de riesgos posiblemente más importantes. Por ejemplo, se crea una política de seguridad que requiere que todas las computadoras de escritorio estén protegidas con contraseña en una determinada instalación nuclear. Esta política general también requiere que todas las estaciones del operador en la sala de control estén protegidas con contraseña, pero estas estaciones del operador deben estar abiertas debido a las normas de seguridad. La política de contraseña para las computadoras de escritorio

haría que el sistema no cumpla con las políticas de HSE. La política de ciberseguridad debería haberse redactado originalmente teniendo en cuenta el efecto que tendría en todos los diferentes sistemas en una instalación en particular. Un mejor enfoque sería definir una política que establezca que las computadoras de escritorio deben protegerse contra el uso no autorizado y luego tener procedimientos que pueden requerir protección con contraseña en algunos casos, mientras que proporcionan aislamiento físico en otras situaciones.

A.3.2.6.3 Determinación de la tolerancia de la organización al riesgo.

Una organización debe definir una política de tolerancia al riesgo relacionada con los niveles de riesgo, que corresponda a una combinación particular de probabilidad y consecuencia. Esta política puede basarse en una evaluación de riesgos cualitativa que consiste en una lista de activos o escenarios con una probabilidad general y una clasificación de consecuencias, que se definen y asignan como parte del proceso de evaluación de riesgos de la organización (ver A.2.3).

En el ejemplo típico de matriz de niveles de riesgo que se muestra en la Tabla A.3, la probabilidad y la consecuencia se han desglosado en tres niveles. El nivel de riesgo también se ha dividido en tres niveles. Los niveles de riesgo en cada bloque (Alto, Medio y Bajo) corresponden a una combinación particular de probabilidad y consecuencia. Una organización define una política de Tolerancia al Riesgo relacionada con cada nivel, que corresponderá a un nivel particular de respuesta corporativa al riesgo. Por ejemplo, los riesgos de nivel alto pueden resolverse dentro de los 6 meses; los riesgos de nivel bajo no tendrán ningún esfuerzo dedicado a ellos; y los elementos de nivel de riesgo medio merecerán un esfuerzo intermedio. En otras palabras, la organización ha declarado que puede tolerar un riesgo de alto nivel durante 6 meses y no más.

A.3.2.6.4 Revisión y validación de políticas de ciberseguridad.

Las políticas de seguridad cibernética deben revisarse periódicamente, validarse para confirmar que estén actualizadas y se sigan y revisen según sea necesario para garantizar que sigan siendo apropiadas. Cuando las políticas de seguridad cibernética se encuentran en un nivel superior, no deberían necesitar actualizarse con tanta frecuencia, ya que describen qué, en lugar de como. Si bien la forma del procedimiento puede cambiar con nuevas amenazas o técnicas, la razón para proteger el sistema seguirá siendo relativamente constante.

A.3.2.6.5 Implementación de políticas de ciberseguridad.

Durante la creación de políticas de ciberseguridad, se debe definir el método para implementarlas. Por ejemplo, las políticas de seguridad podrían publicarse en la Intranet corporativa y los usuarios podrían recibir capacitación sobre cómo les afecta la política. Las políticas son la base del CSMS, por lo que el sistema de implementación debe ser coherente con la implementación del sistema de gestión.

A.3.2.6.6 Prácticas de apoyo.

A.3.2.6.6.1 Prácticas de referencia.

Las siguientes cinco acciones son prácticas básicas:

a) Establecer el compromiso, la participación y el apoyo de la gerencia al crear y hacer cumplir las políticas de seguridad cibernética.

b) Exigir la revisión y aprobación de todas las unidades de negocio y departamentos afectados, incluida la gestión de operaciones.

c) Publicar documentos escritos que describan las políticas de seguridad cibernética.

d) Revisar, validar y revisar las políticas regularmente para confirmar que estén actualizadas y se sigan.

e) Comunicar y difundir políticas de ciberseguridad a todo el personal.

A.3.2.6.6.2 Prácticas adicionales

Las siguientes diez acciones son prácticas adicionales:

a) Crear políticas consistentes con un ciclo de vida determinado por la organización. Las políticas no se cambian constantemente ni se modifican en respuesta a los temas candentes.

b) Crear políticas de apoyo que pertenezcan a roles o grupos específicos que definan cómo se implementa la política de nivel superior para cada uno de estos grupos. Por ejemplo, el control de acceso físico y las restricciones de contraseña pueden no ser apropiadas en ciertas situaciones de control industrial. Se pueden requerir garantías procesales excepcionales para compensar.

c) Crear políticas de seguridad para abordar una serie de problemas de seguridad, incluida la mitigación de riesgos y el cambio de actitudes del personal hacia la seguridad cibernética.

d) Alinear las políticas de seguridad con las políticas y estrategias organizacionales generales.

e) Integrar las políticas de ciberseguridad con o como parte de una política de seguridad general que también aborde elementos físicos.

f) Identificar cómo se hacen cumplir las políticas y por quién.

g) Identificar cómo los usuarios deben cumplir con las disposiciones de las políticas.

h) Proporcionar un marco coherente de gestión de políticas.

i) Establecer qué políticas se aplican a usuarios específicos o grupos de usuarios.

j) Identificar cómo medir los requisitos de conformidad para las políticas.

A.3.2.6.7 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [23], [26], [30], [43].

A.3.3 Grupo de elementos: contramedidas de seguridad seleccionadas.

A.3.3.1 Descripción del grupo de elementos.

El segundo grupo de elementos dentro de esta categoría es Contramedidas de seguridad seleccionadas. Los elementos dentro de este grupo discuten algunos de los principales tipos de controles de seguridad que forman parte de un CSMS bien diseñado. Este documento no intenta describir la implementación completa de ninguna de estas contramedidas de seguridad seleccionadas. Discute muchos de los problemas de política, procedimiento y práctica relacionados con estas contramedidas de seguridad particulares. La figura A.7 muestra una representación gráfica de los seis elementos en el grupo de elementos:

· Seguridad del personal,

· Seguridad física y ambiental,

· Segmentación de la red,
· Control de acceso - Administración de cuentas,
· Control de acceso – Autenticación.
· Control de acceso - Autorización.

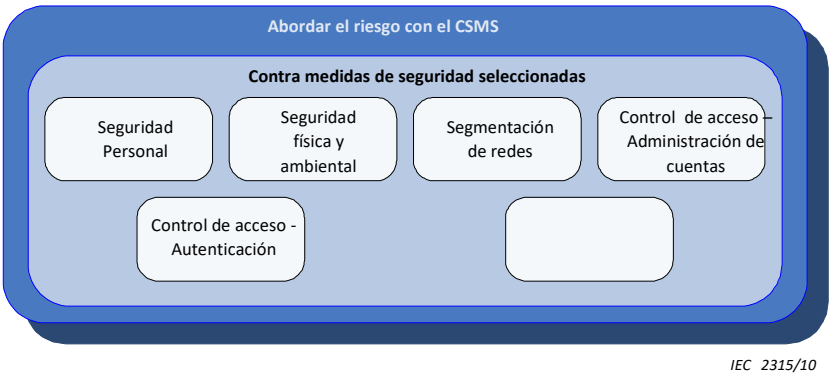

Figura A.7 - Vista gráfica del grupo de elementos: contramedidas de seguridad seleccionadas.

Un CSMS es el sistema a través del cual se seleccionan y mantienen las contramedidas de seguridad de una organización. Por lo tanto, se consideran contramedidas particulares como resultado de este sistema y no como parte del propio CSMS. Sin embargo, las contramedidas discutidas en esta subcláusula se han incluido en esta norma porque su aplicación es fundamental para la formulación de políticas y arquitectura de seguridad. Por esta razón, deben considerarse por adelantado durante la creación de un CSMS.

A.3.3.2 Elemento: seguridad del personal.

A.3.3.2.1 Descripción del elemento.

La seguridad del personal implica observar al personal potencial y actual para determinar si llevarán a cabo sus responsabilidades para la seguridad de IACS en la organización y establecer y comunicar sus responsabilidades para hacerlo. Los empleados, contratistas o personal temporal que tienen acceso a información confidencial de operaciones industriales o las redes, hardware y software de IACS crean una exposición potencial si la información confidencial se revela, modifica o si se otorga acceso no autorizado a los sistemas de TI o IACS.

A.3.3.2.2 Requisitos para la seguridad del personal.

En muchas organizaciones, los requisitos de seguridad del personal han sido impulsados por las preocupaciones sobre las amenazas internas y la posibilidad de accidentes causados por la falta de atención a los detalles o por el personal no apto para un trabajo debido a la falta de antecedentes adecuados o el uso de sustancias que podrían nublar el juicio. Al implementar políticas de seguridad del personal, es posible reducir este tipo de problemas.

Al desarrollar un programa para la seguridad del personal, es importante incluir personal que pueda acceder a todos los sistemas en su alcance y no solo limitar el esfuerzo al personal que utiliza las instalaciones tradicionales de la sala de computadoras.

Las computadoras en las operaciones IACS son herramientas utilizadas para operar la instalación de manera productiva y segura. El personal que opera los sistemas es el corazón de las operaciones y se debe tener mucho cuidado para garantizar que estas personas estén calificadas y sean aptas para estos puestos. Este proceso comienza en la fase de reclutamiento y continúa hasta la finalización. Requiere una atención constante por parte de la gerencia y los compañeros de trabajo para garantizar que el sistema funcione de manera segura.

Una política de seguridad del personal debe establecer claramente el compromiso de la organización con la seguridad y las responsabilidades de seguridad del personal. Debe abordar las responsabilidades de seguridad de todo el personal (tanto los empleados individuales como la organización) desde el reclutamiento hasta el final del empleo, especialmente para puestos delicados. (Esto incluye empleados, posibles empleados, empleados contratados, contratistas externos y organizaciones de la empresa, como las relaciones humanas).

Todo el personal, incluidas las nuevas contrataciones y las transferencias internas a puestos sensibles (por ejemplo, aquellos que requieren acceso privilegiado) deben ser seleccionados durante el proceso de solicitud de empleo. Esta evaluación debe incluir referencias de identidad, personales y laborales y credenciales académicas. Las evaluaciones de antecedentes también pueden incluir historial de crédito, actividad criminal y detección de drogas, ya que esta información puede ser útil para determinar la idoneidad de los solicitantes (sujeto a las leyes de privacidad locales). Los terceros, los contratistas y similares están sujetos a una investigación de antecedentes al menos tan rigurosa como los empleados en puestos comparables. Los empleados y contratistas también pueden estar sujetos a un escrutinio continuo, como actividades financieras, criminales y de drogas. Debido a la cantidad de datos confidenciales de operación industrial y los riesgos potenciales de HSE en algunos entornos de IACS, puede ser necesario evaluar a un amplio grupo de empleados que tienen acceso a IACS. Los empleados de planta pueden necesitar el mismo nivel de verificación de antecedentes y escrutinio que un administrador de sistemas de TI típico. Los términos "evaluación" y "verificación de antecedentes" se dejan intencionalmente vagos para que la organización pueda determinar el nivel de evaluación que se realizará en el personal. La organización también debe definir las "posiciones sensibles" porque se da cuenta de que algunas posiciones pueden tener poco o ningún efecto en la seguridad del sistema.

Durante el proceso de contratación, los términos y condiciones de empleo deben indicar claramente la responsabilidad de los empleados por la seguridad cibernética. Estas responsabilidades deben extenderse por un período de tiempo razonable después de que cese el empleo. Al contratar contratistas o trabajar con personal de terceros, sus responsabilidades de seguridad deben documentarse e incluirse en cualquier acuerdo. Siempre que sea posible, las responsabilidades deben ser específicas y medibles.

El personal debe ser consciente de las expectativas de seguridad de la organización y sus responsabilidades a través de declaraciones claramente documentadas y comunicadas por la organización. El personal debe aceptar su responsabilidad mutua para garantizar el funcionamiento seguro de la organización. Las organizaciones pueden considerar que todo el personal de las instalaciones de procesamiento de información firme un acuerdo de confidencialidad o no divulgación. Cualquier acuerdo de confidencialidad debe ser revisado y firmado por los empleados como parte del proceso de empleo inicial. Los contratistas externos, el personal eventual o los empleados temporales no cubiertos por un acuerdo formal de confidencialidad también deben firmar un acuerdo de confidencialidad antes de comenzar a trabajar.

Las organizaciones deben crear roles de trabajo basados en la segregación de deberes para garantizar que el acceso a la información sea necesario y los pasos operativos de alto riesgo requieren que se complete

más de una persona. Estas tareas deben estar segregadas entre el personal para mantener los controles y equilibrios adecuados, de modo que ningún individuo tenga el control total sobre las acciones que cambian la operación funcional del IACS. Las funciones y responsabilidades de seguridad para un trabajo determinado deben revisarse y revisarse periódicamente para satisfacer las necesidades cambiantes de la empresa.

Se debe esperar que todo el personal permanezca atento a situaciones que puedan conducir a incidentes de seguridad o protección. Las empresas necesitan capacitar a los gerentes para observar el comportamiento del personal que puede conducir a robo, fraude, error u otras implicaciones de seguridad. Se debe establecer y comunicar al personal un proceso disciplinario para las violaciones de seguridad cibernética. Esto debería estar vinculado a las medidas legales y punitivas contra tales crímenes en el país.

A.3.3.2.3 Prácticas de apoyo.

A.3.3.2.3.1 Prácticas de referencia.

Las siguientes ocho acciones son prácticas básicas:

a) Selección de personal durante la fase de reclutamiento, con verificación de antecedentes antes de la contratación o traslado a trabajos delicados, especialmente para puestos sensibles.

b) Examinar al personal, especialmente aquellos en posiciones sensibles, de manera regular para buscar problemas financieros, actividades delictivas o problemas de drogas.

c) Comunicar los términos y condiciones de empleo o contrato a todo el personal declarando la responsabilidad del individuo por la seguridad cibernética.

d) Documentar y comunicar las expectativas de seguridad de la organización y las responsabilidades del personal de manera regular.

e) Requerir que el personal acepte su responsabilidad mutua para garantizar el funcionamiento seguro de la organización.

f) Separar los deberes entre el personal para mantener los controles y equilibrios apropiados.

g) Requerir a todo el personal que firme un acuerdo de confidencialidad o no divulgación.

h) Establecer un proceso disciplinario para el personal que ha violado las políticas de seguridad de la organización.

A.3.3.2.3.2 Prácticas adicionales.

Las siguientes dos acciones son prácticas adicionales:

a) Crear roles de trabajo basados en la separación de deberes para garantizar que el acceso a la información sea necesario y los pasos de procesamiento de alto riesgo requieren que se complete más de una persona.

b) Documentar las responsabilidades de seguridad e incluirlas en las descripciones de trabajo, contratos u otros acuerdos de terceros.

A.3.3.2.4 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [2], [23], [26], [30], [43].

A.3.3.3 Elemento: seguridad física y ambiental.

A.3.3.3.1 Descripción del elemento.

La seguridad física y ambiental se relaciona con la creación de un entorno seguro para la protección de activos tangibles o físicos (es decir, computadoras, redes, equipos de información y operaciones) contra daños, pérdidas, acceso no autorizado o uso indebido. La seguridad física y ambiental de los sistemas de información es una disciplina bien establecida que extrae conocimiento y experiencia de otras áreas de seguridad física o de instalaciones. Las medidas de seguridad física y ambiental deben diseñarse para complementar las medidas de seguridad cibernética adoptadas para proteger estos activos.

Las medidas de seguridad física y ambiental son diferentes, pero están vinculadas, ya que ambas intentan proteger los activos de una organización de las amenazas. Las medidas de seguridad física aseguran que los activos de una organización estén protegidos físicamente contra el acceso no autorizado, la pérdida, el daño, el mal uso y similares. Las medidas de seguridad ambiental aseguran que los activos de una organización estén protegidos contra las condiciones ambientales que los harían inutilizables o dañarían la información que contienen.

Si bien las políticas y los procedimientos de seguridad cibernética son importantes para la protección adecuada de la información y los sistemas de control, para tener una protección verdaderamente efectiva, deben complementarse con el nivel apropiado de seguridad física. Por ejemplo, mantener controles estrictos como la autenticación y el control de acceso, son pocos para proteger la integridad del sistema si es posible ingresar a una instalación y eliminar o dañar físicamente los medios electrónicos.

A.3.3.3.2 Consideraciones para la seguridad física y ambiental.

A.3.3.3.2.1 General.

En muchas organizaciones, los requisitos de seguridad del perímetro físico y ambiental han sido impulsados por preocupaciones sobre los activos físicos de la organización y pueden no cumplir con los requisitos de seguridad cibernética. Debido a la integración de múltiples organizaciones dentro de sitios específicos (es decir, socios comerciales, contratistas y terceros), se puede requerir protección de seguridad física adicional para los activos de IACS. En las instalaciones de IACS, la seguridad física se centra más en proteger los activos de IACS que en la información de las operaciones en sí. La preocupación no es tanto el robo real o la corrupción de los dispositivos informáticos y de control, sino más bien el impacto que esto tendría en la capacidad de mantener la producción de manera segura.

Al desarrollar un programa para la seguridad física de los activos, es importante incluir todos los sistemas en el alcance y no limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras. IEC / TS 62443 - 1 - 1 analiza los criterios que pueden usarse para determinar qué activos físicos deben considerarse en el alcance del CSMS.

Las computadoras que comprenden el IACS son herramientas utilizadas para operar la instalación de manera productiva y segura. Son un medio para el fin, así como el activo que se debe proteger. En algunos casos, la seguridad y / o la productividad se ven amenazadas por el bloqueo del equipo detrás de las puertas porque el tiempo de respuesta para acceder al equipo puede aumentar.

El juicio práctico de ingeniería que equilibra todos los riesgos debe usarse para determinar los procedimientos de seguridad física para los activos a proteger. Aunque es una práctica común ubicar enrutadores y otros

equipos de red en entornos bloqueados, puede ser de valor limitado expandir esta práctica mucho más allá de este nivel. Los dispositivos de campo (es decir, actuadores de válvula, arrancadores de motor y relés) generalmente tienen la capacidad de activarse directamente en el campo sin señales de control a través de la red IACS. Puede ser costoso proteger cada dispositivo de campo individualmente, por lo que generalmente se necesitan procedimientos físicos de acceso al perímetro físico en instalaciones que impliquen un alto riesgo.

La siguiente lista contiene elementos que deben considerarse al crear un entorno seguro para la protección de activos tangibles contra daños físicos debido a intrusión física o condiciones ambientales.

A.3.3.3.2.2 Política de seguridad.

Una política de seguridad escrita contiene directivas que definen cómo una organización define la seguridad, opera su programa de seguridad y revisa su programa para realizar mejoras adicionales. Estas políticas escritas permiten al personal comprender claramente sus roles y responsabilidades para asegurar los activos de la organización. La organización necesita establecer una política de seguridad física y ambiental que sea complementaria tanto de la política de seguridad cibernética de la organización como de su política de seguridad física. El objetivo principal es cerrar cualquier brecha que pueda existir entre estas dos políticas. La política de seguridad física y ambiental debe ser coherente y seguir las mismas políticas, como se discutió anteriormente, que otras políticas de seguridad relacionadas con la seguridad del sistema de control. Se utiliza una evaluación detallada de riesgos de seguridad física para determinar los procedimientos de seguridad física apropiados que se implementarán.

A.3.3.3.2.3 perímetro de seguridad.

La información crítica o los activos deben colocarse en un área segura protegida por perímetros de seguridad y controles de entrada. Estos controles de seguridad física funcionan en conjunto con medidas de seguridad cibernética para proteger la información. Se deben establecer uno o más perímetros de seguridad física para proporcionar barreras para el acceso no autorizado a las instalaciones. Se pueden anidar varios perímetros para proporcionar controles sucesivamente más estrictos. Un ejemplo puede ser el gabinete cerrado dentro de una sala de control con acceso con tarjeta dentro de una instalación con una cerca perimetral protegida.

A.3.3.3.2.4 Controles de entrada.

En cada barrera o límite, se deben proporcionar controles de entrada apropiados. Estos controles de entrada pueden ser cosas como puertas cerradas, puertas con cerraduras apropiadas o guardias. Los controles de entrada deben ser apropiados para el nivel de seguridad requerido en el área asegurada por los controles de entrada y en relación con la necesidad de un acceso rápido.

A.3.3.3.2.5 Protección contra daños ambientales.

Los activos deben protegerse contra el daño ambiental de amenazas como incendios, agua, humo, polvo, radiación e impacto. Se debe prestar especial atención a los sistemas de protección contra incendios utilizados en áreas que afectan a los IACS para asegurarse de que los sistemas responsables de proteger las instalaciones ofrezcan protección a los dispositivos IACS sin introducir riesgos adicionales para la operación industrial.

A.3.3.3.2.6 Procedimientos de seguridad.

Se debe exigir al personal que siga y aplique los procedimientos de seguridad física que se han establecido para reforzar la entrada y otros controles físicos. El personal no debe eludir ninguna de las entradas automáticas y otros controles físicos. Un ejemplo de un empleado que elude un control físico sería tener una puerta de entrada a una sala de control protegida abierta.

A.3.3.3.2.7 Puntos únicos de falla.

Los puntos únicos de falla deben evitarse cuando sea posible. Los sistemas redundantes proporcionan un sistema más robusto que es capaz de manejar pequeños incidentes que afecten a la planta u organización, por ejemplo, utilizando una fuente de alimentación redundante en un sistema crítico para garantizar que, si una fuente de alimentación está dañada, el sistema crítico seguirá funcionando.

A.3.3.3.2.8 Conexiones.

Todas las conexiones (es decir, alimentación y comunicaciones, incluido el cableado de campo de E / S, el cableado del bus de E / S, los cables de red, los cables de conexión entre controladores, los módems y similares) bajo el control de la organización deben estar adecuadamente protegidos contra la manipulación o daños. Esto puede incluir poner conexiones en gabinetes cerrados o dentro de recintos cercados. El nivel de seguridad física para estas conexiones debe ser acorde con el nivel de seguridad de los sistemas a los que se conectan. Al considerar la seguridad física, también se deben considerar las consecuencias del daño ambiental. Estas conexiones también deben protegerse contra factores naturales como el calor, el fuego, el polvo y similares que podrían causar fallas.

A.3.3.3.2.9 Mantenimiento de equipos.

Todo el equipo, incluido el equipo ambiental auxiliar, debe mantenerse adecuadamente para garantizar un funcionamiento adecuado. Se deben establecer cronogramas de mantenimiento y realizar mantenimiento preventivo. Se debe realizar un seguimiento del mantenimiento del equipo y observar las tendencias para determinar si se deben ajustar los cronogramas de mantenimiento.

A.3.3.3.2.10 Alarmas.

Deben establecerse procedimientos adecuados para el monitoreo y la alarma cuando se compromete la seguridad física y ambiental. Se debe exigir al personal que responda a todas las alarmas con las medidas de respuesta apropiadas. Todas las instalaciones, proporcionales a su nivel de seguridad, deben estar alarmadas por intrusiones físicas y ambientales. Estos pueden incluir detectores de movimiento, cámaras o alarmas de puerta para intrusiones físicas y alarmas de incendio, detectores de agua o sensores de temperatura para problemas ambientales.

A.3.3.3.2.11 Ciclo de vida del equipo.

Deben establecerse y auditarse procedimientos adecuados con respecto a la adición y eliminación de todos los equipos. El seguimiento adecuado de los activos es una buena práctica. Estos procedimientos incluirían la eliminación de estaciones de trabajo, el formato, la unidad limpia y similares. La adquisición de hardware también tendría en cuenta cómo se puede rastrear el equipo y cómo se puede desinfectar y eliminar cuando llegue el momento en que ya no sea necesario.

A.3.3.3.2.12 Información física.

Toda la información, expresada en forma física (es decir, documentos escritos o impresos, medios de almacenamiento magnéticos y discos compactos), debe protegerse adecuadamente contra amenazas físicas. Esto puede incluir colocar estos artículos en habitaciones cerradas o armarios para evitar el acceso no autorizado. También se debe considerar proteger la información del daño ambiental como campos magnéticos, alta humedad, calor o luz solar directa, y similares que podrían dañar la información. Al igual que para los equipos, deben existir procedimientos para eliminar de forma segura los medios físicos cuando ya no sean necesarios.

A.3.3.3.2.13 Uso de activos fuera de entornos controlados.

Se debe tener especial cuidado al usar activos que afectan a IACS fuera de la red de IACS. Esto incluye organizar los activos en una instalación de integración de sistemas antes de la instalación. Además, los activos como las computadoras portátiles con acceso a la red IACS utilizados fuera del sitio deben manejarse como una extensión de la red IACS con todos los procedimientos apropiados de seguridad física y ambiental que se siguen. Se debe considerar el uso del mismo nivel de seguridad para activos que están temporalmente fuera de los límites de seguridad normales. Esto puede requerir una planificación especial o instalaciones para proteger estos activos contra el acceso o uso no autorizado o contra el daño ambiental.

A.3.3.3.2.14 Protección provisional de activos críticos.

Durante y después de un evento físico o ambiental, la energía u otro servicio pueden perderse en los sistemas críticos. Deben tomarse medidas para proteger estos sistemas críticos. Esto podría incluir temas como el suministro de energía de respaldo, la cobertura o la represa para evitar daños por agua, y similares.

A.3.3.3.3 Prácticas de apoyo.

A.3.3.3.3.1 Prácticas de referencia.

Las siguientes nueve acciones son prácticas básicas:

a) Establecer perímetros de seguridad física para proporcionar barreras para el acceso no autorizado a las instalaciones. En cada barrera o límite, se proporcionan controles de entrada apropiados.

b) Proteger los activos contra el daño ambiental de amenazas como incendios, agua, humo, polvo, radiación e impacto.

c) Requerir al personal que siga y aplique los procedimientos de seguridad física que se han establecido para reforzar la entrada y otros controles físicos.

d) Requerir fuentes de energía redundantes para evitar puntos únicos de falla.

e) Proteger todas las conexiones externas contra manipulaciones o daños.

f) Mantener todo el equipo, incluido el equipo ambiental auxiliar, para garantizar un funcionamiento adecuado.

g) Establecer procedimientos para monitorear y alarmar cuando la seguridad física y / o ambiental está comprometida.

h) Establecer y auditar procedimientos con respecto a la adición, eliminación y disposición de todos los activos.

i) Usar procedimientos especiales para asegurar los activos que afectan a IACS fuera de la red IACS.

A.3.3.3.3.2 Prácticas adicionales.

Las siguientes siete acciones son prácticas adicionales:

a) Usar cables de seguridad, armarios cerrados, entradas protegidas en la oficina, mantener el equipo fuera de la vista, etiquetar y marcar los activos.

b) Usar la configuración de contraseña para los comandos de inicio e inicio de sesión en computadoras que no están en la sala de control, sistema de archivos encriptados, computadoras portátiles que usan técnicas de cliente ligero, y similares.

c) Proteger los equipos informáticos que no se encuentran en salas de control, como enrutadores o cortafuegos, colocándolos en un entorno cerrado.

d) Tener salas de control atendidas continuamente. Esto a menudo puede ser la primera línea de defensa en protección física. Use salas de control para albergar activos de información y tecnología.

e) Requerir que el personal que abandona la organización devuelva el equipo en buen estado de funcionamiento.

f) Usar un sistema de seguimiento de equipos para determinar dónde se encuentra el equipo y quién tiene la responsabilidad del mismo.

g) Requerir protección ambiental para los activos, incluido el lugar adecuado para el equipo que se encuentra dónde puede estar expuesto al polvo, temperaturas extremas, humedad y similares.

A.3.3.3.4 Recursos utilizados.

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [2], [23], [27], [31].

A.3.3.4 Elemento: segmentación de red.

A.3.3.4.1 Descripción del elemento.

La segmentación de la red implica la separación de los activos clave de IACS en zonas con niveles de seguridad comunes para gestionar los riesgos de seguridad y lograr el nivel de seguridad objetivo deseado para la zona. La segmentación de la red es una contramedida de seguridad importante empleada junto con otras capas de defensa para reducir el riesgo que puede estar asociado con IACS.

Los IACS de la actualidad están conectados e integrados con los sistemas comerciales tanto dentro como entre empresas asociadas. A pesar de la necesidad de conectividad e integración estrecha, IACS no necesita utilizar la gran mayoría de los datos que atraviesan las redes corporativas. Exponer los dispositivos IACS a todo este tráfico aumenta la probabilidad de un incidente de seguridad dentro de IACS. De acuerdo con el principio de privilegio mínimo y necesidad de saber, IACS debe ser diseñado de manera que filtre / elimine los paquetes de comunicación innecesarios para que no lleguen a los dispositivos IACS. La segmentación de red está diseñada para compartimentar dispositivos en zonas de seguridad comunes donde se emplean prácticas de seguridad identificadas para lograr el nivel de seguridad objetivo deseado. El objetivo es minimizar la probabilidad de un incidente de seguridad que comprometa el funcionamiento del IACS. La compartimentación de dispositivos en zonas no significa necesariamente aislarlos. Los conductos conectan las zonas de seguridad y facilitan el transporte de las comunicaciones necesarias entre las zonas de seguridad segmentadas.

La premisa de seguridad primordial es que el uso de contramedidas de seguridad debe ser acorde con el nivel de riesgo. La segmentación de red de un IACS puede no ser necesaria si los riesgos de seguridad son bajos. El elemento de gestión e implementación de riesgos proporciona información adicional sobre el tema de la gestión de riesgos. Debe revisarse antes de implementar una estrategia de contramedida de segmentación de red discutida en este elemento del CSMS.

A.3.3.4.2 Segmentos y zonas de red

A.3.3.4.2.1 General

IEC / TS 62443 - 1 - 1, la cláusula 6 introduce modelos de referencia y proporciona el contexto para discutir esta contramedida. Las redes se segmentan mediante el uso de algún tipo de dispositivo de barrera que tiene la capacidad de controlar lo que pasa a través del dispositivo. En las redes basadas en Ethernet que ejecutan TCP / IP, los dispositivos de barrera más comunes en uso son firewalls, enrutadores y conmutadores de capa 3. Con frecuencia, IACS se compone de varias redes diferentes que emplean diferentes tecnologías físicas y de capa de aplicación. Estas redes que no son TCP / IP también emplean dispositivos de barrera para separar y segmentar las comunicaciones. Los dispositivos de barrera pueden ser puertas de enlace independientes o integradas en el módulo de interfaz de red de un dispositivo IACS.

Si bien colocar un dispositivo de barrera en la red puede crear un nuevo segmento de red y zona de seguridad, una zona de seguridad también puede abarcar múltiples segmentos de red. La Figura A.8 a continuación ilustra una posible arquitectura segmentada para un IACS genérico. Esta figura intenta describir cómo los niveles de equipo funcional pueden traducirse en el mundo físico de un IACS y el mundo lógico de una zona. (La cifra es de nivel bastante alto y no incluye todos los dispositivos de red necesarios en una instalación real).

Es importante no confundir los niveles funcionales del modelo de referencia con los niveles de seguridad asociados con las zonas de seguridad. Si bien es generalmente cierto que el equipo de nivel inferior desempeña un papel más importante en la operación segura de la operación industrial automatizada, puede no ser práctico o posible emplear una estrategia de segmentación alineada uno a uno con los niveles de equipo.

En esta figura, la zona de control contiene equipos con un nivel de seguridad objetivo común. La figura muestra un segmento de red de control de proceso (PCN) basado en TCP / IP, un segmento de red de control reglamentario (RCN) y un segmento de red de dispositivo de campo (FDN). Estas redes enlazan los equipos de Nivel 0, 1, 2 y 3 que se muestran en los modelos de referencia de IEC / TS 62443 - 1 - 1, 5.2. Los dispositivos de barrera para cada uno de estos segmentos de red regulan la comunicación que entra y sale de su segmento.

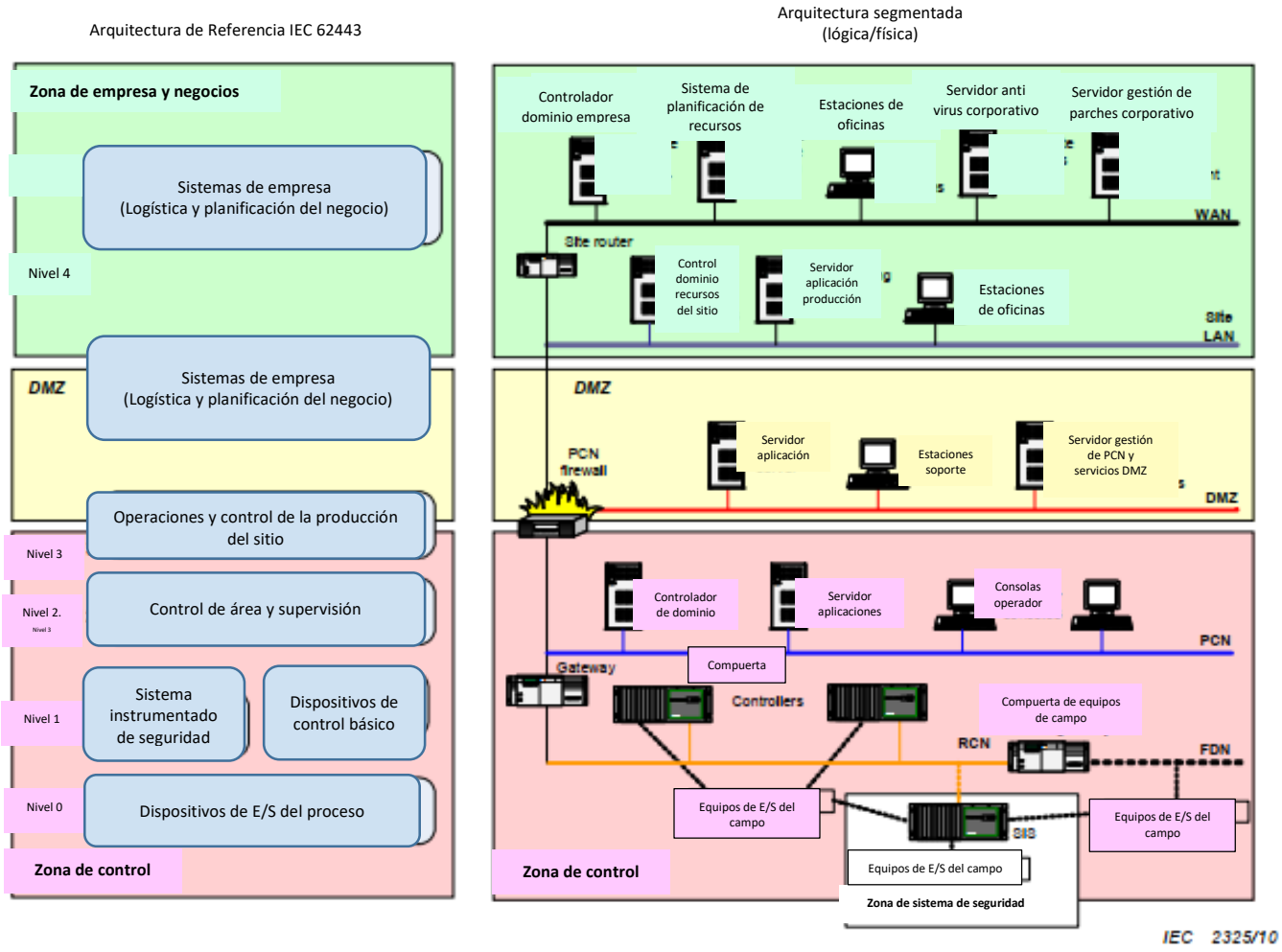

Figura A.8 - Alineación de arquitectura de referencia con un ejemplo de arquitectura segmentada

A.3.3.4.2.2 Zona de control

Para IACS de bajo riesgo, puede no ser necesario emplear la segmentación de la red como una contramedida, lo que requeriría la creación de una zona de control distinta. Sin embargo, para IACS de riesgo medio a alto, la segmentación de la red es una contramedida que proporciona una reducción de riesgo muy significativa.

La buena práctica generalmente aceptada es usar un dispositivo de barrera como un firewall para administrar la comunicación a través del conducto que une la zona de control con la zona de negocios, como se muestra en la Figura A.8.

Las estrategias de filtrado comunes en el dispositivo de barrera incluyen:

a) La configuración básica del dispositivo de barrera debe ser *negar toda* comunicación por defecto y solo permitir la comunicación por excepción para satisfacer una necesidad comercial crítica. Esto se aplica tanto a la comunicación intermitente e interactiva del usuario a través del conducto como a la comunicación continua de tarea a tarea entre dispositivos en estas dos zonas. Siempre que sea

posible, las comunicaciones se deben filtrar por puertos y servicios entre pares de IP coincidentes para los dispositivos que se comunican por el conducto.

b) Los puertos y servicios utilizados con frecuencia como vectores de ataque no deben abrirse a través del dispositivo de barrera. Cuando se requiere el servicio debido a una justificación comercial, se deben emplear contramedidas adicionales para compensar el riesgo. Como ejemplo, puede ser necesario http entrante, que es un vector de ataque común, para admitir una función comercial importante. Las contramedidas compensatorias adicionales, como el bloqueo de scripts entrantes y el uso de un servidor proxy http ayudarían a disminuir el riesgo de abrir este puerto y servicio de alto riesgo.

c) Cuanto menor sea el número de puertos y servicios abiertos a través del dispositivo de barrera, mejor. Deben evitarse las tecnologías de comunicación que requieren una gran cantidad de puertos abiertos.

El dispositivo de barrera puede servir como una buena herramienta automatizada para hacer cumplir las prácticas de seguridad en la zona de control, como no permitir el correo electrónico entrante o las comunicaciones hacia / desde Internet.

A.3.3.4.2.3 Zona desmilitarizada (DMZ)

Para los IACS de alto riesgo, el uso de una DMZ junto con una zona de control ofrece oportunidades adicionales de reducción de riesgos entre la zona comercial de bajo nivel de seguridad y la zona de control de alto nivel de seguridad. El nivel de seguridad para la DMZ es más alto que la zona de negocios pero menor que la zona de control. La función de esta zona es eliminar o reducir en gran medida toda comunicación directa entre la zona de control y la zona comercial.

Los dispositivos deben ubicarse en la DMZ que funcionen como un puente o búfer entre los dispositivos en la zona comercial y la zona de control. La comunicación se configura entre un dispositivo en la zona comercial y la DMZ. El dispositivo en la DMZ luego pasa la información al dispositivo receptor en la zona de control. Idealmente, los puertos y servicios empleados entre el dispositivo en la zona comercial y la DMZ son diferentes de los puertos y servicios utilizados entre el dispositivo DMZ y el dispositivo de la zona de control de destino. Esto reduce la probabilidad de que un código malicioso o un intruso puedan negociar los conductos combinados que conectan la zona comercial con la zona de control.

Las estrategias de filtrado enumeradas anteriormente para la zona de control también son aplicables para la DMZ. Sin embargo, algunos protocolos más riesgosos como telnet pueden permitir la administración de dispositivos en las zonas de control y DMZ.

Hay varios casos de uso en los que una DMZ puede ser beneficiosa. Estos se incluyen aquí para ilustrar los conceptos de seguridad. No están destinados a ser una lista exhaustiva o detallada de cómo implementar una DMZ:

a) Minimizar el número de personas que acceden directamente a los dispositivos de la zona de control.

Las personas ubicadas en el sitio LAN en la zona de negocios a menudo acceden a los servidores de Historia. En lugar de ubicar el servidor histórico en la zona de control y permitir el acceso directo a este dispositivo desde la zona comercial por un gran número de usuarios, el nivel de seguridad de la zona de control puede mantenerse en un nivel superior si el servidor histórico se encuentra en el DMZ.

b) Proporcionar mayor seguridad para dispositivos IACS importantes.

En el caso del servidor de historiador mencionado anteriormente, una opción sería ubicar el historiador en la LAN del sitio donde se encuentra la mayoría de los usuarios. Esto reduciría la cantidad de personas que necesitan acceder al PCN. Sin embargo, dado que la zona de negocios es una zona de bajo nivel de seguridad, el servidor de historiador estaría sujeto a un entorno menos seguro. El potencial de compromiso del servidor sería mayor.

c) Compensar los retrasos en los parches.

La DMZ ofrece protección de seguridad adicional para dispositivos IACS importantes que no pueden ser parcheados tan rápidamente mientras esperan los resultados de las pruebas de compatibilidad de parches del proveedor de la aplicación.

d) Proporcionar seguridad mejorada para la zona de control al mover los dispositivos de administración a un nivel de seguridad más alto.

La DMZ es un buen lugar para ubicar dispositivos como servidores antivirus y servidores de administración de parches. Estos dispositivos se pueden usar para administrar la implementación de módulos de seguridad en la zona de control y los dispositivos DMZ de una manera más controlada sin someter la zona de control de alto nivel de seguridad a una conexión directa a servidores que pueden comunicarse con cientos de dispositivos.

A.3.3.4.2.4 Zona del sistema de seguridad

Algunos IACS pueden emplear un conjunto de enclavamientos de seguridad basados en relés o microprocesadores. Un solucionador lógico basado en microprocesador SIS puede requerir un conjunto de prácticas de seguridad ligeramente diferente del empleado en la zona de control. Se debe determinar el nivel de seguridad objetivo para esta zona y se deben tomar las medidas apropiadas para garantizar que se empleen las contramedidas apropiadas para cumplir con el nivel de seguridad objetivo.

A.3.3.4.2.5 IACS aislados

El riesgo asociado con el IACS puede ser demasiado grande para permitir cualquier oportunidad de comprometerlo por parte de un agente externo. Una instalación puede elegir desconectar todos los conductos entre la zona de control y cualquier otra zona. Esta es una estrategia de segmentación de red muy válida para su consideración.

Las instalaciones que eligen adoptar este enfoque de aislamiento no eliminan automáticamente todos los riesgos. Todavía puede haber mucha vulnerabilidad que podría explotarse localmente. Se deben emplear capas apropiadas de protección física y cibernética para abordar el riesgo residual que queda después del aislamiento de la IACS de la zona comercial.

A.3.3.4.3 Arquitectura de segmentación SCADA

La discusión anterior describió una arquitectura segmentada para un IACS que generalmente se encuentra en una sola instalación operativa. La segmentación es una contramedida que tiene la misma aplicabilidad para un IACS tipo SCADA. La figura A.9 ilustra un posible enfoque de segmentación para este tipo de arquitectura. Aunque no se muestra debido a limitaciones de espacio, la zona del sistema de seguridad y DMZ descrita en la instalación operativa única IACS también se puede emplear en una arquitectura SCADA.

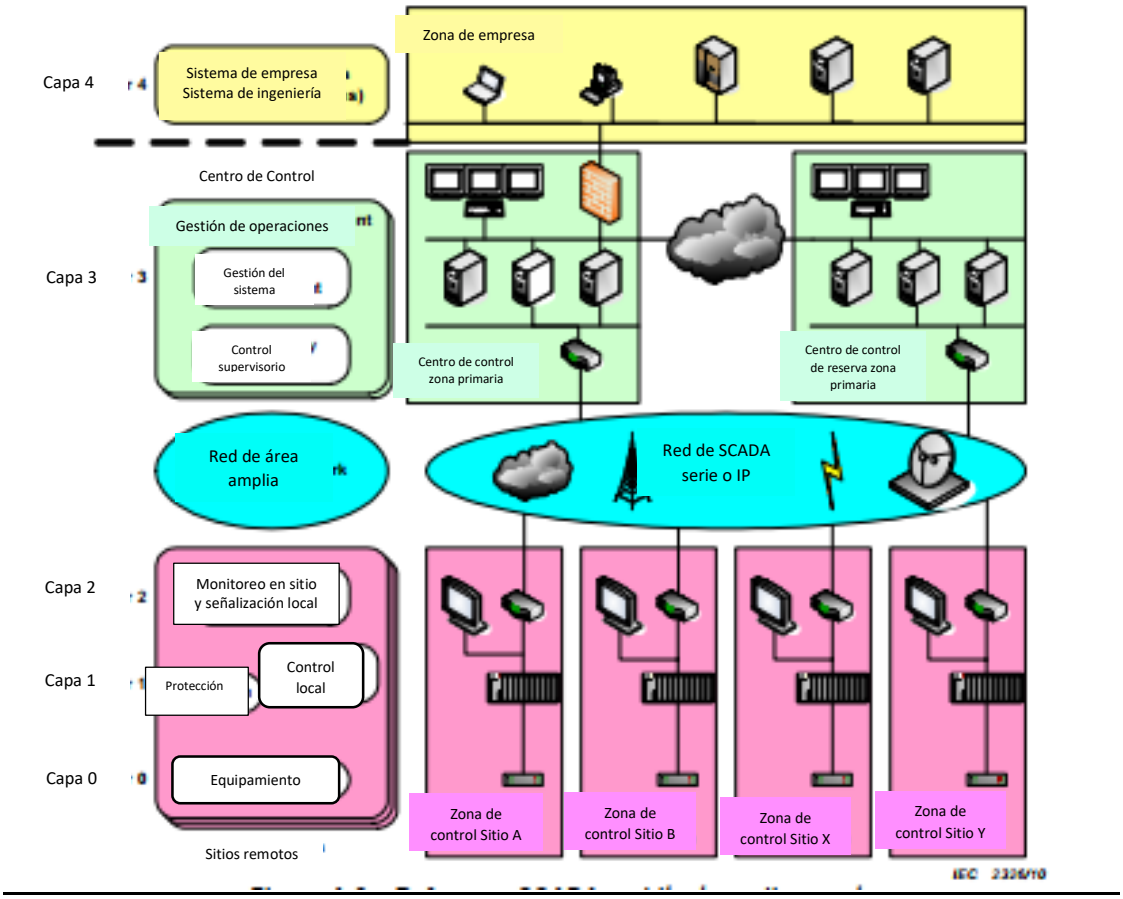

Figura A.9 - Alineación de arquitectura SCADA de referencia con un ejemplo de arquitectura segmentada

A.3.3.4.4 Prácticas sugeridas

A.3.3.4.4.1 Prácticas de referencia

Las siguientes cuatro acciones son prácticas básicas:

a) Emplear dispositivos de barrera como cortafuegos para segmentar dispositivos IACS de alto riesgo en zonas de control.

b) Empleando puertas de enlace o dispositivos de barrera internos dentro del dispositivo IACS para separar las redes de control regulatorio de la PCN.

c) Emplear prácticas sólidas de gestión de cambios en la configuración del dispositivo de barrera.

d) Desconectar IACS de alto riesgo de la zona de negocios.

A.3.3.4.4.2 Prácticas adicionales

Las siguientes cuatro acciones son prácticas adicionales:

a) Emplear dispositivos de barrera complementarios y adicionales dentro de la zona de control para segmentar aún más la red.

b) Emplear un perfil de seguridad común y administrado centralmente en todos los dispositivos de barrera de zona de control.

c) Emplear una arquitectura de segmentación DMZ.

d) Realizar pruebas de evaluación automatizadas para verificar que la configuración del dispositivo de barrera se haya implementado correctamente según las especificaciones de diseño.

A.3.3.4.5 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en la siguiente referencia, que se enumera en la Bibliografía: [1].

A.3.3.5 Elemento: Control de acceso: Administración de la cuenta.

A.3.3.5.1 Descripción general del control de acceso.

El control de acceso es el método para controlar quién o qué recursos pueden acceder a las instalaciones y sistemas y qué tipo de acceso está permitido. El mal uso de datos y sistemas puede tener serias consecuencias, incluyendo daños a la vida humana, daños ambientales, pérdidas financieras y daños a la reputación corporativa. Estos riesgos aumentan cuando el personal tiene acceso innecesario a datos y sistemas. Es muy importante que la política de seguridad que define las reglas y procedimientos de control de acceso esté claramente documentada y comunicada a todo el personal (es decir, empleados, empresas conjuntas, contratistas externos y empleados temporales).

Uno de los elementos de seguridad más importantes para cualquier sistema informático es tener un conjunto sólido y apropiado de procedimientos de control de acceso. Hay tres aspectos clave asociados con el control de acceso: administración de cuentas; Autenticación; y autorización.

Cada uno de estos se describe por separado en su propia subcláusula de elemento de esta norma. Sin embargo, los tres aspectos deben trabajar juntos para establecer una estrategia de control de acceso segura y sólida.

Dentro de cada uno de los tres aspectos del control de acceso, se deben establecer reglas para confirmar que el acceso de un usuario a los sistemas y datos está controlado. Las reglas generalmente deben aplicarse a roles o grupos de usuarios. Deben tener acceso a los sistemas y datos que se requieren para cumplir con los requisitos comerciales definidos, pero no deben tener acceso si no hay un propósito comercial definido para ellos.

Hay reglas que se aplican administrativamente y aquellas que se aplican automáticamente mediante el uso de la tecnología. Ambos tipos de reglas deben abordarse como parte de la estrategia general de control de acceso. Un ejemplo de una regla administrativa que una organización podría tener es la eliminación de la cuenta del empleado o del contratista después de su separación de la organización. Un ejemplo de una regla aplicada por la tecnología requiere que los usuarios remotos que se conectan a la red corporativa utilicen una VPN.

Además de las reglas, existen procedimientos de seguridad física y procedimientos de seguridad cibernética que trabajan juntos para establecer el marco de seguridad general para el sistema. Los procedimientos de seguridad física incluyen medidas tales como salas de bloqueo donde se encuentra el equipo de interfaz de usuario. Esta norma proporciona una descripción básica de las partes de seguridad física que se relacionan con la seguridad cibernética en A.3.3.3.

Hay un aspecto en tiempo real para el control de acceso y un aspecto fuera de línea. Muy a menudo, no se presta suficiente atención a las actividades fuera de línea de control de acceso para IACS. La actividad fuera de línea, aquí descrita como Administración de cuentas, es el primer paso en el proceso e incluye la definición de los privilegios del usuario y las necesidades de recursos para el usuario. Estos se basan en el rol del usuario y el trabajo a realizar. El método fuera de línea también incluye un paso de aprobación por parte del responsable antes de que la cuenta de acceso se configure para proporcionar el acceso adecuado.

A.3.3.5.2 Descripción del elemento

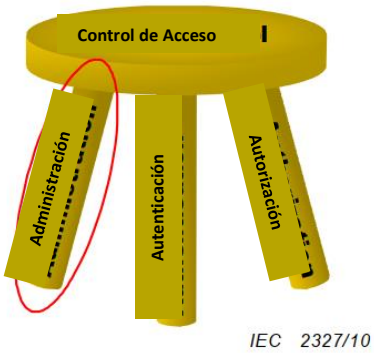

Figura A.10 - Control de acceso: administración de la cuenta

La administración de cuentas, una de las tres etapas del control de acceso, como se muestra en la Figura A.10, es el método asociado con la configuración inicial de permisos y privilegios para acceder a recursos específicos en la red o sistema y para revisar esos permisos y privilegios periódicamente. . Puede estar vinculado de alguna manera al acceso físico a los recursos. La administración de cuentas en el entorno IACS va más allá de la definición tradicional de TI del acceso a la cuenta del sistema operativo para un usuario en particular. En el entorno IACS, las cuentas de acceso están más basadas en roles para las funciones que pueden realizar en una máquina en particular en lugar de los datos a los que pueden acceder. El rol de un usuario puede cambiar en una organización con el tiempo, por lo que el proceso de administración puede usarse con más frecuencia en las cuentas IACS. Los privilegios a menudo incluyen acceso a directorios de archivos, horas de acceso y cantidad de espacio de almacenamiento asignado. El rol asignado a nivel de aplicación para la cuenta de acceso se identificará y comprenderá durante la fase de administración. Se incluyen varios pasos que incluyen la identificación de los recursos necesarios para realizar la función de trabajo de esa persona, la aprobación independiente de una persona de confianza y la configuración / configuración de la cuenta de la computadora que asigna automáticamente los recursos cuando se solicita.

Además de la tarea de crear cuentas de acceso y asignar usuarios a roles a nivel del sistema operativo, muchas aplicaciones de fabricación requieren asignaciones de roles adicionales. Los administradores de sistemas para IACS deberán ser expertos y confiables para realizar estas funciones administrativas de cuenta en aplicaciones de control de equipos en vivo. El proceso de gestión de cambios, para realizar estos cambios

en la cuenta debe identificar claramente cualquier restricción de tiempo que se deba seguir debido a los riesgos de seguridad durante ciertas secuencias de la operación de control.

A.3.3.5.3 Consideraciones para la administración de cuentas

A.3.3.5.3.1 General

Al desarrollar un programa para la administración de cuentas, es importante incluir todos los sistemas dentro del alcance y no limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras.

A.3.3.5.3.2 Reglas para controlar el acceso de un usuario a sistemas, datos y funciones específicas

Cada organización debe establecer reglas para controlar el acceso de un usuario a los sistemas, datos y funciones. Estas reglas deben basarse en el riesgo para el sistema y el valor de la información. Estas reglas deben transmitirse a todo el personal.

A.3.3.5.3.3 Proceso de administración normalizado

Se debe seguir un proceso administrativo normalizado para la creación de cuentas de acceso. Aunque puede ser más rentable para una sola organización proporcionar la función de administración de cuentas para todos los sistemas informáticos de una empresa, los sistemas IACS y de TI pueden tener diferentes conjuntos de personas que proporcionan control administrativo del proceso de creación y mantenimiento de cuentas. Esto a menudo se debe al diferente conjunto de riesgos asociados con estos sistemas. Las aprobaciones de cuenta también pueden requerir la aprobación de un supervisor familiarizado con las tareas y operaciones de IACS.

A.3.3.5.3.4 Cuentas de acceso basadas en roles

Se debe seguir un proceso administrativo normalizado para la creación de cuentas de acceso. Las cuentas deben estar basadas en roles y otorgar al usuario solo los privilegios y el acceso a los recursos necesarios para realizar su función de trabajo particular.

A.3.3.5.3.5 Privilegios mínimos

Los usuarios deben tener asignados los privilegios mínimos y las autorizaciones necesarias para realizar sus tareas. El acceso debe otorgarse en función de la necesidad de apoyar una función laboral particular. Los privilegios basados en roles deben considerar requisitos especiales para instalar software, requisitos para configurar servicios, necesidades de intercambio de archivos y necesidades de acceso remoto.

A.3.3.5.3.6 Separación de deberes

El proceso de administración de cuentas incluye principios de separación de funciones con aprobadores e implementadores separados de la configuración de la cuenta. Este principio proporciona una capa adicional de protección para que una persona no pueda comprometer un sistema solo.

A.3.3.5.3.7 Identificar individuos

Todos los usuarios deben poder identificarse con cuentas de acceso separadas a menos que existan riesgos de HSE para dichas cuentas. En tales casos, se deben emplear otros controles de seguridad física para limitar el acceso. El acceso debe controlarse mediante un método apropiado de autenticación (es decir, ID de usuario y contraseña, números de identificación personal (PIN) o tokens). Estas credenciales personales no se deben compartir, excepto en ciertas situaciones especiales. Un caso especial es en una sala de control donde los operadores funcionan como un solo equipo de trabajo o tripulación. En esta situación, todos los miembros del equipo de trabajo pueden usar las mismas credenciales. (Se proporciona una discusión adicional sobre este tema en A.3.3.6.). Debe existir un proceso de identificación alternativo en el caso de una contraseña olvidada.

A.3.3.5.3.8 Autorización

El acceso debe otorgarse bajo la autoridad de un gerente apropiado (ya sea de la empresa responsable o de una organización asociada). Las aprobaciones deben ser hechas por supervisores familiarizados con las tareas de fabricación / operaciones y la capacitación específica que una persona ha tenido para ese rol.

A.3.3.5.3.9 Cuentas de acceso innecesarias

Las cuentas de acceso son los medios para controlar el acceso al sistema, por lo tanto, es importante que estas cuentas se inactiven, suspendan o eliminen y se revoquen los permisos de acceso tan pronto como ya no sean necesarios (por ejemplo, cambio de trabajo, finalización y similares). El administrador apropiado debe tomar esta acción lo antes posible después de que la cuenta de acceso ya no sea necesaria.

A.3.3.5.3.10 Revisar los permisos de la cuenta de acceso

La necesidad de acceso a sistemas críticos se confirma explícitamente de forma regular. Todas las cuentas de acceso establecidas deben revisarse periódicamente para asegurarse de que la cuenta todavía esté en uso, su función y sus necesidades de acceso sigan siendo correctas, el usuario aún esté autorizado y solo tenga los permisos mínimos requeridos. Las cuentas inactivas o innecesarias deben eliminarse. Si una cuenta de acceso permanece sin usar durante un período prolongado, el propietario de la cuenta y el patrocinador de la cuenta confirman explícitamente su necesidad.

A.3.3.5.3.11 Registro de cuentas de acceso

Una de las funciones principales de la administración de cuentas es el registro de las cuentas de acceso individuales. Se deben mantener registros de todas las cuentas de acceso, incluidos los detalles de la persona, sus permisos y el administrador de autorización.

A.3.3.5.3.12 Gestión del cambio

El proceso de gestión de cambios para la administración de cuentas debe identificar claramente cualquier restricción de tiempo que se deba seguir debido a los riesgos de seguridad de realizar cambios durante ciertas secuencias de operaciones industriales. Estos cambios se tratan con tanta importancia como los cambios en el proceso, el software y el equipo. El proceso de administración de la cuenta de acceso debe integrarse con los procedimientos normalizados de gestión de seguridad del proceso (PSM) e incluir pasos de aprobación y documentación. Los aprobadores de cuentas de acceso para funciones de fabricación / operaciones pueden ser un conjunto diferente de personas que los usuarios aprobados para los sistemas de TI. Las aprobaciones deben ser hechas por supervisores familiarizados con las tareas de fabricación / operaciones y la capacitación específica que una persona ha tenido para ese rol.

A.3.3.5.3.13 Contraseñas predeterminadas

Muchos sistemas de control vienen con contraseñas predeterminadas que se utilizan para configurar el sistema y prepararlo para la operación. Estas contraseñas de cuentas de acceso a menudo son ampliamente conocidas o fáciles de determinar a partir de la literatura publicada u otras fuentes. Estas contraseñas predeterminadas deben cambiarse inmediatamente después de la configuración y antes de la conexión al sistema.

A.3.3.5.3.14 Administración de cuentas de auditoría

Se deben realizar revisiones periódicas para el cumplimiento de la información de administración de la cuenta de acceso. Esto garantiza que los propietarios de la información o los documentos cumplan con las políticas, normas u otros requisitos establecidos por la organización.

A.3.3.5.4 Prácticas de apoyo

A.3.3.5.4.1 Prácticas de referencia

Las siguientes nueve acciones son prácticas básicas:

a) Asignación de los privilegios mínimos y autorizaciones a los usuarios necesarios para realizar sus tareas. El acceso debe otorgarse sobre la base de la necesidad de realizar una función de trabajo particular.

b) Controlar la identificación y el acceso para cada usuario individual mediante un método apropiado de autenticación (por ejemplo, ID de usuario y contraseña). Estas credenciales personales (es decir, contraseñas, PIN y / o tokens) no se comparten, excepto en ciertas situaciones especiales.

c) Establecer un proceso de identificación alternativo en caso de pérdida de credenciales o una contraseña olvidada.

d) Conceder, cambiar o finalizar el acceso bajo la autoridad de un gerente apropiado (de la organización, organización contratante o un tercero). Se mantiene un registro de todas las cuentas de acceso, incluidos los detalles de la persona, sus permisos y el administrador de autorización.

e) Suspender o eliminar todas las cuentas de acceso y revocar permisos tan pronto como ya no sean necesarios (por ejemplo, cambio de trabajo).

f) Revisar todas las cuentas de acceso establecidas de manera regular para asegurar que todavía estén en uso y que aún requieran acceso a sistemas críticos.

g) Reconfirmar la necesidad de acceso a las cuentas con el administrador apropiado si las cuentas no se utilizan durante un período prolongado de tiempo.

h) Requerir que las contraseñas predeterminadas se cambien inmediatamente.

i) Requerir que todo el personal (es decir, empleados, empresas conjuntas, contratistas externos y empleados temporales) acuerde por escrito cumplir con la política de seguridad, incluidas las políticas de control de acceso.

A.3.3.5.4.2 Prácticas adicionales

Las siguientes cinco acciones son prácticas adicionales:

a) Usar herramientas (es decir, aprovisionamiento y gestión de identidad) para gestionar el proceso de creación, suspensión y eliminación de cuentas de acceso. Un sistema de aprovisionamiento también gestiona el flujo de trabajo de aprobación mediante el cual el propietario de la empresa aprueba el acceso, incluido el registro. También puede automatizar el proceso de creación / suspensión de cuentas en los sistemas de destino.

b) Vincular el proceso de administración de la cuenta con el proceso de recursos humanos para que los cambios de los empleados activen revisiones y actualizaciones para acceder a las cuentas.

c) Definir y documentar los roles de aplicación / privilegios de usuario (es decir, funciones de trabajo asignadas a roles de aplicación y derechos de acceso para cada rol) por el propietario o delegado de la información de la aplicación.

d) Prestar especial atención a los usuarios con acceso privilegiado (es decir, revisiones y verificaciones de antecedentes más frecuentes).

e) Permitir a los usuarios tener más de una cuenta de acceso, en función de su rol de trabajo en ese momento en particular. Una persona usaría una cuenta de acceso del administrador del sistema para realizar una actualización de la aplicación en una máquina en particular, pero también necesitaría una cuenta de acceso del operador para ejecutar y probar la aplicación.

A.3.3.5.5 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en la siguiente referencia, que se enumera en la Bibliografía: [6].

A.3.3.6 Elemento: Control de acceso: Autenticación

A.3.3.6.1 Descripción del elemento

NOTA Para obtener información adicional sobre el tema general del control de acceso, consulte el material introductorio en A.3.3.5.1.

La autenticación, otra de las tres etapas del control de acceso, como se muestra en la Figura A.11, es el método para identificar positivamente a los usuarios, hosts, aplicaciones, servicios y recursos de la red para algún tipo de transacción computarizada para que puedan recibir la autorización correcta, en función de los derechos y responsabilidades. El método utiliza una combinación de factores de identificación o credenciales. La autenticación es el requisito previo para permitir el acceso a los recursos en un sistema.

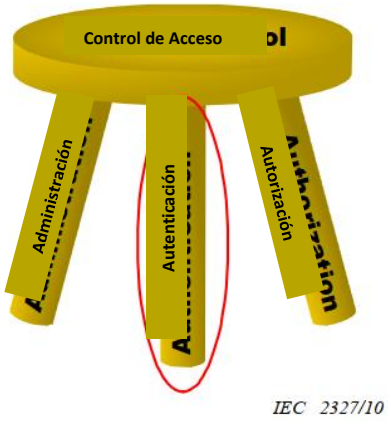

Figura A.11 - Control de acceso: autenticación

La autenticación en el entorno de IACS tiene varios desafíos que normalmente no se encuentran en situaciones de TI normales. Las tecnologías de autenticación de TI actuales tienen varias limitaciones que no son adecuadas para el entorno IACS y que en realidad podrían aumentar los riesgos de HSE a expensas de los menores riesgos de seguridad cibernética.

Es importante en el entorno de IACS asegurarse de que las personas adecuadas tengan acceso a la información y los sistemas correctos y que no se les impida hacer su trabajo a través de la autenticación. No autenticar a un usuario válido podría tener implicaciones de HSE si el usuario no puede realizar tareas en una situación crítica. En el entorno IACS, hay un gran énfasis en combinar medidas de autenticación física con prácticas de autenticación electrónica.

La ubicación física del usuario puede tener un impacto significativo en el nivel de riesgo del acceso. Por ejemplo, el usuario que se conecta a un sistema desde el interior de un edificio que emplea un sistema de guardia y lector de distintivos en la puerta es menos riesgoso que un usuario que se conecta desde alguna otra región del mundo. La estrategia de autenticación aborda los controles combinados de seguridad física y cibernética que se utilizarán para controlar el riesgo general. La estrategia define claramente los requisitos de autenticación para situaciones especiales.

Existen varios tipos de estrategias de autenticación y cada uno tiene diferentes grados de fortaleza. Los métodos de autenticación sólidos son bastante precisos para identificar positivamente al usuario. Los métodos de autenticación débiles son los que pueden ser fácilmente derrotados para proporcionar acceso no deseado a la información.

La ubicación física del usuario puede tener un impacto significativo en el riesgo de acceder al IACS. La autenticación para estos casos se analizará en las siguientes subcláusulas.

A.3.3.6.2 Autenticación para usuarios locales.

Es muy importante que solo los recursos capacitados y designados tomen medidas en las estaciones de HMI de control industrial, como las estaciones de control del operador. Muchas industrias controlan sus equipos desde salas de control atendidas por varios operadores. Estos operadores a menudo funcionan como un equipo y realizan acciones en múltiples estaciones HMI como parte de su función de trabajo normal. Las

cuentas de acceso comunes compartidas por el equipo de operadores se emplean con frecuencia. Hasta que los esquemas de autenticación rentables, robustos y sólidos estén disponibles en las estaciones HMI, la práctica recomendada es utilizar controles físicos para garantizar que solo las personas designadas realicen acciones en las estaciones HMI de la sala de control. El acceso a las salas de control debe gestionarse mediante combinaciones apropiadas de tecnologías de control de entrada y procedimientos administrativos. Considere las implicaciones de HSE al desarrollar los procedimientos de control de acceso.

A.3.3.6.3 Autenticación para usuarios remotos.

Un usuario remoto es cualquier persona que esté fuera del perímetro de la zona de seguridad a la que se dirige.

EJEMPLO Un usuario remoto puede ser una persona en una oficina en el mismo edificio, una persona que se conecta a través de la red de área amplia corporativa (WAN) o una persona que se conecta a través de redes de infraestructura pública.

Los controles físicos y administrativos que dependen de la autenticación visual no funcionan para usuarios interactivos remotos. Sin embargo, existen numerosos esquemas de autenticación basados en tecnología que pueden usarse. Es importante emplear un esquema de autenticación con un nivel de fortaleza apropiado para identificar positivamente al usuario interactivo remoto. Las operaciones industriales con un bajo potencial para crear incidentes HSE y que tienen un bajo impacto financiero pueden protegerse utilizando métodos de autenticación débiles, como una identificación de usuario y contraseña simples. Sin embargo, las operaciones industriales donde hay una gran participación financiera o de HSE deben protegerse utilizando tecnologías de autenticación sólidas. Para este tipo de operaciones, se recomienda que el sistema se diseñe de manera que el usuario de acceso remoto no pueda realizar funciones de control, solo funciones de monitoreo.

A.3.3.6.4 Autenticación para la comunicación de tarea a tarea

La discusión anterior se centró en los usuarios interactivos. Es igual de importante emplear esquemas de autenticación apropiados para la comunicación de tarea a tarea entre servidores de aplicaciones o entre servidores y dispositivos controlados. La interfaz de comunicaciones debe emplear métodos para verificar que el dispositivo solicitante es el dispositivo correcto para realizar la tarea. Algunas formas en que las interfaces críticas podrían autenticar las comunicaciones de tarea a tarea entre dispositivos son verificar la dirección de protocolo de Internet (IP), verificar la dirección de control de acceso a medios (MAC), usar un código secreto o usar una clave criptográfica para verificar que la solicitud proviene del dispositivo esperado. Las interfaces con bajo riesgo pueden usar métodos menos seguros para la autenticación. Un ejemplo de comunicaciones inseguras es un protocolo de transferencia de archivos anónimos (FTP) para cargar / descargar / comparar programas entre la HMI de control y un repositorio de datos.

A.3.3.6.5 Consideraciones para la autenticación

A.3.3.6.5.1 General

Al desarrollar un programa para el control de acceso, es importante incluir todos los sistemas dentro del alcance, y no solo limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras.

a) Definir una estrategia de autenticación

   Las empresas deben tener una estrategia o enfoque de autenticación que defina el método de autenticación que se utilizará.

b) Autenticar a todos los usuarios antes de usar el sistema

Todos los usuarios deben autenticarse antes de usar la aplicación solicitada. Esta autenticación puede ser una combinación de prácticas de autenticación física y cibernética.

c) Requerir cuentas fuertes y seguras para la administración del sistema y / o la configuración de la aplicación

Deben usarse prácticas de identificación de usuario y contraseña de cuenta sólidas en todas las cuentas de acceso de configuración de aplicaciones y administrador del sistema. El administrador del sistema generalmente no necesita acceso rápido para realizar tareas a nivel del sistema en las computadoras. Es más importante evitar que usuarios no capacitados realicen funciones a nivel de sistema que proporcionar un acceso rápido.

d) Requerir administración local

En sistemas muy críticos, es una buena práctica realizar todas las funciones de configuración de aplicaciones o administrador del sistema localmente en el dispositivo para reducir la posibilidad de una interrupción de la red que cause un problema con el control del equipo. El administrador del sistema o el administrador de la aplicación deben coordinar todos los cambios con el operador del área para que la producción no se vea afectada durante un cambio de configuración.

A.3.3.6.5.2 Autenticación para usuarios locales.

Si una práctica presenta el potencial de retrasar la capacidad de un operador para realizar acciones correctivas rápidas en la operación industrial desde la estación de control HMI, son las prácticas normales de autenticación de TI, que pueden no ser apropiadas. Para lograr la seguridad en la operación del sistema de control y al mismo tiempo proporcionar una respuesta rápida, se ha encontrado que una combinación de controles físicos y cibernéticos produce los mejores resultados. Algunos de estos controles incluyen, entre otros:

· Cerraduras manuales (por ejemplo, llave y combinación) en puertas de habitaciones o armarios que contienen componentes del sistema de control;

· Cerraduras automatizadas (por ejemplo, credenciales y lectores de tarjetas);

· Salas de control con personal continuo;

· Responsabilidad individual por parte del personal de la sala de control para mantener el acceso limitado al personal designado y garantizar que solo personal capacitado realice acciones en las estaciones de control del operador.

Algunos ejemplos de prácticas comunes de TI que pueden *no* ser aplicables en un entorno IACS son:

a) ID de usuario y contraseñas individuales para cada operador para entornos de trabajo en equipo.

Muchas industrias controlan sus operaciones desde salas de control atendidas por varios operadores. Estos operadores a menudo funcionan como un equipo y realizan acciones en múltiples estaciones HMI como parte de su función de trabajo normal. Requerir que cada operador inicie sesión y se autentique y autorice cada vez que use una nueva HMI podría comprometer la respuesta rápida a un evento de operación.

b) Acceso a controladores de dominio no locales y servidores de directorio activo para la autenticación de la cuenta de acceso.

Los problemas de red pueden interferir con el inicio de sesión oportuno bajo esta arquitectura.

c) Bloqueo automático de la cuenta de acceso después de cierto número de intentos fallidos de inicio de sesión.

En algunas condiciones que requieren una respuesta rápida por parte de un operador, el operador puede ponerse nervioso e ingresar la contraseña incorrecta. Si el operador queda bloqueado, podría comprometer la capacidad del operador para resolver la situación.

d) Contraseñas largas y robustas que contienen una combinación de caracteres alfabéticos, numéricos y especiales.

Aunque las contraseñas robustas proporcionan una mayor medida de seguridad, en el entorno de la sala de control, el requisito de ingresar dichas contraseñas podría reducir el tiempo de respuesta de un operador. Un nivel similar de seguridad podría lograrse por medios físicos como puertas cerradas o personal continuo de la sala de control por aquellos que conocen a los operadores autorizados.

e) Cambios de contraseña después de un número específico de días.

El impacto de cambiar las contraseñas es muy similar al de las contraseñas robustas, puede retrasar la respuesta a una situación en la que se necesita una respuesta rápida. Las contraseñas deben cambiarse cuando hay un cambio en el personal, pero cambiar después de un número determinado de días puede no ser productivo.

f) Protectores de pantalla con protección por contraseña.

Muchas estaciones HMI están diseñadas para informar por excepción. Es posible que el operador no necesite realizar ninguna acción en la estación del operador hasta que se produzca una alerta. Los protectores de pantalla tienen el potencial de interferir con el operador al bloquear la vista de la operación bajo control y retrasar la respuesta a una situación de emergencia.

A.3.3.6.5.3 Autenticación para usuarios remotos.

Los usuarios remotos normalmente no necesitan responder rápidamente a situaciones comunes a los operadores. Además, para los usuarios remotos, la responsabilidad se vuelve más importante que la disponibilidad. Por lo tanto, algunas de las prácticas comunes a la seguridad de TI también son beneficiosas para los usuarios remotos. Éstas incluyen:

a) Autenticar a todos los usuarios remotos en el nivel apropiado.

La organización debe emplear un esquema de autenticación con un nivel adecuado de fortaleza para identificar positivamente a un usuario interactivo remoto.

b) Registre y revise todos los intentos de acceso a sistemas críticos.

El sistema debe registrar todos los intentos de acceso a sistemas críticos y la organización debe revisar estos intentos si tuvieron éxito o fallaron.

c) Deshabilite la cuenta de acceso después de intentos fallidos de inicio de sesión *remoto.*

Después de cierto número de intentos fallidos de inicio de sesión por parte de un usuario remoto, el sistema debe deshabilitar la cuenta de acceso del usuario durante un cierto período de tiempo. Esto ayuda a disuadir los ataques de descifrado de contraseña de fuerza bruta en el sistema. Aunque los usuarios remotos normalmente no necesitan responder rápidamente a situaciones de operación, puede haber casos, como salas de control no tripuladas o instalaciones remotas (por ejemplo, sistemas SCADA que controlan un sistema de distribución eléctrica) donde se requiere un acceso rápido desde una ubicación remota. En estos casos, deshabilitar la cuenta de acceso puede no ser apropiado. Cada organización debe abordar la autenticación de usuarios remotos de manera apropiada a su situación y tolerancia al riesgo.

d) Requerir autenticación después de la inactividad remota del sistema

Después de un período definido de inactividad, se debe solicitar a un usuario remoto que se vuelva a autenticar antes de poder acceder nuevamente al sistema. Esto asegura que la cuenta de acceso no se deje abierta y accesible desde el dispositivo remoto. Aunque los usuarios remotos normalmente no necesitan conectarse al sistema de control durante largos períodos de tiempo, puede haber casos, como salas de control no tripuladas o instalaciones remotas (por ejemplo, sistemas SCADA en un sistema de distribución eléctrica) donde un operador remoto puede necesitar para monitorear el sistema durante un período prolongado de tiempo. En estos casos, requerir una nueva autenticación puede no ser apropiado. Cada organización debe abordar la autenticación de usuarios remotos de manera apropiada a su situación y tolerancia al riesgo.

Para usuarios remotos, el nivel de autenticación requerido debe ser proporcional al riesgo para el sistema al que se accede. La autenticación débil puede ser apropiada si el sistema no tiene control sobre las operaciones con un alto riesgo de HSE. Para sistemas con riesgos HSE, la autenticación fuerte puede ser más apropiada.

Los ejemplos de autenticación débil incluyen:

· Conectar módems directamente a dispositivos o redes de control de operaciones industriales que emplean autenticación de ID de usuario y contraseña simples;

· Conectar dispositivos o redes de control de operación industrial desde la LAN o WAN corporativa que emplean autenticación de ID de usuario y contraseña simples;

· Utilizando la identificación de usuario de Microsoft Windows® y la autenticación de contraseña a nivel de aplicación en dispositivos de control de operación industrial.

Los ejemplos de autenticación fuerte incluyen:

· Usar un token físico o una tarjeta inteligente de autenticación de dos factores que requiere un dispositivo físico y un conocimiento único (por ejemplo, un número de identificación personal, PIN) en posesión del usuario;

NOTA La seguridad se mejora mediante la entrada segura de PIN, por ejemplo, cuando se ingresa el PIN con un lector seguro para evitar el registro de teclas.

· Autenticación mediante tarjetas inteligentes o datos biométricos;

· Autenticación de usuarios en función de su ubicación;

· Conectar módems a dispositivos o redes de control de operaciones industriales que emplean una función de devolución de llamada a un número de teléfono predefinido;

· Conectar dispositivos o redes de control de operación industrial a la LAN o WAN corporativa y usar tarjetas inteligentes o autenticación biométrica;

· Conectar computadoras domésticas a dispositivos o redes de control de operaciones industriales mediante una conexión VPN y autenticación de dos factores con un token y un PIN.

A.3.3.6.5.4 Autenticación para la comunicación de tarea a tarea.

Las comunicaciones de tarea a tarea generalmente no se supervisarán directamente como las sesiones interactivas del usuario. La autenticación de las comunicaciones de tarea a tarea generalmente se realizará

al inicio de una operación industrial y posteriormente a intervalos regulares. Los sistemas deberían emplear alguna solución técnica para autenticar cada dispositivo o red.

NOTA IEC / TR 62443 - 3 - 1 [6] proporciona una explicación de estas y otras tecnologías. Discute sus fortalezas y debilidades y su aplicabilidad al entorno IACS.

A.3.3.6.6 Prácticas de apoyo.

A.3.3.6.6.1 Prácticas de referencia

Las siguientes cinco acciones son prácticas básicas:

a) Establecer una estrategia o enfoque que defina el método de autenticación que se utilizará. El método puede variar según los riesgos, las consecuencias asociadas con el proceso comercial y la sensibilidad de los datos.

b) Emplear diferentes estrategias para usuarios que se conectan desde diferentes ubicaciones geográficas (incluidas instalaciones remotas) o para dispositivos con requisitos especiales de seguridad. Este problema tiene en cuenta las características de seguridad física que interactúan con las características de seguridad cibernética para establecer el nivel de seguridad general para el usuario.

c) Autenticar a todos los usuarios antes de permitir el uso de una aplicación en particular. Este requisito se puede renunciar cuando hay controles físicos compensatorios.

d) Requerir al menos un ID de usuario y contraseña ingresados manualmente como el nivel mínimo de autenticación electrónica.

e) Autenticar la comunicación de tarea a tarea conociendo la dirección MAC y / o IP del dispositivo, una clave electrónica específica, el nombre del dispositivo y similares.

A.3.3.6.6.2 Prácticas adicionales

La siguiente acción es una práctica adicional:

a) Autorizar a los usuarios dentro de una instalación cerrada que emplea guardias y lectores de credenciales para acceder a los sistemas que tienen un mayor nivel de riesgo que un usuario remoto.

A.3.3.6.7 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [6], [23].

A.3.3.7 ELEMENTO - Control de acceso: Autorización

Para obtener información adicional sobre el tema general del control de acceso, consulte el material introductorio en A.3.3.5.1.

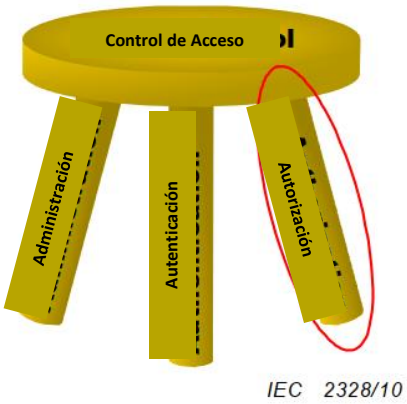

Figura A.12 - Control de acceso: Autorización

La autorización, el tercer tramo del control de acceso se muestra en la Figura A.12, es el procedimiento automatizado realizado por el sistema informático para otorgar acceso a los recursos tras la autenticación exitosa del usuario y la identificación de su cuenta de acceso asociada. Los privilegios otorgados están determinados por la configuración de la cuenta de acceso establecida durante el paso de administración de la cuenta en el procedimiento.

Algunos procedimientos de autorización normalizados empleados en el espacio de trabajo general de TI pueden ser inapropiados o inadecuados para IACS. Por ejemplo, las cuentas de acceso en un sistema de TI típico se basan principalmente en el usuario con un número limitado de roles asignados (es decir, usuario estándar o administrador del sistema). Por lo general, a cada usuario solo se le asigna un rol. Las cuentas de acceso en un sistema IACS típico se basarán principalmente en roles con una mayor granularidad de roles (es decir, operador, ingeniero, especialista en aplicaciones, proveedor y administrador del sistema). A los usuarios se les pueden asignar múltiples roles en función de una función de trabajo que necesitan realizar en un momento particular. El usuario puede tener que iniciar sesión en un dispositivo en particular y, por separado, en una aplicación para ser autorizado a realizar cambios en las variables de control de automatización industrial. O, un usuario puede tener que cerrar sesión en un sistema y volver a iniciar sesión para realizar tareas de administración del sistema en ese mismo dispositivo.

Esta subcláusula explora los controles destinados a proteger la información y los activos de la destrucción, cambio o divulgación deliberada e inadvertida. Se enfoca específicamente en medidas diseñadas para garantizar que los agentes autenticados (es decir, personal, aplicaciones, servicios y dispositivos) tengan acceso a los activos de información requeridos.

La información sensible a la divulgación debe protegerse adecuadamente tanto para mantener una ventaja competitiva como para proteger la privacidad de los empleados.

Las reglas de autorización deseadas por una organización determinarán cómo asigna roles a usuarios específicos o grupos de usuarios y cómo se configuran los privilegios para estas cuentas de acceso. La capacidad de implementar una política de autorización deseada depende de las características de los sistemas subyacentes para distinguir las funciones y los datos requeridos para diferentes roles de trabajo.

Por lo tanto, la definición de una política de autorización es un procedimiento iterativo en el que la organización define una política ideal y luego determina cuán estrechamente se puede implementar utilizando las

capacidades de sus sistemas y redes. Si se adquiere un nuevo sistema, el soporte para una política de autorización deseada puede ser un elemento de la especificación de adquisición. Al diseñar una nueva configuración de red, se pueden agregar tecnologías como firewalls para usuarios remotos para crear una capa adicional de autorización para dispositivos críticos, como se describe en los siguientes párrafos.

A.3.3.7.1 Consideraciones para la autorización

A.3.3.7.1.1 General

Al desarrollar un programa para el control de acceso, es importante incluir todos los sistemas dentro del alcance, y no solo limitar el esfuerzo a las instalaciones tradicionales de la sala de computadoras.

a) Política de seguridad de autorización.

   Las reglas que definen los privilegios autorizados en las cuentas de acceso para el personal en varios roles de trabajo deben definirse en una política de seguridad de autorización que esté claramente documentada y aplicada a todo el personal tras la autenticación.

b) Métodos de permiso lógico y físico para acceder a dispositivos IACS.

   El permiso para acceder a los dispositivos IACS debe ser lógico (reglas que otorgan o niegan el acceso a usuarios conocidos en función de sus roles), físicos (bloqueos, cámaras y otros controles que restringen el acceso a una consola de computadora activa) o ambos.

c) Acceso a información o sistemas a través de cuentas basadas en roles.

   Las cuentas de acceso deben estar basadas en roles para administrar el acceso a información o sistemas apropiados para el rol de ese usuario. Las implicaciones de seguridad son un componente crítico de la definición de roles.

A.3.3.7.1.2 Autorización para usuarios locales.

Muchas industrias de procesos controlan sus operaciones desde salas de control atendidas por varios operadores. Estos operadores a menudo funcionan como un equipo y realizan acciones en múltiples estaciones HMI como parte de su función de trabajo normal. La aplicación proporciona la autorización para realizar funciones de trabajo específicas. El usuario local tiene acceso a ciertos dispositivos o pantallas operativas basadas en una cuenta de acceso basada en roles. El ID de usuario y la contraseña de inicio de sesión reales suelen ser comunes para todos los que desempeñan el puesto de trabajo. Este enfoque de equipo de trabajo para la operación de la sala de control puede entrar en conflicto con la política y la práctica normalizada de autorización de TI.

Las implicaciones de seguridad se considerarán al desarrollar la estrategia de autorización. Para operaciones industriales de alta vulnerabilidad, los privilegios de autorización deben establecerse en el nivel de dispositivo de control de proceso local y no deben requerir acceso a dispositivos en el nivel LAN o WAN para asignar privilegios. Esto apoya el principio de control básico de minimizar los puntos potenciales de falla.

Las cuentas de acceso deben configurarse para otorgar los privilegios mínimos necesarios para el rol de trabajo. La capacitación debe emplearse para establecer niveles comunes de habilidades para cada uno de los roles de trabajo. Se debe evitar personalizar las cuentas de acceso individual para que coincidan con los niveles de habilidad del personal. Todos los usuarios en la misma función de trabajo deben utilizar cuentas de acceso configuradas para el mismo rol.

A.3.3.7.1.3 Autorización para usuarios remotos.

El proceso de autorización discutido hasta ahora coloca la función de autorización en el dispositivo de nodo final y en el nivel de aplicación. En entornos de control críticos, se debe emplear una estrategia de autorización de destino adicional en un dispositivo de barrera (firewall o enrutador) para la red IACS. Una vez que un usuario se autentica en el dispositivo de barrera, los derechos de acceso de destino basados en roles deben asignarse al usuario para que el usuario solo pueda intentar conectarse a dispositivos preasignados en la red IACS. El inicio de sesión del nodo final debe establecer los privilegios finales del usuario para realizar funciones en el dispositivo. Las instalaciones con vulnerabilidades altas deberían aprovechar este nivel adicional de autorización de destino.

Las cuentas de acceso basadas en roles deben tener en cuenta la ubicación geográfica. Una persona puede utilizar una cuenta de acceso cuando trabaja en el sitio y otra diferente cuando llama desde su casa para ayudar al personal local. Esta práctica debe estar claramente definida en los procedimientos administrativos. El cumplimiento de los procedimientos administrativos debe basarse en la responsabilidad individual.

A.3.3.7.2 Prácticas de apoyo

A.3.3.7.2.1 Prácticas de referencia

Las siguientes dos acciones son prácticas básicas:

a) Permitir el acceso a dispositivos IACS con controles lógicos (reglas que otorgan o niegan el acceso a usuarios conocidos en función de sus roles), controles físicos (bloqueos, cámaras y otros controles que restringen el acceso a una consola de computadora activa) o ambos.

b) Registrar y revisar todos los intentos de acceso a sistemas informáticos críticos, tanto exitosos como fallidos.

A.3.3.7.2.2 Prácticas adicionales

Las siguientes seis acciones son prácticas adicionales:

a) Proteger las conexiones de red entre la organización y otras organizaciones mediante el uso de un firewall administrado.

b) Usar un servidor proxy de autenticación para todo el acceso saliente a Internet.

c) Conceder acceso a un usuario remoto habilitando un módem en un dispositivo de control de operaciones industriales solo cuando sea necesario.

d) Usar el acceso marcad cuando se realizan tareas de alto riesgo (por ejemplo, operaciones industriales que tienen consecuencias HSE o que constituyen riesgos comerciales críticos).

e) Segregar datos con alta sensibilidad y / o consecuencias comerciales de otra información interna para que los controles de autorización existentes puedan restringir el acceso a esa información.

f) Separar la red comercial de la red IACS con un dispositivo de control de acceso y limitar el acceso del usuario a activos críticos en ambos lados.

A.3.3.7.3 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [6], [23], [27], [30], [43].

A.3.4 Grupo de elementos: implementación.

A.3.4.1 Descripción del grupo de elementos.

El tercer grupo de elementos en esta categoría es Implementación. Este elemento dentro de este grupo trata temas relacionados con la implementación del CSMS. La figura A.13 muestra una representación gráfica de los cuatro elementos en el grupo de elementos:

· Gestión e implementación de riesgos,
· Desarrollo y mantenimiento del sistema,
· Gestión de información y documentos y
· Planificación y respuesta a incidentes.

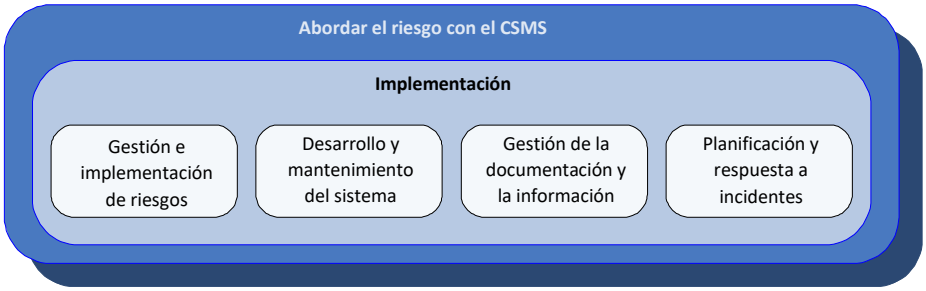

Figura A.13 - Vista gráfica del grupo de elementos: implementación

A.3.4.2 El elemento: gestión de riesgos e implementación.

A.3.4.2.1 Descripción del elemento.

La base de cualquier programa de seguridad o CSMS es mantener el riesgo a un nivel aceptable. La gestión e implementación de riesgos aborda la selección, el desarrollo y la implementación de medidas de seguridad que sean proporcionales a los riesgos. Las medidas de seguridad pueden tener en cuenta un diseño de operación industrial inherentemente más seguro, el uso de productos con fuertes capacidades de seguridad inherentes, contramedidas de seguridad manuales y de procedimiento y contramedidas basadas en tecnología para prevenir o reducir incidentes de seguridad.

Aunque el riesgo nunca se eliminará por completo, se puede gestionar. Esta subcláusula describe un marco para medir el riesgo y luego administrarlo mediante la implementación de varias contramedidas de seguridad para reducir la probabilidad de que ocurra un incidente o las consecuencias del evento resultante.

En la mayoría de los casos, el riesgo se mide en términos de costo y / o concientización social. Si bien puede ser fácil poner un precio a un corte de producción debido a un incidente de seguridad cibernética, no es posible asignar un costo exacto a un evento que resulte en la lesión o muerte de una persona. Las empresas determinarán su tolerancia al riesgo a ciertos tipos de eventos y la utilizarán para impulsar la estrategia de gestión de riesgos.

A.3.4.2.2 Construir un marco de gestión e implementación de riesgos.

Debido a que la eliminación de todos los riesgos suele ser poco práctica o imposible, las organizaciones deben centrarse en las aplicaciones e infraestructuras más críticas para disminuir el riesgo a un nivel aceptable. Decidir qué contramedidas de ciberseguridad implementar es una cuestión de equilibrar el riesgo y el costo. Las decisiones deben basarse en una evaluación de riesgos y documentarse para que sirvan de base para la planificación y la acción futuras.

Las organizaciones deben analizar la evaluación detallada del riesgo, identificar el costo de la mitigación para cada riesgo, comparar el costo con el riesgo de ocurrencia y seleccionar aquellas contramedidas donde el costo es menor que el riesgo potencial. Debido a que puede ser poco práctico o imposible eliminar todos los riesgos, enfóquese primero en mitigar el riesgo para las aplicaciones e infraestructuras más críticas. Los mismos riesgos a menudo se encuentran en más de una ubicación. Tiene sentido considerar seleccionar un conjunto normalizado de contramedidas que puedan ser aplicables en más de una instancia y luego definir cuándo usarlas. Este enfoque permitirá a la organización aprovechar soluciones comunes y reducir los costos de diseño e implementación para mejorar la postura de seguridad de la organización. Una posible forma de abordar esto es desarrollar un marco general para la implementación que incorpore la evaluación de riesgos, la tolerancia de la organización al riesgo, la evaluación y selección de contramedidas y la estrategia para implementar actividades de reducción de riesgos.

Es probable que cada organización tenga una tolerancia al riesgo diferente que estará influenciada por las regulaciones, los impulsores comerciales y los valores fundamentales. La tolerancia al riesgo de la organización para los incidentes de IACS determina la cantidad de esfuerzo que una organización está dispuesta a gastar para reducir el nivel de riesgo a un nivel aceptable. Si la organización tiene una baja tolerancia al riesgo, puede estar dispuesta a comprometer una mayor cantidad de recursos financieros y / o de personal para la tarea de mejorar el nivel de seguridad del IACS.

La Tabla A.2 identifica la sensibilidad de la organización a los diferentes tipos de riesgo y agrega las diversas consecuencias en categorías de alto, medio o bajo. Cuando estas categorías de consecuencias se combinan con la probabilidad de que ocurra un incidente, como en la Tabla A.1, el resultado es una matriz de categoría de consecuencia versus probabilidad. En ausencia de un método analítico para medir cuantitativamente la probabilidad y la consecuencia, puede ser práctico simplemente asignar niveles de riesgo cualitativos de bajo, medio y alto a los puntos de intersección en la matriz. Estos niveles de riesgo reflejan la sensibilidad de la organización al riesgo, como se muestra en la Tabla A.3. Estos niveles de riesgo implican umbrales de tolerancia que impulsarán la estrategia de implementación de reducción de riesgos. Esta es una manera clara de comunicar la posición de la organización sobre el riesgo.

La estrategia de reducción de riesgos puede emplear diferentes contramedidas, prácticas de arquitectura, selección de dispositivos IACS y las decisiones de cuándo y dónde emplearlas en función del nivel de riesgo que se muestra en la Tabla A.3. Sistemas con una garantía de alto riesgo que emplean contramedidas más amplias para lograr un mayor nivel de seguridad.

Una forma de capturar las decisiones de la organización sobre la selección de contramedidas es desarrollar un cuadro que enumere las contramedidas específicas que se utilizarán para los dispositivos IACS en función del nivel de riesgo del IACS. Un ejemplo de un posible gráfico de contramedidas se muestra en la Tabla A.4.

La tabla define el conjunto de soluciones comunes de contramedidas que se utilizarán para tratar de alcanzar el nivel de seguridad objetivo. Estas contramedidas deben emplearse a menos que haya alguna restricción

única que haga que esta solución sea indeseable para un IACS dado. La estrategia de reducción de riesgos de la organización también puede usar las clasificaciones de nivel de riesgo para establecer prioridades y plazos para implementar las contramedidas identificadas que se muestran en la Tabla A.4. Los IACS con clasificaciones de alto riesgo probablemente deberían abordarse con mayor urgencia que los IACS de menor riesgo.

Las contramedidas para abordar un riesgo específico pueden ser diferentes para diferentes tipos de sistemas. Por ejemplo, los controles de autenticación de usuario para un servidor de control de aplicaciones avanzado asociado con un DCS pueden ser diferentes a los controles de autenticación para la HMI en la línea de empaquetado. Documentar y comunicar formalmente las contramedidas seleccionadas, junto con la guía de aplicación para usar las contramedidas, es una buena estrategia a seguir.

Tabla A.4 - Ejemplo de contramedidas y prácticas basadas en los niveles de riesgo de IACS

Contramedidas y prácticas de arquitectura.	**IACS de alto riesgo**	**IACS de riesgo medio**	**IACS de bajo riesgo**
Autenticación de dos factores para controlar el acceso al dispositivo.	Necesario	Necesario	Opcional
Endurecimiento del sistema operativo.	Necesario	Recomendado	Opcional
Emplear segmentación de red	Necesario	Necesario	Opcional
Emplear aplicación antivirus	Necesario	Necesario	Necesario
Uso de WLAN	No permitido	Puede ser permitido	Permitido
Autenticación de contraseña segura a nivel de aplicación	Necesario	Recomendado	Recomendado
Otras contramedidas	...	...	...

Existen muchas contramedidas de mitigación de riesgos de tecnología de la información que pueden y deben aplicarse a los dispositivos IACS. La orientación sobre contramedidas específicas se aborda en otras partes de la serie IEC 62443 que todavía están en desarrollo, como IEC 62443 - 3 - 2 [7] e IEC 62443 - 3 - 3 [8], que proporcionan una mirada en profundidad a diferentes contramedidas disponibles y su aplicación al entorno IACS.

La mayoría de las organizaciones tendrán un conjunto limitado de recursos financieros y de personal para aplicar a las actividades de CSMS. Como resultado, es importante utilizar estos recursos de una manera que produzca los mayores beneficios. Un marco de gestión de riesgos comienza con la comprensión de las vulnerabilidades que existen dentro del IACS y las posibles consecuencias que podrían ocurrir si se explota esa vulnerabilidad. Una vez que se comprenden los riesgos, la empresa necesita desarrollar un marco de implementación para reducir el riesgo o mantenerlo en un nivel aceptable. Varios de los modelos de seguridad discutidos en IEC / TS 62443 - 1 - 1 se utilizarán para crear el marco de implementación. Los modelos incluyen el Modelo de Nivel de Seguridad junto con el Modelo de Zona y Conducto.

NOTA Esta subcláusula trata una posible forma de abordar este elemento clave del CSMS utilizando los modelos de seguridad IEC / TS 62443 - 1 - 1. No hay un enfoque correcto para este elemento. Los enfoques alternativos pueden dar como resultado un marco muy funcional para gestionar el riesgo.

La discusión detallada y el ejemplo que sigue sobre el tema de la gestión e implementación de riesgos describe el proceso del marco tal como se aplica para reducir los riesgos de seguridad cibernética a un sistema existente en un área operativa industrial única. El marco es igualmente aplicable a muchos nuevos IACS en múltiples ubicaciones en todo el mundo.

No importa qué enfoque de gestión de riesgos e implementación se emplee, un marco de buena calidad debe abordar cuatro conjuntos principales de tareas durante la vida de un IACS:

· Evaluar el riesgo de la IACS;

· Desarrollar e implementar contramedidas;

· Documentar las contramedidas y el riesgo residual;

· Gestionar el riesgo residual durante la vida del IACS.

Estas tareas están cubiertas en detalle en A.3.4.2.3 hasta A.3.4.2.5 y están representadas gráficamente en los modelos de ciclo de vida de seguridad discutidos en IEC / TS 62443 - 1 - 1, 5.11.

A.3.4.2.3 Evaluación del riesgo. Determinar el nivel de riesgo de seguridad cibernética de IACS.

A.3.4.2.3.1 General

El modelo de zona y conducto, el modelo de ciclo de vida de nivel de seguridad y el modelo de referencia se describen en detalle en IEC / TS 62443 - 1 - 1. El uso y la integración de estos modelos se discutirán en esta subcláusula.

A.2.3 proporciona orientación sobre un procedimiento a seguir para analizar el riesgo del IACS. Esta es una de las primeras actividades en la fase de evaluación del modelo de ciclo de vida del nivel de seguridad. Una organización necesita desarrollar y documentar un proceso de análisis de riesgos para que pueda usarse en múltiples IACS en diferentes ubicaciones en toda la organización con resultados repetibles.

Esta subcláusula explica cómo la fase de evaluación se ajusta a la estrategia general de gestión de riesgos. Esto se ilustra al recorrer el escenario de examinar un IACS existente y mejorar la posición de seguridad cibernética de este sistema para reducir el riesgo. La figura A.14 muestra la fase de evaluación del modelo de ciclo de vida del nivel de seguridad.

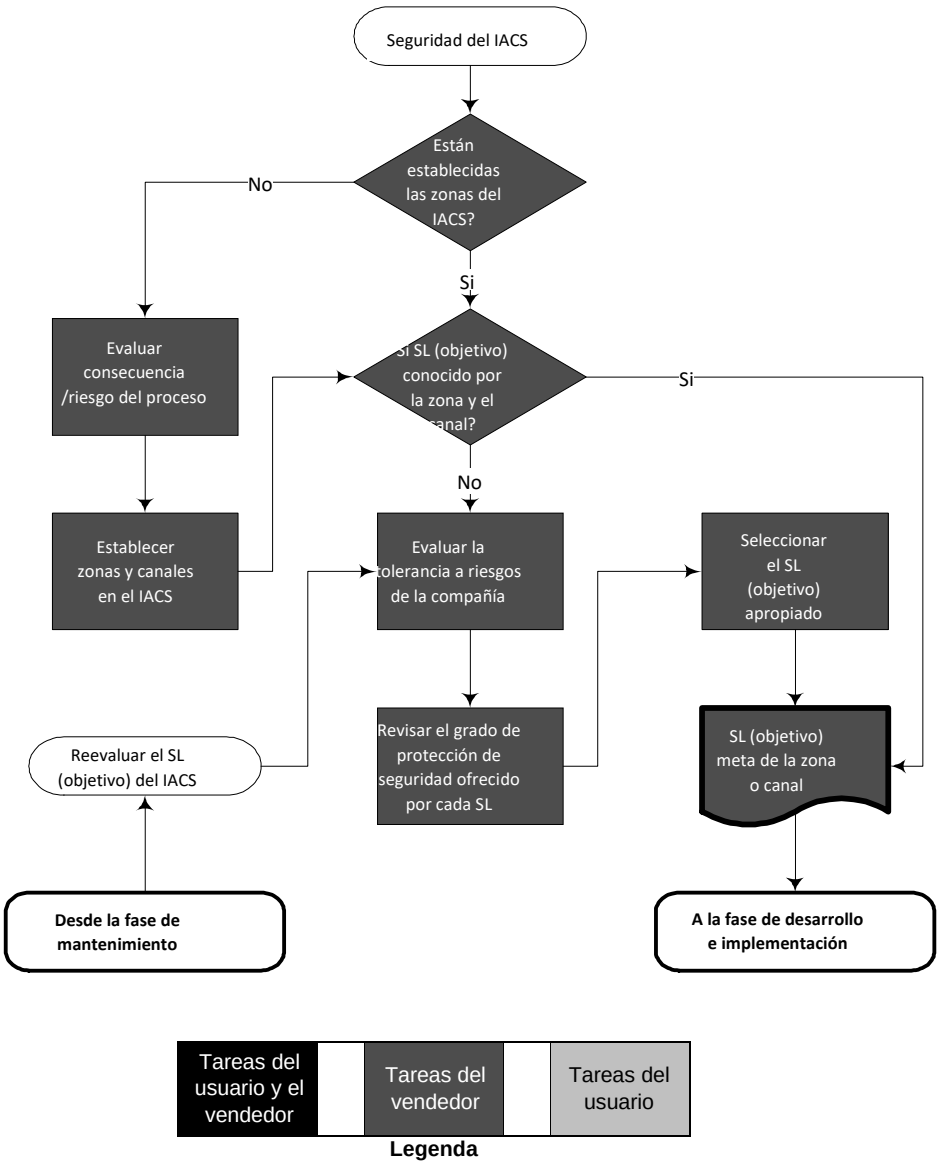

Figura A.14 - Modelo de ciclo de vida de nivel de seguridad: fase de evaluación

Para un IACS existente que nunca se ha sometido a una evaluación de riesgos y aún no ha empleado el modelo de Zona, la actividad comienza con el recuadro titulado "Evaluar consecuencia / riesgo del proceso".

El propósito de la evaluación es comprender el impacto del riesgo para el negocio en caso de que el IACS se vea comprometido por un incidente cibernético y no pueda realizar sus funciones de control previstas o funciones no intencionadas. Una vez que se ha documentado el riesgo asociado con el IACS, se deben realizar las actividades asociadas con la gestión y la mitigación del riesgo.

El resultado del análisis de riesgo será una tabla que enumere la calificación de consecuencia y la calificación de probabilidad para cada activo IACS o alguna colección de activos. La Tabla A.5 es un resultado de ejemplo de una evaluación detallada de riesgos y los resultados de combinar la Tabla A.1, la Tabla A.2 y la Tabla A.3

de esta norma. La calificación de probabilidad se asigna en función de la evaluación detallada de la vulnerabilidad de cada uno de los activos enumerados, y la probabilidad de que se realicen amenazas relacionadas.

Tabla A.5 - Ejemplo de tabla de activos IACS con resultados de evaluación

Dispositivo de dispositivo IACS	Clasificación de Consecuencia	Calificación de Probabilidad
Consola de sala de control del operador	A	Medio
Consola de operador remoto	C	Alto
Estación de configuración de ingeniería	A	Alto
Servidor historiador	B	Medio
Controlador	A	Medio
Puerta	B	Medio
Otros dispositivos	C	Bajo

A.3.4.2.3.2 Determinación del nivel de riesgo de IACS

La Tabla A.3 anterior es un modelo de ejemplo simplificado para traducir la sensibilidad de una empresa al riesgo en niveles cualitativos de riesgo para el IACS. Debe ser preparado por el liderazgo responsable de la organización antes de realizar el análisis de riesgos.

La intersección de las calificaciones de Consecuencia y Probabilidad produce el Nivel de riesgo.

EJEMPLO Un dispositivo IACS con una calificación de consecuencia de B y una probabilidad de Alto representaría un dispositivo de alto riesgo.

Las posturas de riesgo en la Tabla A.3 se pueden aplicar a los activos del dispositivo IACS en la Tabla A.5, lo que resulta en una calificación general para el IACS como se muestra en la Tabla A.6. Esta tabla proporciona un orden de prioridad para vulnerabilidades particulares.

Cada dispositivo tiene un nivel de riesgo de seguridad cibernética asociado. En un IACS estrechamente integrado, las funciones de control proporcionadas por cada dispositivo dependen en gran medida de la integridad de los otros dispositivos en el IACS. La integridad funcional del sistema de control se verá afectada por la integridad del dispositivo más débil.

Una suposición de seguridad simplificada es que el dispositivo con el nivel de riesgo IACS más alto establece el nivel de riesgo inherente para todo el IACS. En el ejemplo de IACS enumerado en la Tabla A.6, el nivel de riesgo inherente para el IACS es de alto riesgo porque varios de los dispositivos IACS tienen un nivel de riesgo identificado como de alto riesgo.

Tabla A.6 - Ejemplo de tabla de activos IACS con resultados de evaluación y niveles de riesgo

Dispositivo de dispositivo IACS	Consecuencia clasificación	Calificación de probabilidad	Nivel de riesgo del dispositivo IACS
Consola de sala de control del operador	A	Medio	Alto riesgo
Consola de operador remoto	C	Alto	Riesgo medio
Estación de configuración de ingeniería	A	Alto	Alto riesgo
Servidor historiador	B	Medio	Riesgo medio
Controlador	A	Medio	Alto riesgo
Puerta	B	Medio	Riesgo medio
Otros dispositivos	C	Bajo	Riesgo bajo

Comprender este nivel de riesgo inherente básico es clave para llevar a cabo un plan de gestión de riesgos. Establece el nivel de seguridad objetivo necesario para reducir el riesgo. Esto establece la justificación para implementar un plan de gestión y reducción de riesgos, si el IACS aún no está operando a ese nivel objetivo. Se emplearán varias contramedidas de seguridad para reducir el riesgo para el IACS a un nivel tolerable. Sin embargo, el fracaso de estas contramedidas para mitigar el riesgo podría resultar en un incidente con una consecuencia de la magnitud identificada durante la tarea de análisis de riesgo.

A.3.4.2.3.3 Establecer zonas de seguridad y asociar dispositivos IACS a las zonas

El modelo de referencia discutido en IEC / TS 62443 - 1 - 1 identifica varios niveles operativos o de equipo diferentes de un IACS. Aunque puede haber diferentes niveles operativos dentro de un IACS, los requisitos de seguridad cibernética pueden ser similares para varios de estos niveles operativos o de equipo. Es posible incorporar varios niveles operativos / de equipo en una sola zona de seguridad lógica.

El modelo de nivel de seguridad introduce el concepto de emplear zonas asignadas a uno de tres o más niveles de seguridad. Con fines ilustrativos en este ejemplo, suponga que hay tres niveles de seguridad cualitativamente descritos como Bajo, Medio y Alto. La tarea en cuestión es examinar las necesidades de seguridad de los diversos activos del dispositivo IACS y asignarlos a estas diferentes zonas.

La Tabla A.6 enumera el nivel de riesgo de seguridad cibernética de IACS para cada uno de los activos. Los activos con un nivel de alto riesgo comparten la necesidad de un alto nivel de protección cibernética para reducir el riesgo. Estos activos deben asignarse a una zona de seguridad común. Los activos con niveles de riesgo más bajos deben asignarse a una zona de seguridad más baja. En este punto del proceso de gestión de riesgos, es apropiado superponer las zonas de seguridad identificadas en el diagrama de red física del sistema desarrollado para realizar el análisis de riesgos.

Dadas las tecnologías de contramedidas de seguridad actuales, las zonas de seguridad generalmente se alinearán con los segmentos físicos de la red. Es posible que un dispositivo IACS no se encuentre actualmente en el segmento de red adecuado según los resultados del análisis de riesgos para ese dispositivo. Si este es el caso, es posible que sea necesario reubicar el dispositivo en un segmento de red diferente. Un activo con un nivel de bajo riesgo puede asignarse a una zona de seguridad de mayor riesgo, pero los activos con un nivel de alto riesgo no deben ubicarse en una zona de seguridad de menor riesgo.

Hacerlo aumentaría el riesgo de una consecuencia inaceptable en caso de un incidente de seguridad cibernética.

Durante la fase de implementación del modelo de ciclo de vida de nivel de seguridad, los dispositivos con necesidades de seguridad que no coinciden con la zona en la que se ubican físicamente deben reubicarse en los segmentos de red apropiados para cumplir con los requisitos de seguridad.

Una organización puede optar por establecer un enfoque común para las zonas de seguridad en un esfuerzo por mejorar la eficiencia de la gestión de riesgos. Una forma de hacerlo es adoptar una arquitectura de plantilla corporativa que incorpore estrategias de segmentación de red y zonas de seguridad para los diversos tipos de dispositivos y sistemas empleados en la empresa. La Figura A.15 muestra un ejemplo de una arquitectura de plantilla de zona de seguridad para una organización. La Figura A.16 muestra cómo los activos de IACS en el ejemplo se asignan a las zonas en la arquitectura de plantilla que emplea un enfoque de zona de tres niveles.

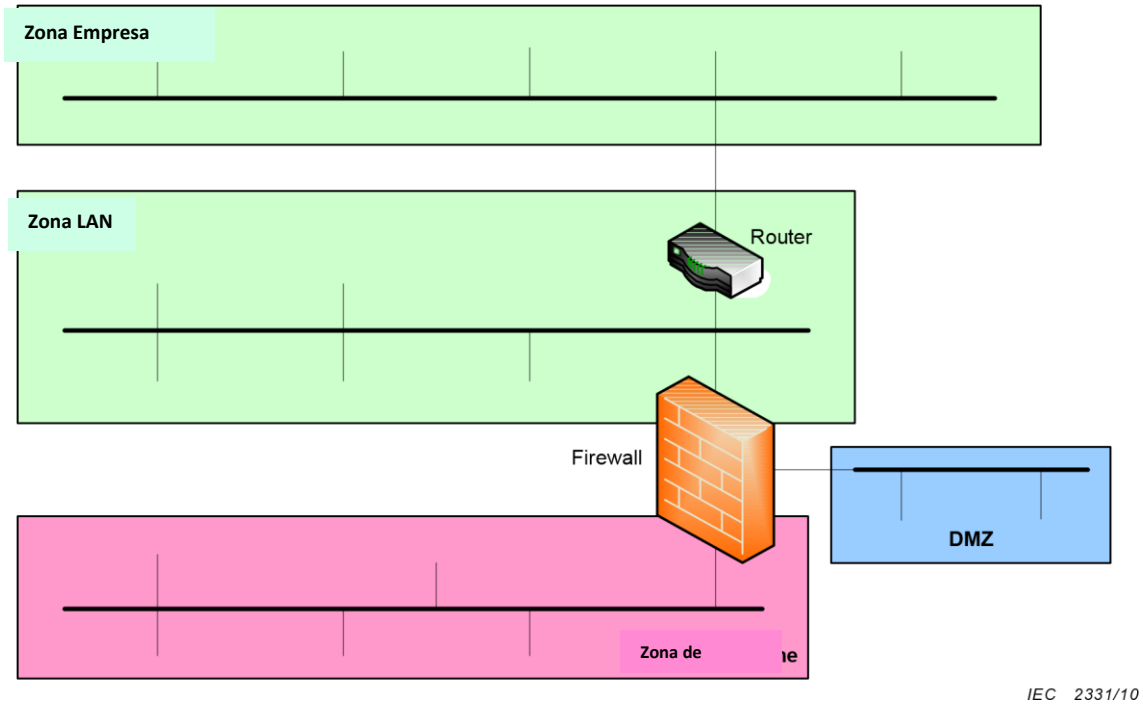

Figura A.15 - Arquitectura de plantilla de zona de seguridad corporativa

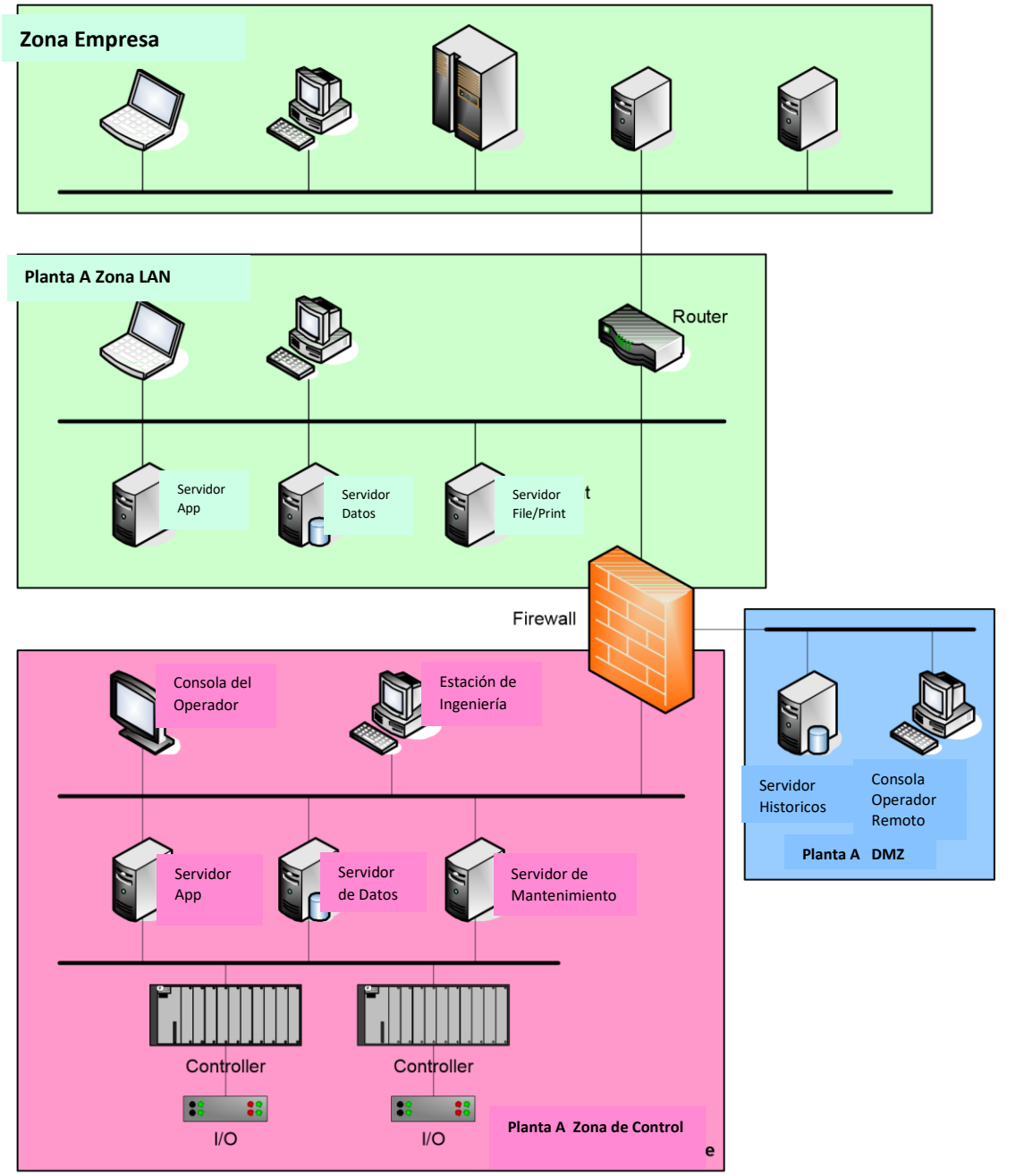

Figura A.16 - Zonas de seguridad para un ejemplo IACS

A.3.4.2.3.4 Determinación del nivel de seguridad objetivo.

El modelo de nivel de seguridad introduce el concepto de asignar un nivel de seguridad a la zona. En el ejemplo que se muestra en la Figura A.16 anterior, se determinó que el nivel de riesgo inherente del IACS era de alto riesgo basado en la evaluación detallada del riesgo de cada dispositivo IACS. Se deben emplear contramedidas de seguridad adicionales para proteger los dispositivos que caen dentro de la zona de control de la Planta A. Utilizando los niveles de seguridad enumerados en IEC / TS 62443 - 1 - 1, Tabla 8, es apropiado asignar un nivel de seguridad objetivo a cada una de las zonas, como se ve en la Tabla A.7.

Tabla A.7 - Niveles de seguridad objetivo para un IACS de ejemplo

Zona	Nivel de seguridad objetivo = SL (objetivo)
Zona de control de la planta A	Alto
Planta A DMZ	Medio
Planta una zona LAN	Bajo
Zona empresarial	Bajo

A.3.4.2.3.5 Seleccionar dispositivos y un diseño de sistema basado en SL (capacidad)

Se examinará la capacidad de nivel de seguridad de cada dispositivo para comprender las fortalezas y vulnerabilidades de seguridad que introduce en la zona. Aunque la SL (capacidad) no puede medirse cuantitativamente en este momento, existen algunos medios más cualitativos para evaluar la SL (capacidad) relativa de los dispositivos que comprenden el IACS. Estos elementos de evaluación generalmente se cubren como parte de una evaluación de vulnerabilidad detallada. Por ejemplo:

- Si el dispositivo es un servidor web, ejecuta una herramienta de evaluación para identificar las debilidades de las aplicaciones del servidor web y determinar si las debilidades se pueden remediar.
- Ejecutar una herramienta de evaluación para identificar la cantidad de servicios y puertos necesarios para que la aplicación funcione en el dispositivo.
- Examinar los puertos y servicios necesarios para determinar si los atacantes los han usado históricamente para explotar vulnerabilidades del sistema.
- Examinar el sistema operativo del dispositivo y determinar si todavía se suministran parches de seguridad y actualizaciones para la versión en uso.
- Ejecutar una herramienta de evaluación para someter la aplicación a entradas inusuales para determinar si el dispositivo y la aplicación continuarán funcionando bajo flujos de comunicación anormales.
- Examinar el historial de exploits de las tecnologías subyacentes utilizadas en el dispositivo para determinar la probabilidad de futuros exploits.

La organización debe tener algunos criterios de aceptación para que un dispositivo se use en un nivel de seguridad objetivo en particular basado en los resultados de estas herramientas de evaluación y las debilidades identificadas. Si el SL (capacidad) del dispositivo es simplemente demasiado bajo para alcanzar el SL (objetivo) para la zona, puede ser necesario seleccionar un dispositivo alternativo. Para un IACS existente compuesto por dispositivos de generación anterior, puede ser necesario reemplazar el dispositivo con un dispositivo de generación más nueva con SL (capacidad) mejorada. Un ejemplo de esto podría ser una estación de control de operador basada en PC que se ejecute en Microsoft Windows® NT como su sistema operativo. Los resultados detallados de la evaluación de vulnerabilidad para este dispositivo y aplicación pueden mostrar vulnerabilidades significativas. Las características de seguridad integradas en este sistema operativo anterior son menores que en muchos de los sistemas operativos de última generación. Además, el proveedor ya no suministra parches de seguridad para abordar estas vulnerabilidades. Esto deja al dispositivo en una posición relativamente débil con respecto a su SL (capacidad).

La SL (capacidad) de cada nuevo dispositivo IACS debe examinarse para asegurarse de que sea compatible con la meta SL (objetivo) para la zona. Aunque las mediciones cuantitativas de SL (capacidad) pueden no estar disponibles y / o publicadas, los proveedores pueden proporcionar algunas medidas más cualitativas basadas en evaluaciones que ellos o terceros han realizado utilizando herramientas de seguridad normalizadas y pruebas de campo. Estos resultados detallados de evaluación de vulnerabilidad deben considerarse y usarse en el proceso de decisión para seleccionar dispositivos IACS.

El diseño preliminar que identifica los dispositivos IACS y las asignaciones de zona se transformará en un diseño detallado que identifique todos los segmentos de equipos y redes que se emplearán en los IACS. Este es el momento de reubicar dispositivos cuyas necesidades de riesgo de seguridad no se alinean con el SL (objetivo) de la zona. El resultado de este paso debe ser un diagrama de red detallado que ubique todos los IACS y dispositivos de red que formarán parte del IACS general.

A.3.4.2.4 Desarrollar e implementar las contramedidas seleccionadas para cada zona

A.3.4.2.4.1 General

La fase de desarrollo e implementación del modelo de ciclo de vida de nivel de seguridad aborda los pasos y las tareas para reducir el riesgo. El concepto general de esta fase es emplear contramedidas a un IACS para lograr el nivel de seguridad objetivo para la zona establecida durante la fase de evaluación. La figura A.17 aborda varios puntos de partida diferentes. Se aplica a la implementación de un nuevo IACS, hacer cambios a un IACS existente en forma de nuevos equipos y mejorar la seguridad de los IACS existentes. La Figura A.17 es un marco de referencia para guiar el pensamiento en lugar de un diagrama de flujo detallado o una lista de verificación de los pasos que deben seguirse.

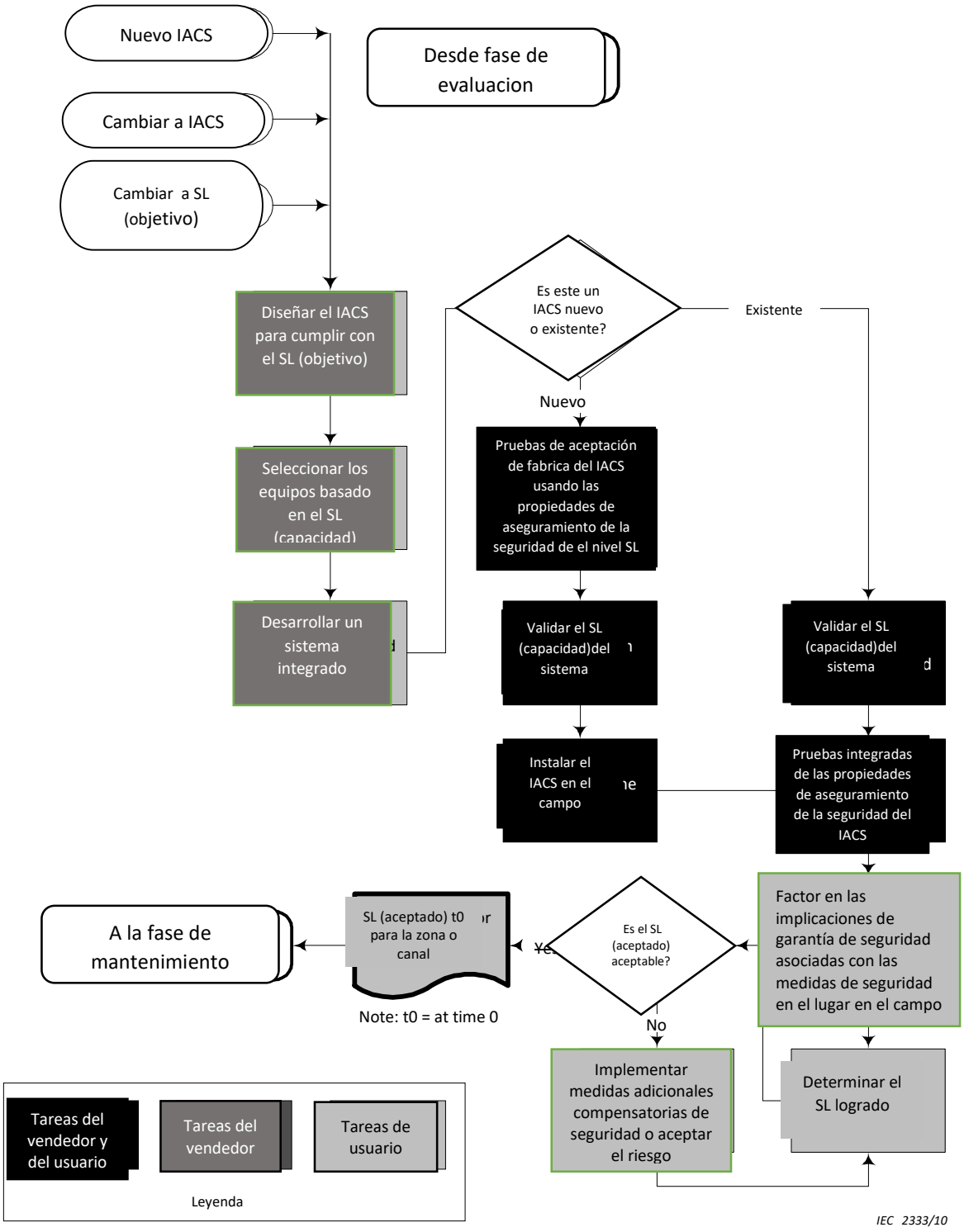
Nuevo IACS
Cambiar a IACS
Cambiar a SL (objetivo)
Desde fase de evaluacion
Diseñar el IACS para cumplir con el SL (objetivo)
Seleccionar los equipos basado en el SL (capacidad)
Desarrollar un sistema integrado
Es este un IACS nuevo o existente?
Existente
Nuevo
Pruebas de aceptación de fabrica del IACS usando las propiedades de aseguramiento de la seguridad de el nivel SL
Validar el SL (capacidad)del sistema
Validar el SL (capacidad)del sistema
Instalar el IACS en el campo
Pruebas integradas de las propiedades de aseguramiento de la seguridad del IACS
Factor en las implicaciones de garantía de seguridad asociadas con las medidas de seguridad en el lugar en el campo
Es el SL (aceptado) aceptable?
No
SL (aceptado) t0 para la zona o canal
Note: t0 = at time 0
A la fase de mantenimiento
Implementar medidas adicionales compensatorias de seguridad o aceptar el riesgo
Determinar el SL logrado
Tareas del vendedor y del usuario
Tareas del vendedor
Tareas de usuario
Leyenda
IEC 2333/10

Figura A.17 - Modelo de ciclo de vida de nivel de seguridad: fase de desarrollo e implementación

El punto de partida de esta fase es el objetivo de seguridad a alcanzar. Esto se expresa como el objetivo de nivel de seguridad para cada zona del IACS. En la fase de evaluación, se establecieron estos objetivos y se realizaron asignaciones de zona preliminares para cada uno de los dispositivos IACS. La tarea en cuestión es adoptar este enfoque preliminar y crear un diseño detallado para su implementación.

A.3.4.2.4.2 Pruebas de seguridad sin conexión

Así como las pruebas funcionales de un IACS son críticas para implementarlo de modo que satisfaga las necesidades de la instalación operativa, las pruebas de seguridad de los dispositivos también son importantes para garantizar que se logre la integridad operacional y la solidez. A.3.4.3 proporciona información más detallada sobre la realización de pruebas de seguridad.

Si el IACS es un sistema nuevo, las pruebas de seguridad deben realizarse mientras el sistema está en un entorno fuera de línea. Esto podría ser una prueba de aceptación de fábrica en la ubicación del proveedor o un paso de preparación fuera de línea en la ubicación de campo final. La ubicación no es tan importante como asegurarse de que se realicen los pasos de prueba de seguridad. Si bien sería muy valioso probar la seguridad de todos los dispositivos y contramedidas empleados en el estado de instalación final, esto puede no ser asequible y práctico. Por lo tanto, el diseño de la prueba debería centrarse más en el SL (capacidad) de los dispositivos IACS y las contramedidas que no son específicas de la ubicación de campo instalada.

La subcláusula anterior señaló varias herramientas y elementos de consideración para probar SL (capacidad). Estos elementos generalmente se cubren como parte de una evaluación detallada de vulnerabilidad. Las pruebas de seguridad deben incluir no solo pruebas para evaluar la capacidad de resistir las amenazas de seguridad típicas encontradas en condiciones operativas, sino que también deben incluir las medidas que formarán parte del soporte continuo de seguridad del sistema. Estos incluyen, pero no se limitan a:

· Probar el proceso para parches y actualizaciones del sistema operativo;

· Probar el proceso de actualización y parcheo para proveedores de IACS;

· Probar el entorno de desarrollo del sistema fuera de línea;

· Prueba de implementación de software antivirus y actualizaciones de firmas de malware.

El objetivo general de las actividades de prueba de seguridad, que se muestran en el centro de la Figura A.17, es validar que el SL (capacidad) de los dispositivos se alinea con la base del diseño.

A.3.4.2.4.3 Pruebas de seguridad de campo

Los elementos que se muestran en el lado derecho de la Figura A.17 anterior identifican las actividades de prueba asociadas con el entorno de destino final. Este es el punto donde todas las contramedidas empleadas se prueban y / o examinan para determinar si el nivel de seguridad alcanzado es igual o superior a la base de diseño de nivel de seguridad objetivo para la zona.

Si se está instalando un IACS nuevo, es probable que sea posible realizar estas pruebas antes de que el IACS se coloque en línea. Si la actividad es actualizar y reemplazar un dispositivo IACS existente o implementar algunas nuevas contramedidas de seguridad para el IACS, es posible que no se pueda obtener

una ventana de oportunidad para realizar pruebas de seguridad de campo fuera de línea completas. En cambio, el desafío a menudo es implementar el nuevo dispositivo o contramedidas y pruebas de campo de que la función operativa básica del IACS no se ha visto inaceptablemente afectada por las medidas de seguridad.

Es importante tener en cuenta que las pruebas de rendimiento del sistema deben incluir la respuesta del sistema a eventos de tipo de operación industrial normales y anormales, así como a eventos de tipo de incidente de seguridad normales y anormales. Estos se combinan para producir una medida general de la robustez e integridad del sistema.

Debido a que cada operación industrial es ligeramente diferente, no es posible identificar un procedimiento de tipo libro de receta para esta prueba. Se requerirá un trabajo de diseño considerable para determinar la mejor manera de garantizar que las funciones de seguridad cumplan con los objetivos de seguridad para alcanzar el Nivel de seguridad objetivo.

A.3.4.2.4.4 Alcanzar el nivel de seguridad objetivo

El logro del nivel de seguridad objetivo en el campo puede requerir cierto grado de iteración. El campo no es un mundo perfecto. Por lo general, es apropiado intentar aplicar un conjunto común de contramedidas a todos los dispositivos dentro de la zona para lograr el nivel de seguridad deseado. Una contramedida seleccionada identificada para la implementación en todos los dispositivos puede no ser utilizable en un dispositivo en particular debido a una restricción operativa o física no reconocida inicialmente durante el diseño de seguridad del sistema. Por lo tanto, es importante reconocer que las situaciones del mundo real pueden requerir la eliminación y la adición de contramedidas para dispositivos individuales dentro de una zona para lograr el equilibrio adecuado de beneficio de seguridad versus riesgo para que todas las partes involucradas en el proceso de decisión estén satisfechas.

A.3.4.2.4.5 Ilustrar el proceso de diseño utilizando el ejemplo IACS

Las subcláusulas anteriores discutieron los principios con respecto a la implementación de contramedidas de seguridad para cumplir con el SL (objetivo) para la zona. Esta subcláusula describe el proceso de diseño de la aplicación de estos principios a un ejemplo del mundo real.

La Tabla A.6 identificó un servidor histórico con un nivel de riesgo Medio. Usando la arquitectura de seguridad de la plantilla corporativa, este dispositivo se identificó como necesario para ubicarse en una zona de seguridad con un SL (objetivo) de nivel medio o superior. La DMZ de la Planta A se identificó como la zona apropiada para este dispositivo a pesar de que el dispositivo se encuentra actualmente en la zona LAN de la Planta A.

En preparación para la implementación física de la DMZ de la Planta A, se examina el SL (capacidad) del servidor histórico para determinar si cumple con el SL (objetivo). El examen de las vulnerabilidades al realizar una evaluación detallada de la vulnerabilidad revela que:

- El sistema operativo para el servidor es Microsoft Windows® NT, para el cual no hay actualizaciones de seguridad disponibles.
- No se está ejecutando ninguna aplicación antivirus en el servidor. El proveedor de la aplicación de historicos no ha calificado ningún producto de software antivirus como compatible con la aplicación historian.

- La mayoría de los usuarios de la aplicación históricos se encuentran en áreas de oficina con conexiones de PC a la zona LAN de Planta A de menor seguridad.
- Los esfuerzos para fortalecer el servidor al cerrar las tareas no necesarias no tuvieron éxito porque el proveedor de la aplicación histórica no certificaría que la aplicación se ejecutaría correctamente si los servicios se cerraran.

La conclusión es que la SL (capacidad) inherente del servidor histórico es inconsistente con la SL (objetivo) para la DMZ de la Planta A.

Dado que el SL (capacidad) inherente es demasiado bajo, se examina el uso de contramedidas suplementarias adicionales para determinar si pueden reducir con éxito el riesgo de cumplir el SL (objetivo). Se examinan contramedidas adicionales como eliminar el acceso a Internet, eliminar el correo electrónico, deshabilitar los puertos de medios en el servidor y emplear contraseñas seguras. Aunque estos pueden contribuir a la reducción de riesgos, se considera que el empleo de estas prácticas de seguridad adicionales no compensaría la baja SL (capacidad) inherente del servidor de históricos.

Dado que el servidor de históricos interactúa directamente con la puerta de enlace IACS de la red de control y regulación, las debilidades de seguridad de este dispositivo también reducen el SL (logrado) de la zona de control de la Planta A. La conclusión es que la mejor manera de abordar estos estados inaceptables de SL (logrados) tanto de la zona de control de la Planta A DMZ como de la Planta A es reemplazar el servidor de historia actual con una nueva aplicación de software de históricos que se ejecuta en un sistema operativo actualmente compatible. Después de examinar el SL (capacidad) del servidor más nuevo y la aplicación de históricos para asegurarse de que se alinea con el SL (objetivo), el servidor y la aplicación se prueban e implementan en la planta A DMZ durante el cierre de una operación industrial.

Hay algunos puntos importantes que vale la pena destacar en asociación con este ejemplo. El SL (logrado) de una zona depende del SL (capacidad) de los dispositivos en la zona, pero también de la conectividad dentro y entre zonas. Un análisis de vulnerabilidad para un dispositivo considera no solo las propiedades inherentes del dispositivo consideradas de forma aislada, sino también la conectividad de este dispositivo en la red. Esto es importante porque un IACS que usa solo dispositivos que tienen alto SL (capacidad) cuando se considera de forma aislada, puede, cuando se considera en conjunto, no necesariamente logra el alto SL (objetivo) deseado para una zona. Por ejemplo, un nuevo dispositivo IACS que emplea un nuevo sistema operativo, incluso si está completamente parcheado y ejecuta un software antivirus, tiene un SL más bajo (logrado) cuando se conecta directamente a la red de TI corporativa. Por el contrario, si uno limita el acceso físico y la conectividad de red a una zona, los dispositivos de menor SL (capacidad) juntos podrían lograr un mayor SL (logrado) para la zona.

La seguridad del conducto entre zonas también puede afectar el SL (logrado) de la zona. Por ejemplo, un conducto que utiliza un enlace de comunicaciones inalámbricas en lugar de un cable físico puede tener un SL diferente (logrado) para el conducto y tener un impacto en el SL (logrado) de las zonas unidas por el conducto.

Del mismo modo, el SL (logrado) de la zona en consideración puede verse afectado por el nivel de seguridad de la zona que se conecta a la zona en consideración. En el ejemplo, los usuarios de la aplicación históricos están en una zona con un nivel de seguridad más bajo que el servidor historian. Incluso si el SL (logrado) del conducto entre estas zonas es Alto, el SL más bajo (logrado) de la zona LAN de la Planta A puede impactar potencialmente negativamente en el SL (logrado) de la DMZ de la Planta A.

A.3.4.2.5 Mantenimiento de los niveles de seguridad para cada zona

A.3.4.2.5.1 General

El nivel de seguridad de un dispositivo se está deteriorando constantemente. Se descubren nuevas vulnerabilidades de seguridad casi todas las semanas. Durante el período de tiempo en que se conocen y no se mitigan las vulnerabilidades, el IACS puede estar en riesgo y el SL (logrado) de la zona es potencialmente más bajo que el SL (objetivo). Esta situación del mundo real se abordará con un plan para mantener el nivel de seguridad de la zona a un nivel de seguridad aceptable.

La fase de Mantenimiento del modelo de ciclo de vida de Seguridad, que se muestra en la Figura A.18 a continuación, muestra el conjunto cíclico de actividades que son críticas para mantener la seguridad de la zona. Los factores desencadenantes para iniciar la reevaluación del riesgo incluyen, entre otros:

- Un cambio en la operación industrial física o cambios en el IACS que podrían introducir nuevos riesgos;
- Una nueva vulnerabilidad descubierta en un módulo de software utilizado en el IACS;
- El lanzamiento de un nuevo sistema operativo o parche de aplicación que desencadena el despliegue de código de explotación en Internet;
- Auditorías y revisiones periódicas de seguridad programadas.

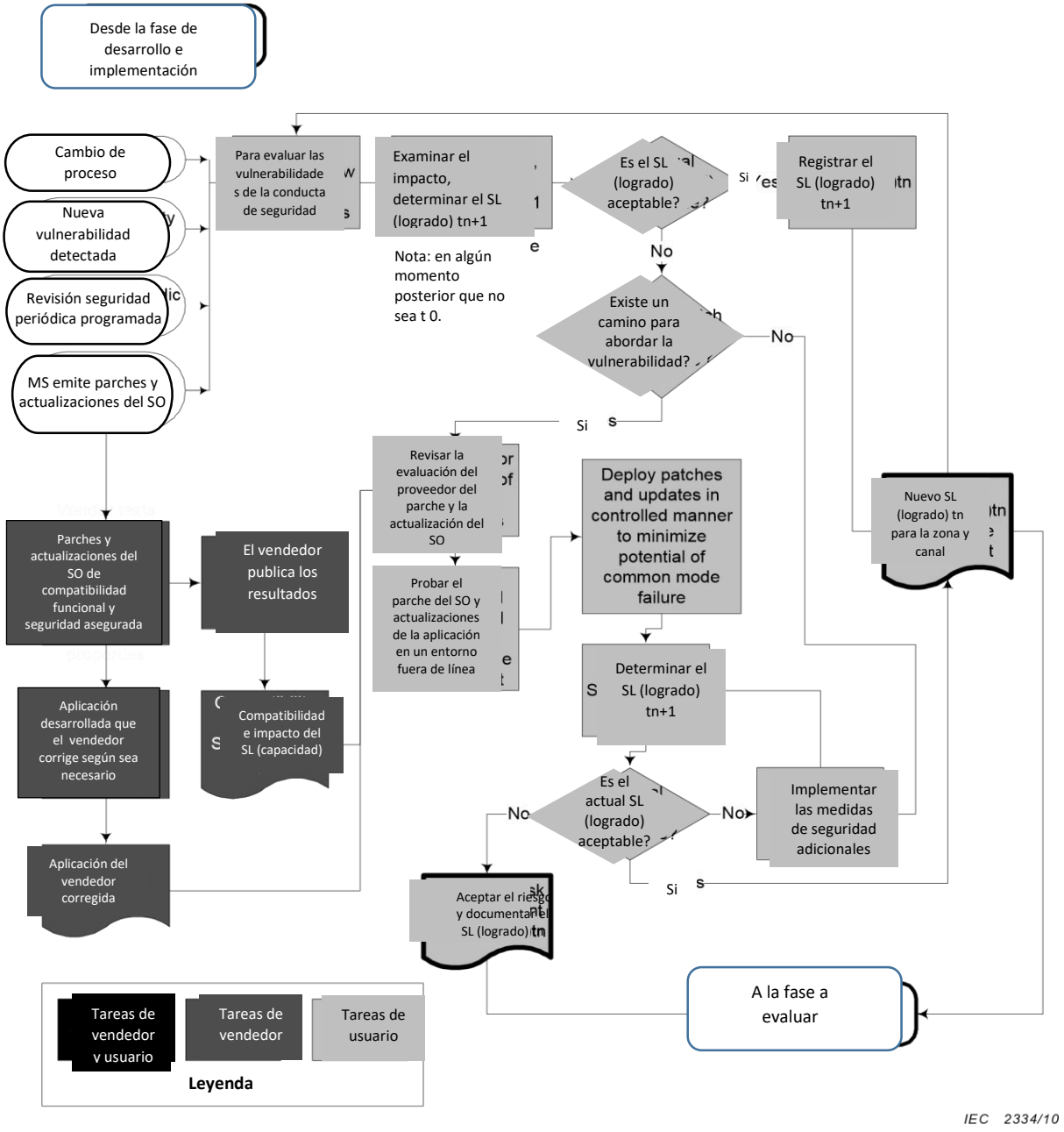

Figura A.18 - Modelo de ciclo de vida de nivel de seguridad: fase de mantenimiento

A.3.4.2.5.2 Parchear dispositivos IACS

La Figura A.18 anterior ofrece una descripción general de alto nivel de cómo encaja el parche en la fase de mantenimiento del modelo de ciclo de vida de nivel de seguridad. Esta subcláusula no pretende ser una discusión exhaustiva de todos los aspectos asociados con la aplicación de parches. El objetivo es representar el aspecto iterativo de examinar el estado SL (logrado) de la zona y la necesidad de tomar decisiones sólidas sobre qué parches aplicar y cuándo aplicarlos.

Los proveedores de dispositivos y aplicaciones IACS comparten la responsabilidad con los usuarios de abordar los riesgos de seguridad. Los usuarios cuentan con los proveedores para comprender el funcionamiento interno de sus aplicaciones IACS, para determinar la aplicabilidad del parche y para realizar pruebas de regresión automatizadas exhaustivas para la compatibilidad de la aplicación IACS con parches del sistema operativo y actualizaciones de revisión importantes. Dado que la instalación de parches tiene el potencial de interferir con el funcionamiento normal de la aplicación de software IACS, los usuarios necesitan tanta seguridad como sea posible de que la instalación del software revisado no resultará en una falla del dispositivo de control.

Como lo indica la Figura A.18, las pruebas de compatibilidad del proveedor son el primer paso en un plan de pruebas multifase antes de realizar parches generalizados en el IACS en ejecución. Se deben realizar pruebas adicionales con el entorno de destino del dispositivo. Idealmente, esto se realizaría en un dispositivo fuera de línea idéntico al IACS en línea. Si esto no es posible, se deben considerar enfoques alternativos que podrían incluir pruebas en un entorno virtual o en una implementación muy controlada en el IACS en línea.

Armado con información de vulnerabilidad del proveedor del sistema operativo, información de aplicabilidad del parche del proveedor de IACS, información de compatibilidad del proveedor de IACS, conocimiento del uso del dispositivo IACS y, finalmente, las pruebas del usuario, el usuario tomará una decisión sobre el despliegue de campo del parche.

A.3.4.2.5.3 Empleo de contramedidas adicionales

Puede ser necesario emplear contramedidas adicionales para abordar vulnerabilidades no mitigadas de parches o vulnerabilidades introducidas por cambios en la operación industrial. Esto se determina evaluando el SL (logrado) y comparándolo con el SL (objetivo) para la zona. Como se señaló anteriormente, esto es bastante subjetivo en lugar de medirse fácilmente en buenos términos cuantitativos.

En algunos casos, el riesgo comercial de tomar medidas para elevar el SL (logrado) puede ser un costo prohibitivo a corto o largo plazo. En este caso, los encargados de tomar decisiones técnicas deben documentar:

- Los riesgos;
- Las contramedidas empleadas;
- Las contramedidas consideradas, rechazadas y los motivos;
- La recomendación a los líderes empresariales de aceptar el riesgo por un período de tiempo hasta que se pueda identificar, probar e implementar una solución de contramedida o seguridad más aceptable.

Los líderes empresariales deben firmar formalmente para documentar la aceptación de esta estrategia.

A.3.4.2.5.4 Revisiones de seguridad programadas

Un CSMS completo incluye un elemento de conformidad que debe incluir una evaluación periódica de que las prácticas de seguridad y las contramedidas identificadas en la política y normas de seguridad corporativa se están empleando y son efectivas para reducir el riesgo de alcanzar el nivel SL (objetivo). Este es otro desencadenante de la fase de mantenimiento del modelo de ciclo de vida de nivel de seguridad.

Una auditoría de seguridad puede medir el grado de conformidad con las políticas y normas definidas y generar métricas que son valiosas para mantener la seguridad. Sin embargo, además de verificar la alineación con las prácticas requeridas, una organización debe evaluar periódicamente (y basándose en los desencadenantes como se muestra en la Figura A.18), evaluar si el SL (logrado) cumple o excede el SL (objetivo) en sus zonas IACS.

A.3.4.2.6 Prácticas de apoyo.

A.3.4.2.6.1 Prácticas de referencia

Las siguientes ocho acciones son prácticas básicas:

a) Definición y validación de políticas de seguridad. Las declaraciones detalladas de la política de seguridad definen el compromiso a nivel operativo para mitigar cada uno de los riesgos de seguridad durante la evaluación de riesgos.

b) Desarrollar procedimientos que brinden detalles, como acciones a tomar para prevenir, detectar y responder a las amenazas.

c) Adaptar normas de organizaciones internacionales en el área de seguridad cibernética para su uso en el entorno IACS de la organización.

d) Servicios de desarrollo como imágenes seguras del sistema operativo y aplicaciones comunes para el uso seguro de IACS.

e) Identificar herramientas y productos de seguridad para implementar partes de la política de seguridad. Si bien las herramientas y productos de seguridad, como los firewalls y las VPN, se pueden usar en los entornos de TI e IACS, los conjuntos de reglas y la aplicación de este tipo de herramientas y productos pueden ser significativamente diferentes debido a los diferentes riesgos asociados con los entornos.

f) Establecer una metodología formal para aceptar el riesgo, incluida la aprobación apropiada del nivel de gestión basada en el alcance y la documentación.

g) Implementar políticas, procedimientos, herramientas y similares de una manera que minimice la sobrecarga administrativa y la carga para el usuario final sin comprometer la efectividad. Los controles bien diseñados a menudo dejan atrás su propio rastro de auditoría que puede usarse para la verificación posterior.

h) Documentar las razones para seleccionar o no ciertas contramedidas de seguridad y los riesgos que abordan en una Declaración de Aplicabilidad (SoA). La buena documentación sobre los controles de mitigación de seguridad ayuda en el proceso de toma de decisiones, facilita la comunicación de las decisiones, proporciona una base para capacitar a las personas para responder a incidentes y amenazas y proporciona una base para autoevaluaciones o auditorías de la conformidad con las contramedidas.

A.3.4.2.6.2 Prácticas adicionales

NOTA 1 IEC / TR 62443 - 3 - 1 [6] e IEC 62443 - 3 - 3 [8] abordarán las prácticas relacionadas cuando se completen.

NOTA 2 Los autores de esta norma se dan cuenta de que hay muchos tipos diferentes de contramedidas disponibles. También se dan cuenta de que incluir una lista de diferentes tipos de contramedidas aquí proporcionaría al lector demasiada información para digerir o no proporcionaría suficientes detalles para que el lector aplique con precisión los controles a IACS. Por lo tanto, los autores han optado por diferir la discusión de prácticas de seguridad de IACS adicionales relacionadas con las contramedidas a otros documentos, lo

que puede proporcionar al lector una visión mucho más profunda de los diferentes tipos de contramedidas disponibles y cómo aplicarlas correctamente al IACS ambiente.

A.3.4.2.7 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [23], [24], [27], [28], [29], [30], [31] [33]

A.3.4.3 Elemento: Desarrollo y mantenimiento del sistema.

A.3.4.3.1 Descripción del elemento

Este elemento aborda los métodos de apoyo necesarios para desarrollar y mantener los sistemas de tecnología de la información de IACS que impactan y son impactados por el CSMS. Analiza los aspectos de seguridad cibernética de: documentación de requisitos, diseño, adquisición, pruebas, gestión de cambios, gestión de parches y procesos de copia de seguridad y recuperación.

El punto clave de este elemento es dar una idea de cómo implementar estos métodos de una manera consciente de la seguridad cibernética. El objetivo del enfoque no es reproducir documentación que describa los fundamentos de estos métodos, sino explicar cómo los problemas de seguridad son inherentes al desarrollo del sistema y los procesos de mantenimiento. Los problemas de seguridad se abordarán a lo largo del curso normal de todos los procesos de Desarrollo y mantenimiento del sistema.

A.3.4.3.2 Documentación de requisitos

A.3.4.2 introduce el concepto de un nivel de seguridad objetivo. El término "requisitos" se refiere a las capacidades y / o características de un sistema o dispositivo dado. Los requisitos pueden referirse a muchas características en muchos contextos: sistemas o software, producto u operación industrial, requisitos funcionales o no funcionales. Sin embargo, para el propósito de este elemento, los "requisitos del sistema" se definen como los atributos del nivel de seguridad objetivo y los "requisitos del dispositivo" se definen como las características de contramedida necesarias para que los dispositivos dentro de la zona alcancen el nivel de seguridad objetivo deseado. Debido a que los requisitos del sistema definen el nivel de seguridad objetivo, se determinarán en la fase de implementación y gestión de riesgos. Estos requisitos del sistema a menudo se denominan requisitos de alto nivel. Los requisitos del dispositivo pueden cambiar según los resultados de la fase de diseño.

Por ejemplo, un requisito del sistema para la zona de control podría ser limitar todo el tráfico de red al control auténtico y al tráfico de automatización. Un requisito del dispositivo para una consola de operador de control podría ser desactivar todos los protocolos de redes y comunicaciones no utilizados. En este caso, ese requisito de dispositivo podría alcanzar solo parcialmente el requisito de nivel de sistema. Puede ser necesario tener múltiples requisitos de dispositivo para cumplir con los requisitos del sistema.

El conjunto detallado y verificable de requisitos del sistema y del dispositivo es la base de los métodos de prueba y de los procesos de diseño de verificación y validación, adquisición, gestión de cambios y gestión de parches. Es extremadamente difícil saber si el diseño, las adquisiciones, los cambios en el sistema o los parches violan el Nivel de seguridad objetivo si las capacidades específicas necesarias para alcanzar ese nivel no están definidas.

A.3.4.3.3 Diseño

La seguridad cibernética debe integrarse en el IACS durante el proceso de diseño. Este objetivo debe considerarse durante la adquisición y el desarrollo del sistema, así como durante el mantenimiento del sistema. Existen numerosos documentos que discuten los procesos de diseño de sistemas. Esta norma no intenta cubrir este tema. Pero vale la pena enfatizar que un aspecto crítico del proceso de diseño es que las contramedidas específicas deben asignarse a cada uno de los requisitos del sistema para verificar que los dispositivos y el sistema en su conjunto satisfagan el nivel de seguridad objetivo.

El proceso de diseño no solo cubre la preparación de la especificación del proyecto, sino que también planifica el enfoque de verificación y la verificación inicial de que el proyecto cumple con los requisitos establecidos. La verificación inicial puede realizarse a través de un análisis en papel. La verificación final se realiza mediante la prueba del sistema.

Es importante darse cuenta de que continuamente se inician y ejecutan nuevos proyectos. Para evitar la posibilidad de retrabajo cuando estos proyectos se instalan y se ponen en línea, los grupos de operaciones e ingeniería responsables de la ejecución de los proyectos deben conocer las normas de seguridad cibernética específicos de la industria y las políticas y procedimientos corporativos de seguridad cibernética.

A.3.4.3.4 Adquisiciones

El proceso de adquisición es particularmente importante para alcanzar el nivel de seguridad objetivo deseado. Al especificar equipos nuevos o actualizados a un proveedor, es importante incluir requisitos de seguridad cibernética. Si hay requisitos específicos del dispositivo que se requieren para cumplir con los requisitos del sistema, entonces estos deben declararse explícitamente en el proceso de adquisición de esos dispositivos. También puede ser necesario especificar cualquier requisito de dispositivo para cosas que el vendedor o integrador no debe hacer. Hay algunas prácticas que son comunes para los vendedores o integradores de dispositivos que pueden hacer en sus dispositivos que pueden conducir a agujeros de seguridad innecesarios que evitarían que el sistema alcance el nivel de seguridad objetivo. Por ejemplo, los proveedores históricamente colocaron puertas traseras en sus productos para facilitar la resolución de problemas y mejorar los tiempos de respuesta del servicio al cliente. Estas puertas traseras son una vulnerabilidad que un atacante podría aprovechar. Es posible que un representante de ventas ni siquiera esté al tanto de estas puertas traseras y que dichos puntos de solución de problemas no deberían permitirse a menos que estén explícitamente incluidos en los requisitos de adquisición.

El tema del lenguaje de adquisición para la seguridad cibernética es demasiado amplio para esta norma. Otros grupos han estado desarrollando este lenguaje y pueden proporcionar más información (por ejemplo, ver [58]).

A.3.4.3.5 Pruebas

A.3.4.3.5.1 General

El propósito de un programa de prueba es asegurar que el sistema cumpla con los requisitos establecidos para el proyecto. Para un sistema bien diseñado, debe cumplir con los requisitos operativos y de seguridad. Una de las decisiones anteriores que se deben tomar al desarrollar un programa de prueba es qué nivel de seguridad requiere la organización de sus proveedores e integradores sobre la seguridad cibernética de los dispositivos o sistemas. El nivel de garantía requerido para un dispositivo o sistema en particular determinará el tipo de prueba requerida. Un proveedor puede tener una estrategia de prueba recomendada para un

dispositivo o sistema en particular, pero el usuario deberá determinar si esa estrategia de prueba es suficiente para validar sus requisitos de seguridad.

Idealmente, se probaría un sistema en todos los estados posibles para garantizar que se cumplan todas las contingencias de seguridad o al menos para que se conozca el riesgo residual. Si bien la prueba completa del sistema es teóricamente posible, no se puede obtener para la mayoría de las especificaciones dadas las limitaciones financieras y de personal. Por lo tanto, el desafío es determinar un nivel aceptable de riesgo y luego realizar un nivel suficiente de prueba acorde con el riesgo aceptable.

Después de la planificación inicial de la prueba, se deben preparar planes y procedimientos de prueba escritos para cada etapa de prueba. Estos deben definir las pruebas a realizar y los resultados esperados. Deben incluir la configuración del sistema, entradas y salidas del sistema y bandas de error tolerables. Durante las pruebas, es importante al menos hacer una verificación rápida de los resultados para verificar que sean los esperados o determinar si es necesario tomar medidas correctivas. Después de completar cada etapa de la prueba, se deben evaluar los resultados. Después de la prueba de validación del sistema, se debe preparar un informe final que revise los resultados de todas las pruebas y resuma las conclusiones.

A.3.4.3.5.2 Tipos de pruebas

Las pruebas de seguridad cibernética, como otras pruebas en otros dominios, incluyen pruebas de verificación y validación. Según el Modelo de Madurez de Capacidades [39]: *“La verificación confirma que los productos de trabajo reflejan adecuadamente los requisitos especificados para ellos. En otras palabras, la verificación asegura que "lo construiste bien". La validación confirma que el producto, según lo previsto, cumplirá su uso previsto. En otras palabras, la validación asegura que "usted construyó lo correcto".* Para resumir esto, la verificación determina si la implementación satisface la especificación, mientras que la validación determina si la especificación satisface el requisito.

La prueba específica realizada dependerá del nivel de prueba requerido, el componente o sistema que se está probando y el tipo de prueba requerida para el sistema o componente. Las pruebas de seguridad cibernética generalmente se realizan en tres etapas: pruebas de componentes, pruebas de integración y pruebas del sistema. Las pruebas de verificación se implementarán durante las etapas de componentes e integración, aunque las pruebas de validación también pueden ser útiles. Las pruebas de verificación y validación se implementarán en la etapa de prueba del sistema.

A.3.4.3.5.3 Prueba de componentes

Las pruebas de componentes deben ser realizadas por el proveedor y verificadas por el propietario del sistema. El componente puede ser software, hardware, firmware o cualquier combinación de estos. El componente debe ser probado para verificar que cumple con los requisitos operativos y de seguridad específicos. La prueba de componentes es normalmente una prueba de banco de trabajo y es necesaria para garantizar que, cuando los componentes se combinen en un sistema, exista la confianza de que cada componente individual se desempeña según lo previsto.

A.3.4.3.5.4 Pruebas de integración

Las pruebas de integración deben ser realizadas por el integrador y verificadas por el propietario del sistema. Dichas pruebas implican pruebas operativas y de seguridad de los diversos componentes, quizás de diferentes proveedores, que están conectados entre sí en un banco de trabajo o en un banco de pruebas

auxiliar en un esfuerzo por ver si todos los componentes funcionarán juntos correctamente antes de colocarlos en el entorno IACS. Las pruebas de integración pueden implicar el uso de herramientas de prueba adicionales, como herramientas de administración y administración de red, que no fueron necesarias durante la fase de prueba de componentes.

Raramente un banco de pruebas tendrá la configuración exacta del sistema de control que existe en la instalación operativa. A menudo, un sistema simplificado o replicado en una configuración de desarrollo o laboratorio es el más adecuado para las fases de prueba de componentes e integración. Las pruebas de integración deben diseñarse en torno a esta instalación de banco de pruebas. Se debe tener cuidado al notar las diferencias entre la configuración de la prueba de integración y el entorno IACS, así como cualquier herramienta adicional necesaria para que los elementos que no se pudieron probar completamente durante la prueba de integración se prueben durante la prueba del sistema. Por esta razón, puede ser útil, especialmente durante la fase de prueba de integración, ubicar el sistema simplificado o de réplica cerca del sitio de un sistema operativo.

En algunos casos, es posible realizar una prueba de integración sin producción para ver cómo las contramedidas de seguridad funcionarán juntas y cómo interactuarán con las características operativas. Por ejemplo, las contramedidas de seguridad que consisten en hardware / software discreto pueden conectarse a través de una red de banco de pruebas de laboratorio. En otros casos, esta integración puede no ser posible. El plan de prueba de integración debe aprovechar cualquier esquema de banco de pruebas que pueda configurarse para probar combinaciones de condiciones operativas que pueden estar presentes en el sistema operativo.

A.3.4.3.5.5 Prueba del sistema

Las pruebas del sistema deben ser verificadas y validadas por el propietario. El objetivo de las pruebas de validación es demostrar mediante técnicas apropiadas, procedimientos y refinamientos de procedimientos (según sea necesario) que las contramedidas administrativas, operativas y técnicas para el IACS se implementan correctamente, son efectivas en su aplicación y aseguran que las nuevas contramedidas de seguridad, según lo adquirido e instalado, cumpla con los requisitos.

Las pruebas del sistema pueden incluir pruebas de penetración del sistema para garantizar que los componentes de seguridad sean capaces de proteger el sistema de diversas amenazas según sea necesario para satisfacer el nivel de seguridad de cada zona. La prueba de penetración es cuando una persona conocida intenta penetrar las defensas de seguridad en un sistema, buscando debilidades y vulnerabilidades que puedan explotarse para obtener acceso o control sobre ese sistema. Muchas empresas se especializan en pruebas de penetración para sistemas de TI tradicionales. Puede ser más difícil encontrar un grupo que comprenda los requisitos especiales de IACS.

Una variedad de herramientas de prueba, como scripts de prueba, bases de datos de variables, configuraciones de línea de base con un estado de inicio asumido, métricas y herramientas de calibración están disponibles para ayudar con la prueba real. También hay disponibles herramientas comerciales y gratuitas que están preconfiguradas para realizar rutinas de diagnóstico y simular puertas de enlace y dispositivos conectados.

Si se realizan pruebas de penetración, debe observarse el rendimiento del sistema durante las pruebas además de los resultados de las pruebas de penetración. Lo más probable es que haya una degradación del

rendimiento en el sistema o los componentes debido a las pruebas de penetración. Estas degradaciones de rendimiento deben tenerse en cuenta para su uso futuro.

Es importante enfatizar que las contramedidas de seguridad también pueden involucrar a personas que operan a través de políticas y procedimientos, así como verificaciones manuales de seguridad. Una contramedida, por ejemplo, puede consistir en un ingeniero de control que instale un parche de seguridad emitido para hardware o software. El plan de prueba podría pasar por la secuencia de una ejecución en seco de la instalación del parche, señalando otros factores que influye.

A.3.4.3.5.6 Separación de entornos de desarrollo y prueba.

Las actividades de desarrollo y prueba pueden causar serios problemas, como modificaciones no deseadas de archivos o entorno del sistema o incluso fallas del sistema. Es importante realizar pruebas de seguridad cibernética en sistemas que no están operativos, reduciendo así el riesgo de cambio accidental o acceso no autorizado al software operativo y a los datos comerciales a través de un acceso inapropiado del desarrollador. Si el personal de desarrollo y prueba tiene acceso al sistema operativo y su información, pueden introducir código no autorizado y no probado o alterar los datos operativos. Los desarrolladores y evaluadores también representan una amenaza para la confidencialidad de la información operativa. Las actividades de desarrollo y prueba pueden causar cambios no deseados en el software y la información si comparten el mismo entorno informático.

El método preferido para eliminar estos problemas es utilizar un sistema que esté separado del sistema operativo para realizar el desarrollo y las pruebas iniciales. Si esto no es posible, se debe tener cuidado para garantizar que el sistema utilice un sistema de gestión de cambios adecuadamente definido para documentar cualquier cambio que se realice en el sistema y proporcionar la capacidad de deshacer esos cambios.

A.3.4.3.6 Gestión del cambio

Los sistemas de gestión de cambios para SIS se utilizan en algunas industrias según los requisitos reglamentarios. Para un CSMS completo, los sistemas de gestión de cambios deben usarse para todos los IACS. El proceso de gestión del cambio debe seguir los principios de separación de deberes para evitar conflictos de intereses. Esto significa que el mismo individuo no puede aprobar un cambio e implementarlo. Una persona con conocimientos técnicos debe revisar los cambios propuestos a IACS por su impacto potencial en los riesgos de HSE y los riesgos de seguridad cibernética basados en políticas claramente definidas. Si el cambio viola una de las políticas, entonces el cambio propuesto puede necesitar ser revisado por otro personal capacitado para verificar que sea válido o desaprobar el cambio.

Para que la gestión del cambio sea efectiva, debe haber un registro detallado de lo que está instalado y esto debe formar la base para las propuestas de cambio. El sistema de gestión de cambios estará respaldado por un procedimiento documentado y comprobado de respaldo y restauración. Es fundamental que todas las actualizaciones del sistema, parches y cambios de política se implementen de acuerdo con los procedimientos del sistema de gestión de cambios.

A.3.4.3.7 Gestión de parches

La instalación de parches, actualizaciones y cambios de políticas, que parecen inocuos de forma aislada, pueden tener serias ramificaciones de seguridad cibernética. No instalarlos también puede presentar serios peligros. Se desarrollará un método para determinar la relevancia y la importancia crítica de las

vulnerabilidades que los nuevos parches están destinados a mitigar. Dicho método determinará el impacto en la capacidad de mantener el Nivel de seguridad objetivo si se aplica el parche *y* si no se aplica.

NOTA IEC / TR 62443 - 2 - 3 [5] es un informe técnico planificado sobre la gestión de parches.

A.3.4.3.8 Copia de seguridad y recuperación

Se debe tener especial cuidado para verificar que los procesos de copia de seguridad y recuperación sean compatibles con el Nivel de seguridad objetivo para el sistema. En general, el proceso de copia de seguridad y recuperación debe garantizar que las copias de seguridad estén protegidas en la misma medida que los originales. Esto puede requerir procedimientos especiales para verificar que las copias de seguridad no se hayan dañado y que los mecanismos que marcan una copia de seguridad o restauración exitosa no se hayan visto comprometidos. La estabilidad de las copias de seguridad debe verificarse regularmente para asegurarse de que los medios que contienen los archivos no se hayan degradado y que los datos contenidos en los medios aún puedan leerse y utilizarse. Puede ser necesario mantener el equipo heredado en casos en que los equipos más nuevos no puedan leer las copias de seguridad más antiguas.

A.3.4.3.9 Prácticas de apoyo

A.3.4.3.9.1 Prácticas de referencia

Las siguientes seis acciones son prácticas básicas:

a) Documentar los requisitos de seguridad (amenazas / contramedidas / planes de prueba).

b) Mapear las contramedidas de seguridad a los requisitos de seguridad.

c) Definir el comportamiento esperado de respuesta a fallas.

d) Definir, desarrollar y probar la funcionalidad del componente para que todo el sistema cumpla con el nivel de seguridad objetivo.

e) Verificar y validar la seguridad cibernética durante las pruebas de componentes, integración y sistemas.

f) Incluyendo un rastro de autorización, un sistema de respaldo y restauración, un sistema de administración de parches y un procedimiento de antivirus / malware en el sistema de administración de cambios.

A.3.4.3.9.2 Prácticas adicionales

Las siguientes cinco acciones son prácticas adicionales:

a) Implementación de entornos de desarrollo, prueba y operativos separados.

b) Emplear procedimientos independientes de verificación y validación de componentes.

c) Emplear procedimientos independientes de verificación y validación de integración.

d) Emplear procedimientos independientes de verificación y validación del sistema.

e) Integrar los procedimientos de gestión de cambios IACS con los procedimientos PSM existentes.

A.3.4.3.10 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [23], [38], [39].

A.3.4.4 Elemento: Gestión de información y documentos.

A.3.4.4.1 Descripción del elemento.

La gestión de información y documentos es el proceso para clasificar todos los datos, salvaguardar la información, gestionar los documentos y poner a disposición de manera apropiada la información asociada con el IACS y el CSMS. La gestión de documentos IACS puede incluirse en el sistema de gestión de documentos y retención de registros generales de la organización. La gestión de la información y los documentos garantiza que los datos estén disponibles durante el tiempo requerido en función de los requisitos internos (por ejemplo, políticas de la organización y mantenimiento del dispositivo) o externos (por ejemplo, legales, reglamentarios y políticos).

A.3.4.4.2 Consideraciones para la gestión de información y documentos.

La información asociada con el CSMS de una organización es importante, a menudo sensible y debe controlarse y gestionarse adecuadamente. Por lo tanto, las organizaciones deberían emplear políticas integrales de gestión de documentos e información para su CSMS. La información asociada con el desarrollo y la ejecución de un CSMS, análisis de riesgos, estudios de impacto empresarial, perfiles de tolerancia al riesgo y similares pueden ser sensibles a la organización y pueden necesitar protección, al igual que las contramedidas, la filosofía y las estrategias de implementación. Además, las condiciones comerciales cambian y requieren análisis y estudios actualizados. Se debe tener cuidado para proteger esta información y verificar que se conserven las versiones apropiadas. Inherente a esto, hay un sistema de clasificación de información que permite que los activos de información reciban el nivel apropiado de protección.

Uno de los primeros pasos para crear un sistema de gestión de información y documentos IACS es definir los niveles de clasificación de la información. La información (por ejemplo, confidencial, restringida y pública) debe definirse para gestionar el acceso y el control de los activos de información. Los niveles y las prácticas asociadas deben abordar el intercambio, la copia, la transmisión y la distribución de los activos de información apropiados para el nivel de protección requerido.

Una vez definidos los niveles básicos, la información asociada con el IACS (por ejemplo, información de diseño del sistema de control, evaluaciones de vulnerabilidad, diagramas de red y programas de control de operaciones industriales) debe clasificarse para indicar el nivel de protección requerido. Este nivel de protección debe determinarse en función de la sensibilidad de la información y las posibles consecuencias si la información fue divulgada. El nivel de clasificación debe indicar la necesidad y la prioridad de la información, así como la sensibilidad de la información. Las políticas y los procedimientos para el acceso a la información o los documentos deben estar vinculados a los procedimientos de control de acceso definidos en A.3.3.5, A.3.3.6 y A.3.3.7.

Se debe desarrollar y mantener un proceso de gestión de documentos del ciclo de vida para este propósito. Este proceso debe confirmar la seguridad, disponibilidad y usabilidad de la configuración del sistema de control. Esto incluye la lógica utilizada en el desarrollo de la configuración o programación para la vida de IACS. Este proceso también debe incluir un mecanismo para actualizaciones cuando se producen cambios.

Deben desarrollarse políticas y procedimientos que detallen la retención, protección, destrucción y eliminación de información de la compañía, incluidos registros escritos y electrónicos, equipos y otros medios que contengan información, teniendo en cuenta los requisitos legales o reglamentarios. Las políticas y procedimientos desarrollados para el sistema de gestión de documentos e información de IACS deben ser coherentes y alimentar cualquier sistema de gestión de documentos e información corporativa. Se deben realizar revisiones legales de las políticas de retención para garantizar el cumplimiento de las leyes o regulaciones. Deben identificarse los documentos que requieren retención y debe documentarse un período de retención.

También es necesario asegurarse de que se empleen las medidas adecuadas para garantizar que se puedan recuperar los registros a largo plazo (es decir, convertir los datos a un formato más nuevo, retener equipos más antiguos que puedan leer los datos). Deben desarrollarse métodos y procedimientos para evitar la corrupción de los datos de respaldo. Las copias de respaldo deben hacerse de manera regular. Estas copias de seguridad deben probarse para verificar que todavía sean viables. Los procedimientos de restauración también deben ser revisados y probados regularmente.

Se deben realizar revisiones periódicas de los niveles de clasificación de la información y los documentos. La necesidad de tratar cierta información o documentos con un control o manejo especial debe evaluarse durante estas revisiones. También será necesario desarrollar un método para aumentar o disminuir el nivel de clasificación de una determinada información o documento.

También se debe realizar una revisión periódica del sistema de gestión de información y documentos en su conjunto. Esto garantiza que los propietarios de la información o los documentos se ajusten a las políticas, normas u otros requisitos establecidos por la organización.

A.3.4.4.3 Prácticas de apoyo.

A.3.4.4.3.1 Prácticas de referencia

Las siguientes seis acciones son prácticas básicas:

a) Definir los niveles de clasificación de la información (es decir, confidencial, restringida y pública) para el acceso y el control que incluye compartir, copiar, transmitir y distribuir de manera apropiada para el nivel de protección requerido.

b) Clasificar toda la información (por ejemplo, información de diseño del sistema de control, resultados de evaluación de vulnerabilidad, diagramas de red y programas de control de operaciones industriales) para indicar la necesidad, la prioridad y el nivel de protección requerido de acuerdo con su sensibilidad y consecuencia.

c) Revisar periódicamente la información que requiere un control o manejo especial para validar si aún se requiere un manejo especial.

d) Desarrollar e incluir políticas y procedimientos que detallen la actualización de registros, retención, destrucción y eliminación de información, incluidos registros escritos y electrónicos, equipos y otros medios que contienen información. Cualquier requisito legal o regulatorio debe ser considerado al desarrollar estas políticas y procedimientos.

e) Desarrollar y emplear métodos para evitar la corrupción de datos en torno a los procesos de copia de seguridad y el registro.

f) Confirmar la seguridad, disponibilidad y usabilidad de la configuración del sistema de control. Esto incluye la lógica utilizada en el desarrollo de la configuración o programación para la vida de IACS.

A.3.4.4.3.2 Prácticas adicionales

Las siguientes cuatro acciones son prácticas adicionales:

a) Emplear las medidas apropiadas para garantizar que se pueda recuperar la información de los registros a largo plazo (es decir, convertir los datos a un formato más nuevo o retener equipos más antiguos que puedan leer los datos).

   EJEMPLO Datos de emisiones registrados hace más de una década en un sistema que actualmente no existe o está en un formato propietario.

b) Realizar revisiones periódicas de conformidad con la política de información y gestión de documentos.

c) Realizar revisiones legales de las políticas de retención para garantizar el cumplimiento de las leyes o reglamentos.

d) Cifrar todas las comunicaciones a través de Internet que impliquen información privada con una capa de conexión segura (SSL) o un cifrado de fuerza equivalente.

A.3.4.4.4 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [6], [23], [24], [26].

A.3.4.5 Elemento: planificación y respuesta a incidentes

A.3.4.5.1 Descripción del elemento.

La planificación y respuesta a incidentes aborda la necesidad de estar atentos en los esfuerzos para detectar incidentes de seguridad cibernética e identificar y responder de inmediato a estos incidentes. No importa cuánto cuidado se tome al proteger un sistema, siempre es posible que intrusiones no deseadas puedan comprometer el sistema. Las vulnerabilidades tecnológicas continúan existiendo y las amenazas externas están aumentando en número y sofisticación, lo que requiere una estrategia sólida para determinar la planificación y respuesta adecuadas. La planificación y respuesta a incidentes permite a una organización predefinir cómo detectará y reaccionará ante incidentes de seguridad cibernética. Esto permite que la organización sea proactiva con su programa de seguridad cibernética en lugar de ser reactiva.

La planificación y respuesta a incidentes brinda a la organización la oportunidad de planificar incidentes de seguridad y luego responder de acuerdo con las prácticas establecidas. Los objetivos de la planificación y respuesta a incidentes son muy similares a los de la planificación de continuidad del negocio, pero generalmente se relacionan con incidentes de menor escala y posiblemente en tiempo real. Parte del plan de incidentes debe incluir procedimientos sobre cómo responderá la organización a los incidentes, incluidos los procesos de notificación, los procesos de documentación, la investigación y las prácticas de seguimiento posteriores. Responder a emergencias, garantizar la seguridad del personal y volver a poner en línea los sistemas son parte de la respuesta a incidentes. Identificar un incidente temprano y responder adecuadamente puede limitar el daño / consecuencia del evento.

La planificación y respuesta a incidentes es un elemento clave del sistema de gestión para cualquier tipo de riesgo para una organización, incluidos los riesgos de seguridad cibernética. Las prácticas sólidas de gestión de la información reconocen la necesidad de contar con un sistema formal de planificación y respuesta a incidentes.

Hay tres fases principales que forman parte de la planificación y respuesta a incidentes: planificación, respuesta y recuperación. La fase de planificación incluye el desarrollo inicial del programa del sistema y los esfuerzos específicos de planificación de contingencia. La fase de respuesta implica la capacidad de responder a incidentes reales. La fase de recuperación restaura IACS a sus estados operativos anteriores.

A.3.4.5.2 Fase de planificación

Se debe establecer un programa para reconocer y responder a incidentes dentro del entorno IACS. Este programa debe incluir un plan escrito que documente los tipos de incidentes que se tratarán y la respuesta esperada a cada uno de esos incidentes.

El plan de incidentes debe incluir los tipos de incidentes que pueden ocurrir y la respuesta esperada a esos incidentes. Los diversos tipos de incidentes que puede causar una intrusión del sistema deben identificarse y clasificarse en cuanto a los efectos y la probabilidad, de modo que se pueda formular una respuesta adecuada para cada incidente potencial. Este plan debe incluir acciones paso a paso que las diversas organizaciones deben tomar. Si hay requisitos de informes, estos deben tenerse en cuenta, así como también dónde se debe realizar el informe y los números de teléfono para reducir la confusión de los informes. Durante la preparación del plan de respuesta a incidentes, se deben obtener los aportes de los diversos interesados, incluidas las operaciones, la gestión, la legislación y la seguridad. Estas partes interesadas también deben firmar y aprobar el plan.

El plan de incidentes debe incluir planes de contingencia que cubran la gama completa de consecuencias que pueden ocurrir debido a fallas en el programa de seguridad cibernética de IACS. Estos planes de contingencia deben incluir procedimientos para separar el IACS de todos los conductos no esenciales que pueden proporcionar vectores de ataque, proteger los conductos esenciales de futuros ataques y restaurar el IACS a un estado previamente conocido en caso de un incidente. También deben probarse periódicamente para asegurarse de que continúan cumpliendo sus objetivos.

Otra información importante que debe incluirse en el plan de incidentes es la información de contacto de todo el personal responsable de responder a los incidentes dentro de la organización. Puede ser difícil ubicar esta información en caso de que ocurra un incidente.

Una vez que se completa el plan de incidentes, la organización necesita distribuir copias a todos los grupos de personal apropiados dentro de la organización, así como a cualquier organización externa apropiada. Todo el personal y las organizaciones asociadas deben ser conscientes de sus responsabilidades antes, durante y después de un incidente.

Además de distribuir el plan a todas las organizaciones apropiadas, el plan debe probarse periódicamente para garantizar que sigue siendo relevante. La organización debe realizar simulacros del plan de respuesta a incidentes y analizar los resultados de esos simulacros. Cualquier problema encontrado durante los simulacros debe abordarse y el plan debe actualizarse.

A.3.4.5.3 Fase de respuesta

Hay varias respuestas que se pueden tomar en caso de un incidente de seguridad. Estos van desde no hacer nada hasta tener un apagado completo del sistema. La respuesta particular tomada dependerá del tipo de incidente y su efecto en el sistema. Se debe haber preparado un plan escrito durante la Fase de Planificación que documente claramente los tipos de incidentes que pueden ocurrir y la respuesta esperada a esos incidentes. Esto proporcionará orientación durante los momentos en que puede haber confusión o estrés debido al incidente.

La organización necesita tener procedimientos establecidos para identificar e informar incidentes. Estos procedimientos deben establecer pautas para determinar qué podría constituir un incidente y cómo se deben informar y clasificar los posibles incidentes. Estas pautas deben incluir información sobre cómo reconocer e informar experiencias inusuales que en realidad pueden ser incidentes de seguridad cibernética. Los procedimientos también deben incluir cualquier responsabilidad especial (por ejemplo, métodos de identificación, requisitos de informes y acciones específicas) que el personal debe tener en cuenta cuando se trata de un incidente de seguridad cibernética.

Si se detecta un incidente, los detalles de ese incidente deben documentarse para registrar el incidente en sí, las respuestas tomadas, las lecciones aprendidas y cualquier acción que se tome para modificar el CSMS a la luz de este incidente. Los detalles del incidente deben comunicarse a todos los grupos apropiados dentro de la organización (por ejemplo, gestión, TI, seguridad de procesos, automatización y control de ingeniería y fabricación) y a cualquier organización externa afectada por el incidente. Es importante que estos detalles se comuniquen de manera oportuna para ayudar a la organización a evitar nuevos incidentes.

Dado que cada incidente puede no ser inicialmente reconocido o detectado, la organización debe tener procedimientos establecidos para identificar fallas de seguridad cibernética fallidas y exitosas. Dependiendo de la magnitud del daño infligido por un incidente en particular, es posible que sea necesario consultar a especialistas forenses de seguridad cibernética para determinar la causa raíz del incidente, evaluar la efectividad de la respuesta o respuestas tomadas y, en caso de una pérdida intencional, para preservar la cadena de evidencia para apoyar los esfuerzos para enjuiciar al autor. Si el incidente ocurre en un sistema IACS crítico que resulta en una interrupción de la continuidad del negocio, es probable que el objetivo sea que la instalación vuelva a funcionar lo más rápido posible. Esto puede implicar volver a formatear los discos duros y una recarga completa del sistema operativo y las aplicaciones que probablemente eliminen todos los datos forenses. Establecer prioridades de respuesta a incidentes y prácticas antes de un incidente es importante para que todos comprendan los objetivos y métodos.

A.3.4.5.4 Fase de recuperación

Los resultados del incidente pueden ser menores o pueden causar muchos problemas en el sistema. Las acciones de recuperación paso a paso deben documentarse para que el sistema pueda volver a sus operaciones normales de la manera más rápida y segura posible.

Un componente importante de la fase de recuperación es la restauración de sistemas e información (es decir, datos, programas y recetas) a los estados operativos. Esto requiere un sistema de respaldo y recuperación suficiente capaz de manejar todo el IACS. Puede estar compuesto por uno o varios dispositivos físicos de respaldo y recuperación, pero todos deben trabajar juntos para ayudar en la recuperación del IACS.

La organización debe tener un proceso de análisis de incidentes para abordar los problemas que se descubren y garantizar que se corrijan. Los hallazgos del proceso de análisis deben incorporarse en las políticas y procedimientos de seguridad cibernética apropiados, contramedidas técnicas y planes de

respuesta a incidentes. Los incidentes relacionados con la seguridad cibernética se pueden dividir en tres categorías:

· Código malicioso como virus, gusanos, bots, rootkits y troyanos;

· Pérdida accidental de disponibilidad, integridad o confidencialidad (incluida la disponibilidad de producción);

· Intrusión no autorizada que se extiende a los activos físicos.

Los incidentes en las dos primeras categorías generalmente se administran dentro del proceso de respuesta a incidentes de seguridad de TI. La tercera categoría generalmente se administraría en colaboración con especialistas de HSE y liderazgo del sitio.

A.3.4.5.5 Prácticas de apoyo

A.3.4.5.5.1 Prácticas de referencia

Las siguientes nueve acciones son prácticas básicas:

a) Establecer procedimientos para que la organización general reconozca e informe experiencias inusuales que en realidad pueden ser incidentes de seguridad cibernética.

b) Establecer procedimientos de planificación y respuesta a incidentes que incluyen:

- Nombrar a la persona responsable de ejecutar el plan cuando surja la necesidad;
- Estructurar un equipo de respuesta a incidentes que pueda ser llamado, incluidos los contribuyentes de seguridad de TI y IACS y personal adicional;
- Establecer la responsabilidad de coordinar la defensa y la respuesta a un incidente;
- Manejar el incidente desde el inicio hasta la revisión final;
- Crear procedimientos para identificar, clasificar y priorizar incidentes;
- Crear procedimientos para diferentes tipos de incidentes como ataques DoS, piratería de sistemas, código malicioso, acceso no autorizado y uso inapropiado.

c) Identificar mediciones proactivas para identificar automáticamente los incidentes durante su etapa inicial.

d) Preplanificación de respuestas a escenarios de amenaza identificados a partir de evaluaciones de vulnerabilidad y riesgo.

e) Comunicar los incidentes de IACS a todas las organizaciones apropiadas, incluidas las organizaciones de TI, seguridad de operaciones industriales, ingeniería de automatización y control y organizaciones de operaciones para crear concientización.

f) Comunicar métricas e incidentes a la dirección ejecutiva.

g) Realizar revisiones periódicas de incidentes pasados, para mejorar el CSMS.

h) Documentar los detalles del incidente, las lecciones aprendidas y cualquier acción a tomar para modificar el CSMS a la luz de este incidente.

i) Realización de simulacros para probar el plan. Celebrar reuniones después de los simulacros para identificar áreas de mejora.

A.3.4.5.5.2 Prácticas adicionales

Las siguientes trece acciones son prácticas adicionales:

a) Desarrollar capacidades de investigación forense para sistemas IACS, ya sea interna o externamente.

b) Desarrollar un proceso para informar de inmediato los incidentes de seguridad cibernética. Asegurar que el proceso tenga vínculos con el equipo de gestión de crisis de la organización. Educar al personal con ejemplos de incidentes reportables para que puedan cumplir mejor con los requisitos de informes.

c) Comprender los posibles vínculos entre TI, seguridad e IACS e incorporar esta comprensión en los procedimientos integrados de respuesta a incidentes de seguridad.

d) Desarrollar, probar, desplegar y documentar el proceso de investigación de incidentes.

e) Desarrollar políticas corporativas para informar incidentes de seguridad cibernética y compartir información de incidentes con grupos de toda la industria y agencias gubernamentales donde las políticas corporativas lo permitan.

f) Especificar roles y responsabilidades con respecto a la policía local y / u otras partes interesadas críticas en un programa de investigación de incidentes internos y compartidos.

g) Ampliar la investigación de incidentes con base en el resultado potencial que podría haber ocurrido en lugar del resultado real, reconociendo que el incidente cibernético puede incluir intenciones maliciosas. Es posible que deba actualizarse el nivel de investigación del incidente, dependiendo de la posible gravedad del incidente.

h) Desarrollar metodologías y mecanismos para garantizar que las acciones correctivas identificadas como resultado de un incidente de seguridad cibernética o un simulacro se implementen por completo.

i) Proporcionar capacitación en respuesta a incidentes de seguridad a equipos de capacitación multifuncionales de la organización.

j) Revisar los resultados finales de la investigación del incidente con todo el personal cuyas tareas laborales son relevantes para los hallazgos. Revisar el incidente a la luz de las tendencias y registrarlo para que pueda usarse en análisis de tendencias posteriores.

k) Promover actividades de asistencia mutua entre pares y entre industrias para aprender de las experiencias de otros con respecto a la evaluación, respuesta, investigación, comunicación y corrección de incidentes de seguridad cibernética.

l) Identificar consecuencias imprevistas anteriormente, especialmente aquellas que pueden afectar la aplicación futura del plan. Los incidentes pueden incluir eventos de riesgo, casi accidentes y mal funcionamiento. También se incluye cualquier debilidad observada o sospechada en el sistema o riesgos que pueden no haber sido reconocidos previamente.

m) Incorporar la planificación de respuesta a emergencias en la planificación de respuesta a incidentes.

A.3.4.5.6 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [26], [36].

A.4 Categoría: Monitoreo y mejora del CSMS

A.4.1 Descripción de la categoría.

Un CSMS incluye todas las medidas necesarias para crear y mantener un programa de seguridad cibernética. El alcance y el nivel de este esfuerzo dependen de los objetivos de la organización, la tolerancia al riesgo y la madurez del programa de seguridad cibernética. Este sistema de gestión debe abordar los requisitos,

métodos, dispositivos, interfaces y personal necesarios para implementar el programa de seguridad cibernética.

Monitorear y mejorar el CSMS implica tanto garantizar que el CSMS se esté utilizando como también revisar el propio CSMS para determinar su eficacia. La figura A.19 muestra los dos elementos que forman parte de la categoría:

· Conformidad y

· Revisar, mejorar y mantener el CSMS.

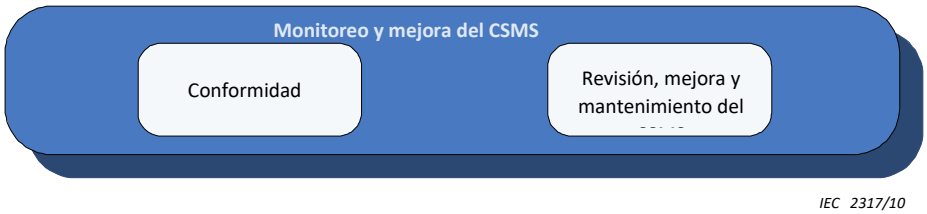

Figura A.19 - Vista gráfica de la categoría: Monitoreo y mejora del CSMS

A.4.2 Elemento: conformidad

A.4.2.1 Descripción del elemento

La conformidad es el proceso de validar que la organización está siguiendo el programa de seguridad cibernética que se desarrolló. El CSMS es tan bueno como la capacidad de una organización para seguirlo. La organización debe ser responsable de las políticas y procedimientos establecidos como parte del CSMS o el sistema de gestión será ineficaz. Al validar su conformidad con el CSMS, la organización puede utilizar los procesos integrados del CSMS para mejorar el sistema en general en el futuro.

Como parte de la validación de conformidad con el CSMS, hay actividades programadas y no programadas. Las revisiones periódicas del CSMS se considerarían programadas, pero la respuesta a un incidente de seguridad cibernética probablemente se consideraría no programada.

El establecimiento de indicadores clave de desempeño (KPI) le dará a la organización una forma de medir el desempeño del CSMS. El uso de KPI que sean consistentes con las mejores soluciones de grupos industriales u otras organizaciones permitirá la evaluación comparativa del CSMS.

A.4.2.2 Actividades programadas versus actividades no programadas

Muchas subcláusulas del CSMS incluyen la idea de revisiones periódicas de algún elemento para monitorear o mejorar el CSMS con el tiempo. Todas estas revisiones son parte del Modelo de Madurez de un programa de seguridad como se discutió en IEC / TS 62443 - 1 - 1. Las revisiones realizadas como parte normalizada de un CSMS evitan que el sistema se degrade con el tiempo debido a nuevas amenazas, vulnerabilidades o situaciones. eso no existía cuando el sistema se desarrolló por primera vez.

También pueden surgir amenazas críticas, vulnerabilidades o situaciones que deben abordarse antes del próximo período de revisión programado. Estas constituirían actividades no programadas y pueden requerir una reevaluación del CSMS para garantizar la efectividad.

Las revisiones y auditorías periódicas del CSMS determinan si las políticas, los procedimientos y las contramedidas deseadas se han implementado correctamente y si están funcionando según lo previsto. En el entorno de IACS, los auditores deben comprender completamente las políticas y procedimientos de seguridad cibernética corporativa y los riesgos específicos de HSE asociados con una instalación particular y / o operación industrial. Se debe tener cuidado para garantizar que las auditorías no interfieran con las funciones de control proporcionadas por el equipo IACS. Puede ser necesario desconectar un sistema antes de poder realizar la auditoría. La auditoría debe verificar que:

· Las políticas, procedimientos y contramedidas presentes durante las pruebas de validación del sistema todavía están instaladas y funcionan correctamente en el sistema operativo; · El sistema operativo está libre de compromisos de seguridad;

NOTA En caso de que ocurra un incidente, se espera que se generen registros y registros, que capturen información sobre la naturaleza y el alcance del incidente.

· Se sigue rigurosamente el programa de gestión del cambio con una pista de auditoría de revisiones y aprobaciones para todos los cambios.

Una actividad no programada particular que puede desencadenar una revisión del CSMS puede ser la adición o eliminación de activos del IACS. Una práctica común durante el mantenimiento del sistema o la reestructuración puede ser agregar, actualizar o eliminar equipos o software del IACS. Un proceso de gestión de cambios bien definido y seguido detectará esto, lo que puede desencadenar una revisión o auditoría del CSMS. Esta revisión o auditoría garantizaría que el cambio no afectara negativamente la seguridad cibernética del IACS. Otro ejemplo de una actividad no programada sería una respuesta a un brote de virus en una instalación. Después de que el sistema CSMS se haya utilizado para responder y recuperarse del incidente, se debe realizar una revisión o auditoría del CSMS para determinar dónde ocurrió la falla que permitió la propagación del virus.

Cualquier revisión o auditoría de seguridad cibernética (interna o externa) proporcionará a la organización datos valiosos para mejorar el CSMS. Los resultados de estas revisiones o auditorías deben incluir tanta información detallada como sea necesaria para garantizar que se cumplan los requisitos legales o reglamentarios y que se puedan realizar las modificaciones indicadas por la revisión o auditoría. Los resultados deben enviarse a todo el personal apropiado (es decir, partes interesadas, gerentes y personal de seguridad).

A.4.2.3 Indicadores clave de rendimiento

KPI permite a la organización determinar qué tan bien se desempeña el CSMS y lo ayuda a dirigir los recursos hacia áreas que pueden necesitar mejoras. El KPI debería, en la medida de lo posible, ser valores cuantitativos (es decir, números o porcentajes) que indiquen cómo se desempeña una parte particular del CSMS con respecto a las condiciones esperadas.

Dado que las revisiones o auditorías o el CSMS deben expresarse utilizando estos KPI, es importante elegir indicadores que sean relevantes, significativos y consistentes con el CSMS y otros requisitos de la organización. Los resultados de las actividades periódicas programadas pueden expresarse como el rendimiento en comparación con un conjunto de métricas predefinidas para indicar el rendimiento de seguridad y las tendencias de seguridad. Los resultados de actividades no programadas pueden expresarse como la efectividad del CSMS para tratar el evento o incidente no programado.

Los datos de capacidad organizativa deberían ser parte de los indicadores de desempeño. Las compañías deben rastrear el porcentaje de personal asignado a los roles de IACS y el porcentaje de ese personal que ha pasado los requisitos de capacitación y calificación para sus roles. Si bien estos datos pueden parecer esotéricos, los problemas sistémicos se pueden indicar aquí antes de ser notados en malos resultados de auditoría.

La evaluación comparativa del KPI y los resultados de las revisiones o auditorías con respecto a otras organizaciones o requisitos es un buen método para validar el CSMS. Si los datos de evaluación comparativa se recopilan durante un período de tiempo, es posible que la organización pueda determinar tendencias en amenazas o contramedidas. Estos pueden indicar lugares donde los requisitos del CSMS pueden tener que revisarse como parte de la revisión, mejorar y mantener la subcláusula del CSMS (ver A.4.3).

A.4.2.4 Prácticas de apoyo

A.4.2.4.1 Prácticas de referencia

Las siguientes dos acciones son prácticas básicas:

a) Asegurar que se cumplan la idoneidad del entorno de control y el cumplimiento de los objetivos generales de seguridad cibernética. Detectar si las adiciones, actualizaciones o eliminaciones (es decir, parches de software, actualizaciones de aplicaciones y cambios de equipo) han introducido exposiciones de seguridad.

b) Confirmar que, durante un período de auditoría regular especificado, todos los aspectos del CSMS están funcionando según lo previsto. Se debe planificar un número suficiente de auditorías para que la tarea de auditoría se extienda de manera uniforme durante el período elegido. La gerencia debe garantizar que se realicen auditorías periódicas. La gerencia debe asegurarse de que haya evidencia para:

· Verificar que se sigan los procedimientos documentados y que se cumplan los objetivos deseados;

· Validar que los controles técnicos (es decir, cortafuegos y controles de acceso) estén en su lugar y funcionen según lo previsto, tanto de manera constante como continua.

A.4.2.4.2 Prácticas adicionales

Las siguientes tres acciones son prácticas adicionales:

a) Requerir que el programa de métricas de seguridad cibernética se base en los siete pasos clave enumerados a continuación:

   1) definir las metas y objetivos del programa de métricas;

   2) decidir qué métricas generar para medir el grado de adopción y conformidad con las políticas y procedimientos definidos en el CSMS:

      · Evaluar de manera proactiva las posibles vulnerabilidades de seguridad (por ejemplo,% de debilidades de auditoría de seguridad fijadas en la fecha acordada);

      · Seguimiento de la implementación y el uso de medidas preventivas y de seguridad (por ejemplo,% de conformidad con las normas de seguridad).

   3) desarrollar estrategias para generar las métricas;

   4) establecer puntos de referencia y objetivos;

5) determinar cómo se informarán las métricas y a quién;

6) crear un plan de acción y actuar en consecuencia;

7) establecer un ciclo formal de revisión / refinamiento del programa.

b) Revisar los resultados de auditorías, autoevaluaciones, informes de incidentes de seguridad cibernética y comentarios proporcionados por las partes interesadas clave regularmente para comprender la efectividad del CSMS.

c) Realización de revisiones de seguridad operativa en el IACS por ingenieros de IACS capacitados en seguridad. Además, los problemas de seguridad son revisados con frecuencia en un nivel más amplio por un órgano de gobierno.

A.4.2.5 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [24], [26], [35], [49], [50].

A.4.3 Elemento: Revisar, mejorar y mantener el CSMS

A.4.3.1 Descripción del elemento

El proceso de monitoreo y revisión continua del CSMS le permite a una organización establecer, con evidencia, que está cumpliendo con los objetivos, políticas y procedimientos establecidos en el CSMS. Los KPI definidos durante el desarrollo del CSMS se utilizan para evaluar el rendimiento del CSMS durante el proceso de revisión de conformidad. El elemento de conformidad verifica que el CSMS está funcionando *como se* define, mientras que este elemento verifica que los requisitos utilizados para desarrollar el CSMS cumplan con los objetivos de seguridad cibernética de la organización.

Los métodos de verificación interna, tales como auditorías de conformidad e investigaciones de incidentes, permiten a la organización determinar la efectividad del sistema de gestión y si está operando de acuerdo con las expectativas. También es importante establecer que el sistema de gestión aún cumple con las metas, metas y objetivos establecidos durante el proceso de planificación. Si hay desviaciones de las metas, metas u objetivos originales, pueden ser necesarios cambios sistemáticos en el sistema de gestión.

Debido a que tanto las amenazas como las tecnologías para abordar la seguridad están evolucionando, se anticipa que el programa de seguridad cibernética de la organización evolucionará, reflejando las nuevas amenazas y capacidades disponibles. Las organizaciones deberían estar rastreando, midiendo y mejorando los esfuerzos de seguridad para mantener seguros a las personas, propiedades, productos, operaciones industriales, datos y sistemas de información.

El objetivo general es garantizar que el CSMS siga siendo efectivo incorporando mejoras basadas en nuevas amenazas, nuevas capacidades y revisiones periódicas. La atención continua a la seguridad proporciona un indicador al personal de que la seguridad cibernética es un valor central de la compañía.

A.4.3.2 Revisión de conformidad con el CSMS

La conformidad con el CSMS se ha discutido en un elemento anterior. Verifica que la organización siga las políticas y procedimientos expresados en el CSMS. Como parte del proceso de conformidad, se han definido indicadores clave de desempeño para medir el desempeño del CSMS de la organización. Las malas marcas en estos KPI en un ciclo de revisión pueden indicar un problema singular que puede remediarse con

soluciones simples. Las malas marcas en muchos de los KPI o en el mismo KPI en las revisiones repetidas pueden indicar problemas sistémicos con el CSMS. Puede indicar que la capacitación o la aplicación deben mejorarse, los recursos son inadecuados o que los procedimientos implementados no son prácticos. Administrar el CSMS implica hacer estos juicios. Ya sea que los KPI se evalúen a través de auditorías independientes o de uno mismo, es útil consultar con la organización cuyas acciones se están midiendo, para ayudar a tomar esta determinación.

Es importante que el CSMS incluya requisitos para mejorar los resultados de conformidad. Las personas responsables también deben ser contratadas para desarrollar una estrategia a largo plazo para la mejora a fin de asegurar una ruta de mejora rentable y consistente a lo largo del tiempo.

A.4.3.3 Medir y revisar la efectividad del CSMS

Medir la efectividad del CSMS como mínimo implica revisar los datos del incidente. Cuanto mayor sea la capacidad de una organización para detectar infracciones de seguridad cibernética fallidas y exitosas y registrarlas como incidentes, mayor será su capacidad para medir la efectividad del CSMS para reducir el riesgo. Los datos de incidentes incluyen el número de incidentes, el tipo o clase de incidentes y el impacto económico de los incidentes. Estos datos son extremadamente importantes tanto para comprender el impacto económico actual de las amenazas de seguridad cibernética como para evaluar la efectividad de las contramedidas específicas empleadas.

Si bien el análisis de los datos de incidentes puede medir la efectividad del CSMS en el pasado, la administración del CSMS también se encarga de mantener la efectividad del CSMS en el futuro.

Para lograr esto, es necesario monitorear los cambios en los factores que podrían aumentar o disminuir su efectividad en el futuro. Los factores clave a monitorear son los siguientes:

- El nivel de riesgo, que puede cambiar debido a un cambio en la amenaza, vulnerabilidad, consecuencia o probabilidad;
- La tolerancia al riesgo de la organización;
- La implementación de sistemas u operaciones industriales nuevos o modificados;
- Prácticas de la industria;
- Contramedidas técnicas y no técnicas disponibles; · Requisitos legales y reglamentarios.

El CSMS de una organización debe revisarse a intervalos regulares, para evaluar tanto su efectividad pasada como la visión de futuro. Esta revisión debe incluir una evaluación periódica de las políticas y procedimientos de seguridad cibernética para afirmar que esas políticas y procedimientos están vigentes y funcionan y cumplen con los requisitos legales, reglamentarios y de seguridad interna. En circunstancias apropiadas, las evaluaciones también se aplican a las políticas y procedimientos de los socios comerciales de la organización, como proveedores, proveedores de soporte, empresas conjuntas o clientes.

Además de las revisiones periódicas, los cambios importantes en los factores enumerados anteriormente también deberían desencadenar la revisión de aspectos relacionados del CSMS. Una organización debe determinar un conjunto de desencadenantes y umbrales de cambio, lo que desencadenaría dicha revisión. Estos desencadenantes deben incluir los siguientes factores:

· Factores internos: basados en el desempeño del CSMS y los resultados de KPI y otros indicadores internos adecuados (por ejemplo, tolerancia al riesgo, cambios en la gestión y similares).

· Factores externos: los cambios en el entorno de amenazas, las mejores prácticas de la industria, las soluciones disponibles y los requisitos legales pueden indicar la necesidad u oportunidad de mejorar el CSMS.

La organización asignada para administrar los cambios en el CSMS también debe ser responsable de revisar los desencadenantes y los umbrales para los cambios y de usarlos para iniciar el proceso de revisión.

A.4.3.4 Implicaciones legales y regulatorias para el CSMS

El entorno legal y regulatorio al que está sujeta la organización puede cambiar con el tiempo. La organización aún puede cumplir con el CSMS como se definió originalmente, pero ese CSMS ya no puede satisfacer los requisitos legales y reglamentarios que se aplican.

La organización debe revisar periódicamente sus requisitos legales y reglamentarios aplicables e identificar cualquier área donde puedan afectar el CSMS. Además, cualquier cambio importante en los requisitos legales y reglamentarios, como los requisitos nuevos o actualizados importantes, debe desencadenar una revisión del CSMS para garantizar que cumpla con los nuevos requisitos.

A.4.3.5 Administrar el cambio de CSMS

Para tener un sistema coordinado, se debe asignar una organización / equipo para administrar y coordinar el refinamiento y la implementación de los cambios del CSMS. Es probable que esta organización / equipo sea una organización de tipo matriz basada en personas clave de diferentes organizaciones empresariales. Este equipo debe usar un método definido para realizar e implementar cambios.

Varios factores internos y externos necesitarán cambios en el CSMS. La gestión de estos cambios requiere coordinación con los diversos interesados. Al implementar cambios en el sistema de gestión, es importante examinar los posibles efectos secundarios relacionados con la operación o la seguridad del sistema. La seguridad de IACS también debe tener en cuenta las diferentes organizaciones, prácticas y requisitos de respuesta al incorporar mejoras. Deben desarrollarse procedimientos escritos para gestionar los cambios en el CSMS. Este proceso puede incluir los siguientes pasos:

a) Definir el sistema de gestión actual

Antes de que el CSMS pueda ser refinado, es necesario conocer y comprender el sistema de gestión actual. Todas las políticas relacionadas con la seguridad cibernética deben revisarse para que todos los interesados comprendan claramente la política actual y cómo se está implementando. Además, se deben identificar todos los activos y procedimientos relacionados con el CSMS.

b) Definir los procedimientos para proponer y evaluar cambios en el CSMS

Una vez que se entiende el sistema de gestión actual, se debe revisar su cumplimiento y efectividad, como se describió anteriormente. Deben identificarse debilidades o brechas en el sistema de gestión y proponerse correcciones. La evaluación del sistema de gestión debe identificar las áreas donde se podrían requerir cambios. Además, las mejores prácticas y requisitos de la industria descritos en esta norma podrían considerarse al definir cambios que fortalezcan el CSMS. La selección de nuevas contramedidas seguirá los principios descritos en el elemento de Gestión de Riesgos e Implementación

de esta norma (ver A.3.4.2). Una vez definidos, los cambios propuestos al CSMS deben documentarse de manera concisa para que puedan presentarse de manera consistente a otras partes interesadas.

c) Proponer y evaluar cambios al CSMS

Con los cambios identificados y documentados, deben presentarse a las partes interesadas. Los cambios propuestos deben revisarse para determinar si producirán efectos secundarios negativos o imprevistos. También deben evaluarse para determinar si es necesario realizar algún cambio en el CSMS con respecto a los requisitos y conjuntos de pruebas originales. A medida que se desarrollan nuevas capacidades, la reacción de muchas organizaciones es incorporar la tecnología más nueva al sistema. En el entorno IACS, es importante validar cualquier nueva tecnología o solución de seguridad cibernética antes de incorporarla.

d) Implementación de cambios CSMS

Después de que las partes interesadas acuerden el cambio, se deben implementar los cambios al CSMS. Los cambios en la política deben seguir los procedimientos de la compañía para los cambios en la política y, como mínimo, estos cambios deben documentarse y se debe obtener la aprobación por escrito de las partes interesadas clave. Se requiere especial atención a las pruebas de sistemas, validación y control de la participación del proveedor.

e) Monitorear los cambios del CSMS

Con el CSMS nuevo o revisado, es importante monitorear y evaluar su desempeño. Se debe realizar una revisión del sistema de gestión de forma regular y siempre que haya cambios en el CSMS.

A.4.3.6 Prácticas de apoyo.

A.4.3.6.1 Prácticas de referencia

Las siguientes doce acciones son prácticas básicas:

a) Usar un método para desencadenar una revisión del nivel de riesgo residual y tolerancia al riesgo cuando hay cambios en la organización, la tecnología, los objetivos comerciales, la operación industrial o eventos externos, incluidas las amenazas identificadas y los cambios en el clima social.

b) Analizar, registrar e informar datos operativos para evaluar la efectividad o el desempeño del CSMS.

c) Analizar los resultados de las revisiones periódicas y auditorías del CSMS para determinar si se necesita un cambio.

d) Investigar políticas y procedimientos ineficaces de CSMS para determinar cualquier causa raíz donde haya problemas sistémicos. Las acciones se identifican no solo para resolver el problema, sino también para minimizar y prevenir las recurrencias.

e) Revisar las amenazas potenciales y realizar un análisis de impacto de manera regular para determinar si se requieren contramedidas.

f) Identificar las regulaciones y legislación aplicables y cambiantes y las obligaciones y requisitos contractuales de seguridad cibernética.

g) Involucrar a las partes interesadas clave en la organización para la confirmación de las áreas para una mayor investigación y planificación. Las partes interesadas clave deben incluir personal de todos los diferentes grupos afectados por el CSMS (es decir, TI, IACS y seguridad).

h) Identificar acciones correctivas y preventivas apropiadas para mejorar aún más el proceso de desempeño.

i) Priorizar las mejoras en el CSMS y establecer planes para implementarlas (es decir, presupuestos y planificación de proyectos).

j) Implementar todos los cambios utilizando la gestión de los procesos de cambio dentro de la organización. Se requiere especial atención a la participación de los proveedores de pruebas, validación y control de sistemas debido a las implicaciones de HSE del entorno IACS.

k) Validar que se hayan implementado las acciones acordadas de auditorías y revisiones anteriores.

l) Comunicar planes de acción y áreas de mejora a todos los interesados y al personal afectado.

A.4.3.6.2 Prácticas adicionales

Las siguientes dos acciones son prácticas adicionales:

a) Requerir que el programa de métricas de seguridad cibernética se base en los siete pasos clave enumerados a continuación:

1) definir las metas y objetivos del programa de métricas;

2) decidir qué métricas generar para medir la efectividad del CSMS para cumplir con los objetivos de seguridad de la organización;

NOTA Puede ser bueno proporcionar una visión retrospectiva de la preparación de seguridad mediante el seguimiento del número y la gravedad de incidentes de seguridad pasados, incluidos pequeños eventos con patrones.

3) desarrollar estrategias para generar las métricas;

4) establecer puntos de referencia y objetivos;

5) determinar cómo se informarán las métricas y a quién;

6) crear un plan de acción y actuar en consecuencia;

7) establecer un ciclo formal de revisión / refinamiento del programa.

b) Emprender muchas estrategias diferentes para impulsar la mejora continua en las actividades de seguridad cibernética. Las estrategias son proporcionales al riesgo y dependen de la cultura corporativa, los sistemas existentes y el tamaño o la complejidad de los sistemas digitales. Algunas estrategias potenciales son las siguientes:

· Realizar actividades de evaluación comparativa de seguridad dentro y fuera de la industria, incluido el uso de validación externa para ayudar a validar las mejoras;

· Buscar comentarios de los empleados sobre sugerencias de seguridad de forma activa e informar a la alta gerencia según corresponda sobre las deficiencias y oportunidades de desempeño;

· Utilizando metodologías comerciales corporativas normaliadas, como Six Sigma ™, para medir, analizar, mejorar y mantener las mejoras de seguridad cibernética.

A.4.3.7 Recursos utilizados

Este elemento se basó en parte en el material que se encuentra en las siguientes referencias, todas las cuales se enumeran en la Bibliografía: [24], [26], [35], [49].

Anexo B
(informativo)

Proceso para desarrollar un CSMS

B.1 Descripción general

La Cláusula 4 y el Anexo A detallan los elementos individuales asociados con un CSMS integral e integrado. Desarrollar un CSMS que funcione es un viaje que puede llevar meses o años lograr. Este anexo se centra en el orden y la naturaleza iterativa de las actividades asociadas con el desarrollo de los elementos del CSMS. Los objetivos de este Anexo son los siguientes:

· Brindar información clave sobre cómo las organizaciones exitosas han secuenciado estas actividades, y señalar dificultades comunes relacionadas con el orden en que se abordan los elementos de un CSMS;

· Proporcionar una guía paso a paso que una organización puede consultar al comenzar el proceso de establecer un CSMS;

· Proporcionar una guía paso a paso sobre cómo utilizar esta norma.

B.2 Descripción del proceso.

La Figura B.1 muestra las seis actividades CSMS de nivel superior y sus relaciones. Las cifras posteriores de este anexo desglosan cada una de ellas con más detalle. Si bien la Figura B.1 muestra las interrelaciones entre todas las actividades, no todas estas interrelaciones se muestran en detalle más adelante en este Anexo. Esto se ha hecho para equilibrar la representación concisa con la integridad de los temas que se discuten.

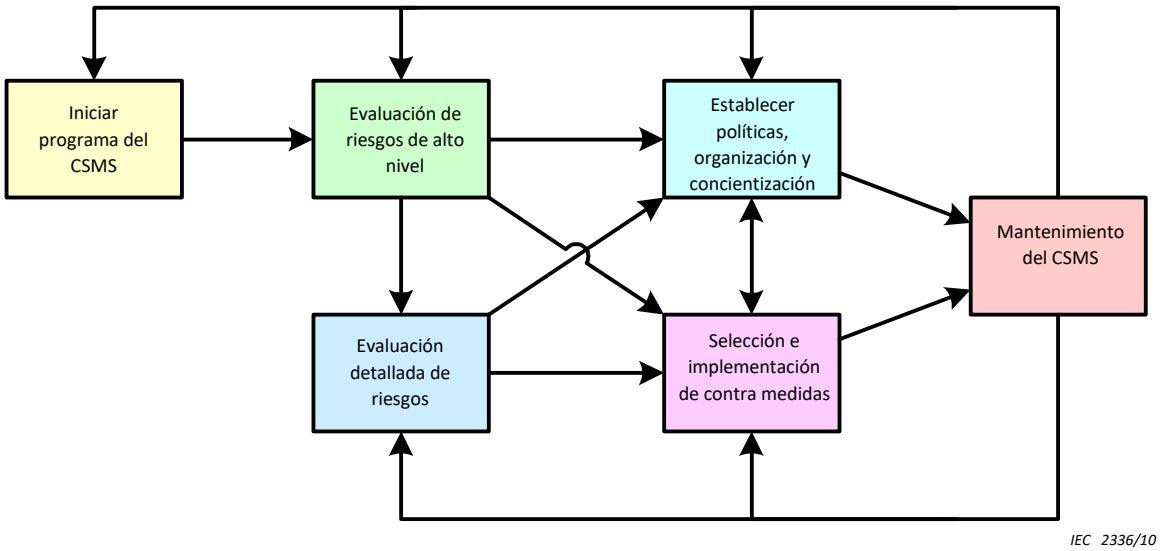

Figura B.1 - Actividades de nivel superior para establecer un CSMS

La actividad "Iniciar programa CSMS" pone al programa en una base sólida al establecer el propósito, el apoyo organizativo, los recursos y el alcance del CSMS. Comenzar con esta actividad maximizará la

efectividad del esfuerzo, como es el caso de cualquier programa con amplio impacto. El alcance inicial puede ser más pequeño de lo deseado, pero puede crecer a medida que el programa tenga éxito.

La evaluación de riesgos impulsa el contenido del CSMS. La actividad de "evaluación de riesgos de alto nivel" presenta amenazas, la probabilidad de su realización, tipos generales de vulnerabilidades y consecuencias. La actividad detallada de evaluación de riesgos agrega una evaluación técnica detallada de vulnerabilidades a esta imagen de riesgo. Es importante abordar la evaluación de riesgos primero a un nivel alto. Una trampa común es gastar recursos desde el principio para realizar una evaluación detallada de la vulnerabilidad y luego experimentar una respuesta apática a estos resultados técnicos, porque no se ha establecido el contexto general de riesgo de nivel superior.

Las dos actividades "Establecer política, organización y concientización" y "Seleccionar e implementar contramedidas" reducen directamente el riesgo para la organización. Estas actividades implementarán decisiones de alto y bajo nivel, impulsadas por las evaluaciones de riesgo detalladas y de alto nivel. La actividad "Establecer políticas, organización y concientización" abarca la creación de políticas y procedimientos, la asignación de responsabilidades organizacionales y la planificación y ejecución de la capacitación. La actividad "Seleccionar e implementar contramedidas" define e implementa las defensas técnicas y no técnicas de seguridad cibernética de la organización. Estas dos actividades principales se llevarán a cabo de manera coordinada. Esto se debe a que, en la mayoría de los casos, las políticas y procedimientos relacionados, la capacitación y la asignación de responsabilidades son esenciales para que una contramedida sea efectiva.

La actividad "Mantener el CSMS" incluye tareas para determinar si la organización se ajusta a sus políticas y procedimientos de CSMS, si el CSMS es eficaz para cumplir los objetivos de seguridad cibernética de la organización y si estos objetivos deben cambiar a la luz de eventos internos o externos. Esta actividad define cuándo se requiere la revisión de sus evaluaciones de riesgo detalladas o de alto nivel o puede precipitar un cambio en los parámetros iniciales del programa. También puede proporcionar información para mejorar las políticas, los procedimientos, las decisiones organizacionales o la capacitación con el fin de maximizar la efectividad de las contramedidas o señalar las debilidades que deben corregirse en la implementación de las contramedidas seleccionadas. Las organizaciones informan que la actividad Mantener el CSMS es muy difícil, ya que el entusiasmo inicial por el programa puede haber disminuido y surgen otras prioridades. Sin embargo, sin una atención adecuada a esta actividad, los resultados positivos del programa se perderán en última instancia, porque el entorno en el que operará el programa no es estático.

El resto de este anexo brinda al lector una mejor comprensión de las seis actividades de nivel superior de CSMS. Se ha hecho referencia al número del elemento o subelemento para ayudar al lector de esta norma a encontrar más información sobre ese tema en particular.

B.3 Actividad: Iniciar el programa CSMS

La Figura B.2 ilustra los pasos involucrados en la actividad "Iniciar programa CSMS".

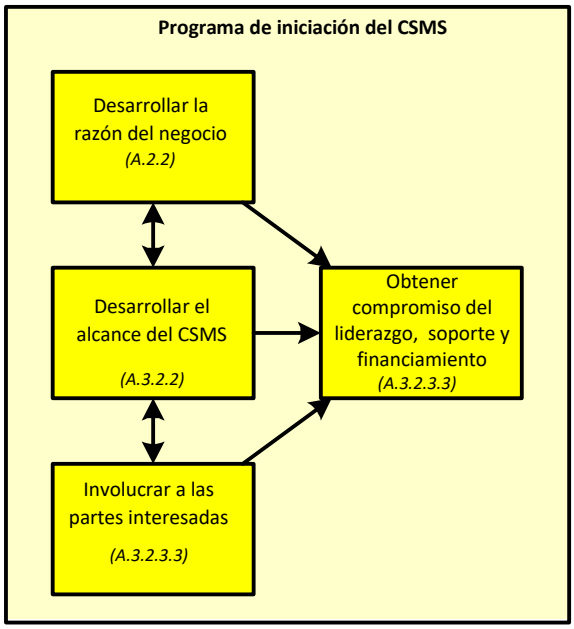

Figura B.2 - Actividades y dependencias para la actividad: iniciar el programa CSMS

El resultado deseado de la actividad "Iniciar programa CSMS" es obtener compromiso de liderazgo, apoyo y financiación para el CSMS. Para lograr esto, los primeros pasos, como se muestra en la Figura B.2, son desarrollar una justificación comercial que justifique el programa para la administración y un alcance propuesto para el programa. En conjunto con estos pasos, las personas que son partes interesadas basadas en esta justificación y alcance son identificadas e involucradas. Es más efectivo identificar a estos interesados por adelantado, siempre que sea posible, y hacerlos parte del esfuerzo para involucrar a la gerencia para que se comprometa con el programa. Luego se puede construir un marco organizacional efectivo para la seguridad, comenzando desde arriba. Una trampa común es intentar iniciar un programa CSMS sin al menos una lógica de alto nivel que relacione la seguridad cibernética con la organización específica y su misión. Las actividades de seguridad cibernética requieren recursos de la organización y, aunque un programa puede comenzar bajo el consenso general de que la seguridad cibernética es buena, el impulso se perderá rápidamente debido a demandas competitivas si no se ha establecido una justificación comercial.

B.4 Actividad: evaluación de riesgos de alto nivel

La Figura B.3 ilustra los pasos involucrados en la actividad de "Evaluación de riesgos de alto nivel".

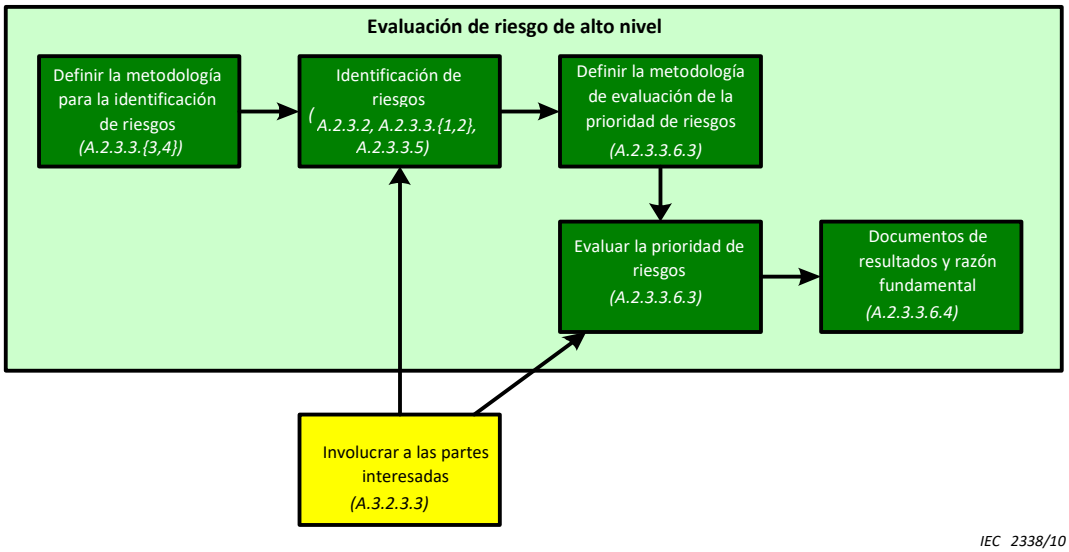

Figura B.3 - Actividades y dependencias para la actividad: evaluación de riesgos de alto nivel

La actividad de "evaluación de riesgos de alto nivel" consiste en seleccionar metodologías para identificar y priorizar los riesgos y luego ejecutar esas metodologías. Es importante definir estas metodologías por adelantado para que proporcionen estructura para el resto de la evaluación de riesgos. La Figura B.3 muestra que es importante involucrar a las partes interesadas, identificadas durante la actividad del Programa Iniciar CSMS, en el proceso de identificación y evaluación de la prioridad de los riesgos. El paso final para documentar los resultados y la justificación es importante porque este registro será invaluable cuando la evaluación de riesgos deba confirmarse o actualizarse en el futuro.

B.5 Actividad: evaluación detallada del riesgo

Como se muestra en la Figura B.4, la actividad de "Evaluación detallada de riesgos" proporciona mayores detalles a la evaluación de riesgos, al hacer primero un inventario de sistemas, redes y dispositivos IACS específicos. Las limitaciones de recursos o tiempo pueden no permitir un examen detallado de todos estos activos. En este caso, las amenazas, las consecuencias y los tipos de vulnerabilidades identificados en la evaluación de riesgos de alto nivel se utilizan para ayudar a establecer prioridades para esos sistemas, redes y dispositivos particulares en los que enfocarse. Otros factores, como el apoyo local o el historial de problemas, también contribuirán a determinar el enfoque para una evaluación detallada del riesgo. La identificación de vulnerabilidades detalladas se guía por los tipos de vulnerabilidad de la evaluación de riesgos de alto nivel, pero no se limita a esos tipos. Por lo tanto, una evaluación detallada de la vulnerabilidad puede descubrir no solo nuevos tipos de vulnerabilidades, sino también amenazas potencialmente nuevas y consecuencias asociadas que no se habían identificado durante la evaluación de riesgos de alto nivel, en otras palabras, nuevos riesgos. En este caso, la evaluación de alto nivel debe actualizarse para incluirlos. Todas las vulnerabilidades encontradas se asocian con un riesgo específico (amenaza, probabilidad y consecuencia) y se priorizan de manera coherente con el método utilizado durante la evaluación de riesgos de alto nivel.

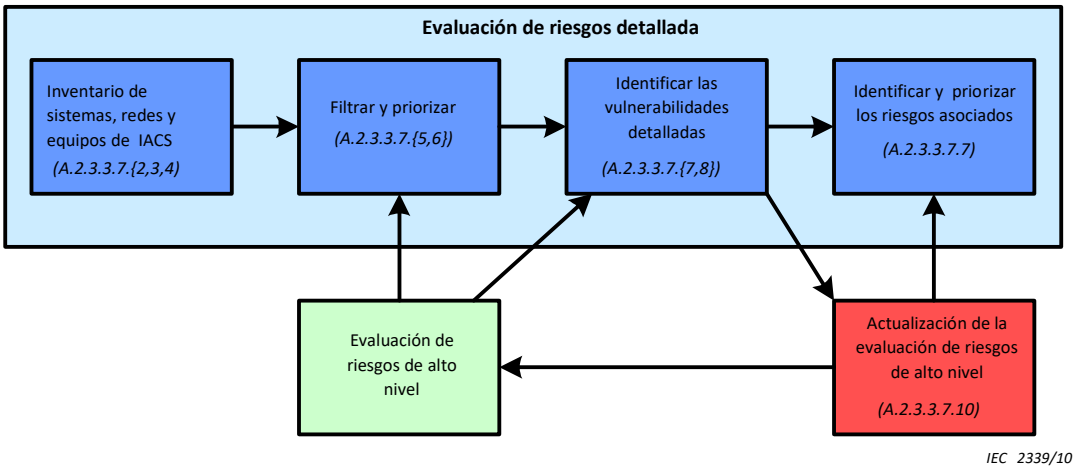

Figura B.4 - Actividades y dependencias para la actividad: evaluación detallada de riesgos

B.6 Actividad: Establecer una política de seguridad, organización y concientización.

Las políticas apropiadas para la organización son una interpretación operativa de la tolerancia al riesgo de la organización. Una organización que crea una política antes de comprender su riesgo o tolerancia al riesgo puede realizar un esfuerzo innecesario para seguir y hacer cumplir una política inapropiada o, de la misma manera, descubrir que sus políticas no respaldan el nivel de reducción de riesgo requerido. La Figura B.5 ilustra los pasos involucrados en la actividad "Establecer una política de seguridad, organización y concientización".

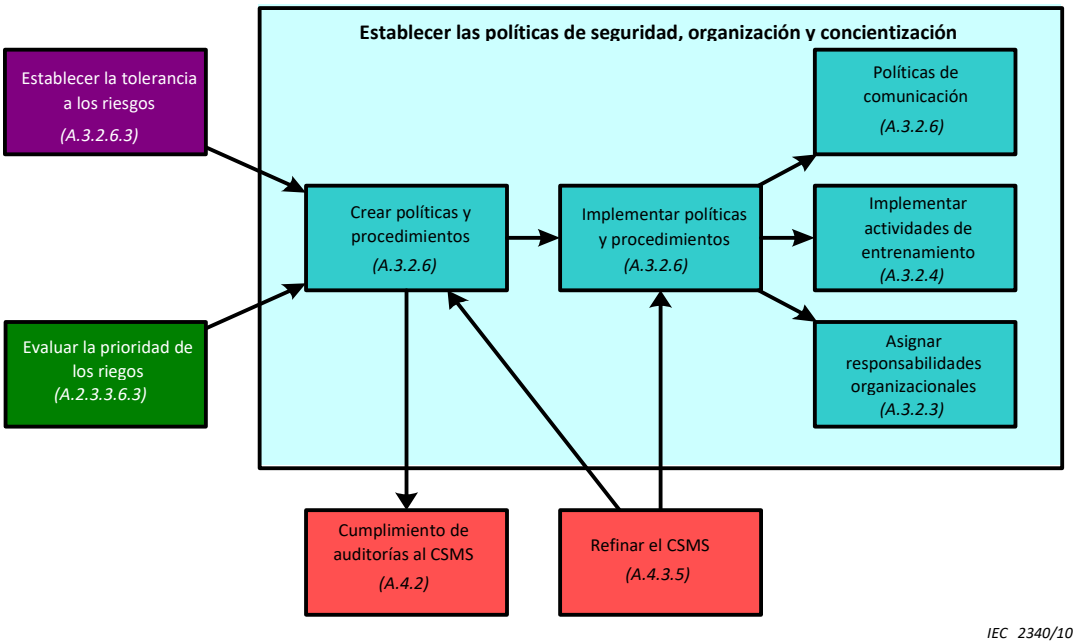

Figura B.5 - Actividades y dependencias para la actividad: establecer una política de seguridad, organización y concientización

La implementación de la política implica comunicar la política a la organización, capacitar al personal de la organización y asignarle la responsabilidad de su cumplimiento. Las políticas y procedimientos pueden afectar cualquier actividad en el CSMS. Por ejemplo, puede haber políticas con respecto a las contramedidas comunes que se utilizarán, que requieran procesos específicos de desarrollo y mantenimiento del sistema o determinar cuándo se debe volver a evaluar el riesgo. Por lo tanto, la Figura B.5 no intenta representar todos los impactos potenciales de las políticas y procedimientos en el CSMS.

La Figura B.6 desglosa las dos actividades "Desarrollar actividades de capacitación" y "Asignar responsabilidades de la organización". Muestra muchas de las diferentes actividades de capacitación que conforman un programa de capacitación, las responsabilidades organizacionales asociadas con esas actividades de capacitación y las actividades relacionadas con partes relacionadas del programa CSMS. Esta figura no muestra todas las responsabilidades organizacionales o temas de capacitación que puedan estar relacionados con el CSMS, pero trata de mostrar los puntos principales que deben considerarse.

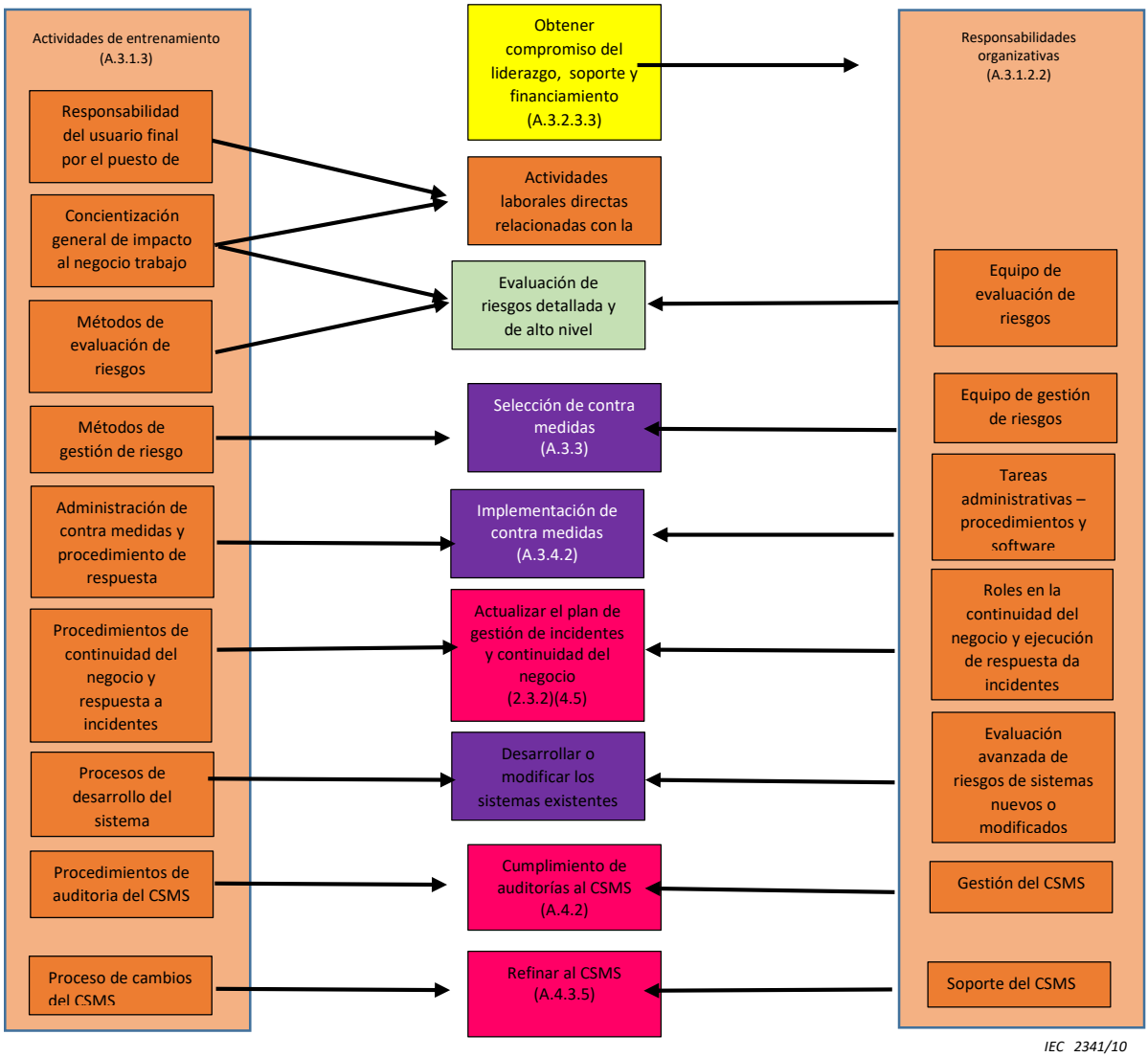

Figura B.6 - Capacitación y asignación de responsabilidades de la organización.

B.7 Actividad: Seleccionar e implementar contramedidas.

La Figura B.7 ilustra los pasos involucrados en la actividad "Seleccionar e implementar contramedidas".

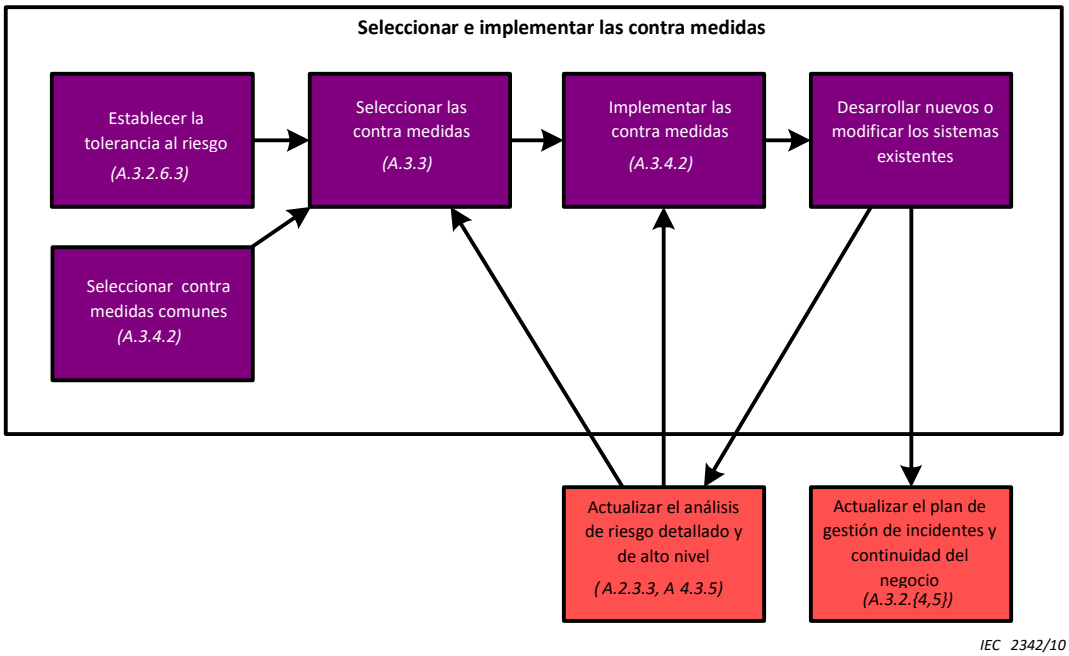

Figura B.7 - Actividades y dependencias para la actividad: seleccionar e implementar contramedidas

La selección de contramedidas es el proceso técnico de gestión de riesgos. La tolerancia al riesgo de la organización, las contramedidas comunes preseleccionadas y los resultados de la evaluación de riesgos de alto nivel y nivel detallado impulsan el enfoque de gestión de riesgos para seleccionar contramedidas. Si la organización está implementando un nuevo sistema o modificando un sistema existente, esto lleva a una actualización de evaluaciones de riesgo detalladas y de alto nivel para el escenario en el que se implementa este nuevo sistema. La selección de contramedidas relacionadas con el sistema nuevo o modificado se realiza en función de esta información de riesgo actualizada. El desarrollo o modificación de sistemas requiere una actualización de los planes de continuidad del negocio y respuesta a incidentes.

B.8 Actividad: Mantener el CSMS

Como se muestra en la Figura B.8, la actividad "Mantener el CSMS" requiere una revisión periódica y un refinamiento del CSMS basado en los resultados de la revisión. Los principales aportes a esta revisión son los resultados de las medidas de efectividad y las auditorías de conformidad del monitoreo interno del propio CSMS. Otros aportes a esta revisión son información externa sobre contramedidas disponibles, prácticas industriales en evolución y leyes o regulaciones nuevas o modificadas.

Una revisión del CSMS identifica deficiencias y propone mejoras, lo que a su vez crea mejoras en el CSMS. Algunas de estas mejoras pueden tomar la forma de nuevas contramedidas o mejoras en la implementación de contramedidas. Otras mejoras pueden modificar políticas y procedimientos o mejorar su implementación. La revisión de los malos resultados de conformidad puede señalar la necesidad de mejoras en la capacitación o asignación de responsabilidades organizacionales.

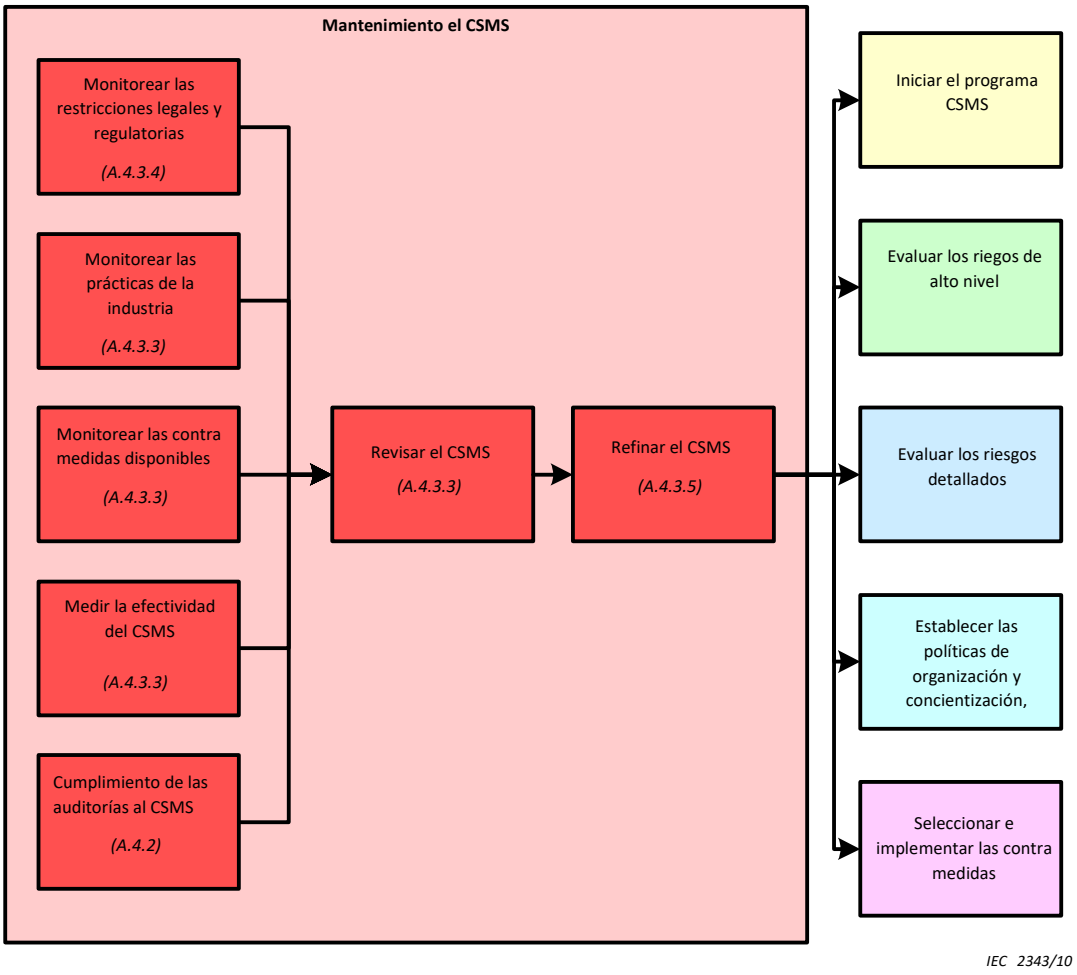

Figura B.8 - Actividades y dependencias para la actividad: mantener el CSMS

Anexo C
(informativo)

Estructura de requisitos a ISO / IEC 27001

C.1 Descripción general

Los requisitos contenidos en este documento son muy similares a los requisitos contenidos en ISO / IEC 27001 [24]. Esta norma, IEC 62443 - 2 - 1, fue desarrollado por referencia a ISO / IEC 27001 y se hacen muchas referencias cruzadas en todas partes. Sin embargo, esta norma no utiliza la misma organización para describir sus requisitos. Esta organización alternativa fue deliberada, como resultado de un cambio realizado durante el desarrollo de la norma en respuesta a los revisores iniciales del usuario final de IACS, para ayudar a la legibilidad del usuario combinando requisitos similares en subcláusulas más grandes y proporcionando una orientación informativa considerable en el Anexo A. Porque muchos El personal con experiencia en seguridad de la información ya está familiarizado con ISO / IEC 27001, este anexo se ha incluido para ayudar a esos lectores a comprender las similitudes en los requisitos de las dos normas.

NOTA Como resultado de los comentarios del comité nacional de IEC sobre la versión del borrador del comité para votación (CDV) de esta norma, el cuerpo normativo de la próxima edición de esta norma reflejará mejor la organización de ISO / IEC 27001, con gran parte de lo solicitado previamente Guía del usuario de IACS relegada a anexos informativos. El trabajo en la próxima edición de esta norma comenzará después de la adopción de esta edición.

Este anexo contiene dos tablas de asignaciones de requisitos. La primera tabla contiene los requisitos de esta norma y muestra sus referencias relacionadas de la norma ISO / IEC 27001. La segunda tabla contiene los requisitos en ISO / IEC 27001 y muestra sus referencias relacionadas de esta norma. El Estructura de requisitos está en un nivel de subcláusula y no representa un análisis exhaustivo de todos los requisitos detallados. Se puede hacer un análisis más detallado de los requisitos en una futura revisión de esta norma.

C.2 Estructura de esta norma a ISO / IEC 27001: 2005

La Tabla C.1 muestra un Estructura de los requisitos en esta norma en un nivel de subcláusula a partes de ISO / IEC 27001: 2005.

NOTA Se ha escrito una revisión de ISO / IEC 27001, pero no se publicó al redactar esta norma. No se ha intentado proporcionar una asignación actualizada de los requisitos de esta norma a la versión más reciente de ISO / IEC 27001.

Tabla C.1 - Estructura de los requisitos en esta norma a las referencias ISO / IEC 27001

IEC 62443 - 2 - 1 requisito	Referencias relacionadas ISO / IEC 27001
4.2.2 Justificación comercial	4.2.1e) Analizar y evaluar los riesgos. 5.2.1 Provisión de recursos
4.2.3 Identificación, clasificación y evaluación de riesgos.	4.2.1c) Enfoque de evaluación de riesgos 4.2.1d) Identificar los riesgos. 4.2.1e) Analizar y evaluar los riesgos. 4.3.1 Requisitos generales del documento A.6.2 Partes externas A.7.1 Responsabilidad por activos
4.3.2.2 Alcance del CSMS	4.2.1a) Alcance y límites del SGSI 4.3.1 Requisitos generales del documento
4.3.2.3 Organización para la seguridad	4.2.1b) Política del SGSI 4.2.1i) Obtener autorización de la gerencia para implementar y operar el SGSI 4.2.2a) Formular un plan de tratamiento de riesgos 4.2.2b) Implementar el plan de tratamiento de riesgos. 4.2.2g) Gestionar recursos para el SGSI 5.1 Compromiso de la gerencia 5.2.1 Provisión de recursos A.6.1 Organización interna
4.3.2.4 Capacitación del personal y concientización de seguridad	4.2.2e) Implementar programas de capacitación y sensibilización. 5.2.2 Formación, sensibilización y competencia. A.8.2 Seguridad de los recursos humanos: durante el empleo
4.3.2.5 Plan de continuidad del negocio	4.3.2 Control de documentos 4.3.3 Control de registros A.9.1 Áreas seguras A.9.2 Seguridad del equipo A.14.1 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.

IEC 62443 - 2 - 1 Requisito	Referencias relacionadas ISO / IEC 27001
4.3.2.6 Políticas y procedimientos de seguridad	4.2.1b) Política del SGSI 4.2.1h) Obtener la aprobación de la dirección de los riesgos residuales propuestos 4.2.1i) Obtener autorización de la gerencia para implementar y operar el SGSI 4.2.2d) Definir cómo medir la efectividad de los controles seleccionados 4.3.1 Requisitos generales del documento 4.3.2 Control de documentos 7.1 Revisión de la gestión del SGSI
4.3.3.2 Seguridad del personal	A.6.1 Organización interna A.6.2 Partes externas A.8.1 Seguridad de los recursos humanos: antes del empleo A.8.2 Seguridad de recursos humanos - Durante el empleo A.8.3 Seguridad de recursos humanos - Terminación o cambio de empleo A.10.1 Procedimientos y responsabilidades operacionales
4.3.3.3 Seguridad física y ambiental.	A.9.1 Áreas seguras A.9.2 Seguridad del equipo A.10.7 Manejo de medios
4.3.3.4 Segmentación de red	A.10.1 Procedimientos y responsabilidades operacionales A.10.3 Planificación y aceptación del sistema. A.10.6 Gestión de seguridad de la red. A.11.4 Control de acceso a la red.
4.3.3.5 Control de acceso: administración de la cuenta	A.11.1 Requisito comercial para el control de acceso A.11.2 Gestión de acceso de usuarios
4.3.3.6 Control de acceso: autenticación	A.11.3 Responsabilidades del usuario A.11.4 Control de acceso a la red. A.11.5 Control de acceso al sistema operativo
4.3.3.7 Control de acceso: autorización	A.11.6 Aplicación y control de acceso a la información. A.11.7 Computación móvil y teletrabajo

IEC 62443 - 2 - 1 Requisito	Referencias relacionadas ISO / IEC 27001
4.3.4.2 Gestión de riesgos e implementación	4.2.1d) Identificar los riesgos. 4.2.1e) Analizar y evaluar los riesgos. 4.2.1f) Identificar y evaluar opciones para el tratamiento de riesgos. 4.2.1g) Seleccionar objetivos de control y controles para el tratamiento de riesgos 4.2.1h) Obtener la aprobación de la dirección de los riesgos residuales propuestos
	4.2.1j) Preparar una declaración de aplicabilidad 4.2.2b) Implementar el plan de tratamiento de riesgos. 4.2.2c) Implementar controles 4.2.2d) Definir cómo medir la efectividad de los controles seleccionados 4.2.2h) Implementar procedimientos y controles para detectar y responder a eventos de seguridad 5.2.1 Provisión de recursos
4.3.4.3 Desarrollo y mantenimiento del sistema.	A.10.1 Procedimientos y responsabilidades operacionales A.10.2 Gestión de prestación de servicios de terceros. A.10.3 Planificación y aceptación del sistema. A.10.4 Protección contra códigos maliciosos y móviles A.10.5 Copia de seguridad A.10.6 Gestión de seguridad de la red. A.10.8 Intercambio de información A.10.9 Servicios de comercio electrónico. A.10.10 Monitoreo A.12.1 Requisitos de seguridad de los sistemas de información. A.12.2 Procesamiento correcto en aplicaciones A.12.3 Controles criptográficos

	A.12.4 Seguridad de los archivos del sistema
IEC 62443 - 2 - 1 requisito	**Referencias relacionadas ISO / IEC 27001**
	A.12.5 Seguridad en los procesos de desarrollo y soporte. A.12.6 Gestión de vulnerabilidades técnicas
4.3.4.4 Gestión de información y documentos.	4.3.1 Requisitos generales del documento 4.3.2 Control de documentos 4.3.3 Control de registros A.10.7 Manejo de medios
4.3.4.5 Planificación y respuesta a incidentes	4.2.2h) Implementar procedimientos y controles para detectar y responder a eventos de seguridad 4.3.2 Control de documentos A.13.1 Informe de eventos de seguridad de la información y debilidades A.13.2 Gestión de incidentes y mejoras de seguridad de la información.
4.4.2 Conformidad	4.2.2d) Definir cómo medir la efectividad de los controles seleccionados 4.2.3a) Ejecutar procedimientos de monitoreo y revisión y otros controles 4.2.3c) Medir la efectividad de los controles 4.2.3e) Realizar auditorías internas del SGSI a intervalos planificados 6 auditorías internas del SGSI A.10.10 Monitoreo A.15.1 Cumplimiento de los requisitos legales. A.15.2 Cumplimiento de políticas y normas de seguridad, y cumplimiento técnico A.15.3 Consideraciones de auditoría de sistemas de información.

IEC 62443 - 2 - 1 requisito	Referencias relacionadas ISO / IEC 27001
4.4.3 Revisar, mejorar y mantener el CSMS	4.2.2f) Gestionar el funcionamiento del SGSI 4.2.3a) Ejecutar procedimientos de monitoreo y revisión y otros controles 4.2.3b) Realizar revisiones periódicas de la efectividad del SGSI 4.2.3c) Medir la efectividad de los controles 4.2.3d) Revise las evaluaciones de riesgos, los riesgos residuales y los niveles aceptables de riesgo a intervalos planificados. 4.2.3f) Revise el SGSI regularmente para determinar si el alcance sigue siendo adecuado y si se identifican mejoras al SGSI 4.2.3g) Actualizar los planes de seguridad de las actividades de monitoreo y revisión 4.2.3h) Registrar acciones y eventos que podrían tener un impacto en la efectividad o desempeño del SGSI 4.2.4a) Implementar las mejoras identificadas del SGSI 4.2.4b) Tomar las medidas correctivas y preventivas apropiadas 4.2.4c) Comunicar las acciones y mejoras a todas las partes interesadas. 4.2.4d) Asegurar que las mejoras alcancen los objetivos previstos 5.1 Compromiso de la gerencia 6 auditorías internas del SGSI 7.1 Revisión de la gestión del SGSI 7.2 Revisión de entrada para revisión de la gerencia 7.3 Resultados de revisión de una revisión de la gerencia 8.1 Mejora continua del SGSI 8.2 Acción correctiva 8.3 Acción preventiva A.13.2 Gestión de incidentes y mejoras de seguridad de la información.

C.3 Estructura de ISO / IEC 27001: 2005 a esta norma

La tabla C.2 contiene la asignación inversa a la de la tabla C.1.

Tabla C.2 - Estructura de los requisitos ISO / IEC 27001 a esta norma

Requisito ISO / IEC 27001	Referencias IEC 62443 2 1 relacionadas
4.2.1a) Alcance y límites del SGSI	4.3.2.2 Alcance del CSMS
4.2.1b) Política del SGSI	4.3.2.3 Organización para la seguridad 4.3.2.6 Políticas y procedimientos de seguridad
4.2.1c) Enfoque de evaluación de riesgos	4.2.3 Identificación, clasificación y evaluación de riesgos.
4.2.1d) Identificar los riesgos.	4.2.3 Identificación, clasificación y evaluación de riesgos. 4.3.4.2 Gestión de riesgos e implementación
4.2.1e) Analizar y evaluar los riesgos.	4.2.2 Justificación comercial 4.2.3 Identificación, clasificación y evaluación de riesgos. 4.3.4.2 Gestión de riesgos e implementación
4.2.1f) Identificar y evaluar opciones para el tratamiento de riesgos.	4.3.4.2 Gestión de riesgos e implementación
4.2.1g) Seleccionar objetivos de control y controles para el tratamiento de riesgos	4.3.4.2 Gestión de riesgos e implementación
4.2.1h) Obtener la aprobación de la dirección de los riesgos residuales propuestos	4.3.2.6 Políticas y procedimientos de seguridad 4.3.4.2 Gestión de riesgos e implementación
4.2.1i) Obtener autorización de la gerencia para implementar y operar el SGSI	4.3.2.3 Organización para la seguridad 4.3.2.6 Políticas y procedimientos de seguridad
4.2.1j) Preparar una declaración de aplicabilidad	4.3.4.2 Gestión de riesgos e implementación
4.2.2a) Formular un plan de tratamiento de riesgos	4.3.2.3 Organización para la seguridad
4.2.2b) Implementar el plan de tratamiento de riesgos.	4.3.2.3 Organización para la seguridad 4.3.4.2 Gestión de riesgos e implementación
4.2.2c) Implementar controles	4.3.4.2 Gestión de riesgos e implementación
Requisito ISO / IEC 27001	**IEC 62443 - 2 - 1 referencias relacionadas**

4.2.2d) Definir cómo medir la efectividad de los controles seleccionados	4.3.2.6 Políticas y procedimientos de seguridad 4.3.4.2 Gestión e implementación de riesgos 4.4.2 Conformidad
4.2.2e) Implementar programas de capacitación y sensibilización.	4.3.2.4 Capacitación del personal y concientización de seguridad
4.2.2f) Gestionar el funcionamiento del SGSI	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.2g) Gestionar recursos para el SGSI	4.3.2.3 Organización para la seguridad
4.2.2h) Implementar procedimientos y controles para detectar y responder a eventos de seguridad	4.3.4.2 Gestión de riesgos e implementación 4.3.4.5 Planificación y respuesta a incidentes
4.2.3a) Ejecutar procedimientos de monitoreo y revisión y otros controles	4.4.2 Conformidad 4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3b) Realizar revisiones periódicas de la efectividad del SGSI	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3c) Medir la efectividad de los controles	4.4.2 Conformidad 4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3d) Revise las evaluaciones de riesgos, los riesgos residuales y los niveles aceptables de riesgo a intervalos planificados.	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3e) Realizar auditorías internas del SGSI a intervalos planificados	4.4.2 Conformidad
4.2.3f) Revise el SGSI regularmente para determinar si el alcance sigue siendo adecuado y si se identifican mejoras al SGSI	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3g) Actualizar los planes de seguridad de las actividades de monitoreo y revisión	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.3h) Registrar acciones y eventos que podrían tener un impacto en la efectividad o desempeño del SGSI	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.4a) Implementar las mejoras identificadas de ISMS	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.4b) Tomar las medidas correctivas y preventivas apropiadas	4.4.3 Revisar, mejorar y mantener el CSMS
Requisito ISO / IEC 27001	**IEC 62443 - 2 - 1 referencias relacionadas**

4.2.4c) Comunicar las acciones y mejoras a todas las partes interesadas.	4.4.3 Revisar, mejorar y mantener el CSMS
4.2.4d) Asegurar que las mejoras alcancen los objetivos previstos	4.4.3 Revisar, mejorar y mantener el CSMS
4.3.1 Requisitos generales del documento	4.2.3 Identificación, clasificación y evaluación de riesgos. 4.3.2.2 Alcance del CSMS 4.3.2.6 Políticas y procedimientos de seguridad 4.3.4.4 Gestión de información y documentos.
4.3.2 Control de documentos	4.3.2.5 Plan de continuidad del negocio 4.3.2.6 Políticas y procedimientos de seguridad 4.3.4.4 Gestión de información y documentos. 4.3.4.5 Planificación y respuesta a incidentes
4.3.3 Control de registros	4.3.2.5 Plan de continuidad del negocio 4.3.4.4 Gestión de información y documentos.
5.1 Compromiso de la gerencia	4.3.2.3 Organización para la seguridad 4.4.2 Conformidad 4.4.3 Revisar, mejorar y mantener el CSMS
5.2.1 Provisión de recursos	4.2.2 Justificación comercial 4.3.2.3 Organización para la seguridad 4.3.4.2 Gestión de riesgos e implementación
5.2.2 Formación, sensibilización y competencia.	4.3.2.4 Capacitación del personal y concientización de seguridad
6 auditorías internas del SGSI	4.4.2 Conformidad 4.4.3 Revisar, mejorar y mantener el CSMS
7.1 Revisión de la gestión del SGSI	4.3.2.6 Políticas y procedimientos de seguridad 4.4.3 Revisar, mejorar y mantener el CSMS
7.2 Revisión de entrada para revisión de la gerencia	4.4.3 Revisar, mejorar y mantener el CSMS
Requisito ISO / IEC 27001	**IEC 62443 - 2 - 1 referencias relacionadas**

7.3 Resultados de revisión de una revisión de la gerencia	4.4.3 Revisar, mejorar y mantener el CSMS
8.1 Mejora continua del SGSI	4.4.3 Revisar, mejorar y mantener el CSMS
8.2 Acción correctiva	4.4.3 Revisar, mejorar y mantener el CSMS
8.3 Acción preventiva	4.4.3 Revisar, mejorar y mantener el CSMS
A.5.1 Política de seguridad de la información	No hay cláusula específica; las políticas de seguridad del sistema de control interpretan y aplican políticas generales a este entorno
A.6.1 Organización interna	4.3.2.3 Organización para la seguridad 4.3.3.2 Seguridad del personal
A.6.2 Partes externas	4.2.3 Identificación, clasificación y evaluación de riesgos. 4.3.3.2 Seguridad del personal
A.7.1 Responsabilidad por activos	4.2.3 Identificación, clasificación y evaluación de riesgos.
A.7.2 Clasificación de la información	No hay cláusula específica; las políticas de seguridad del sistema de control interpretan y aplican políticas generales a este entorno
A.8.1 Seguridad de los recursos humanos: antes del empleo	4.3.3.2 Seguridad del personal
A.8.2 Seguridad de los recursos humanos: durante el empleo	4.3.2.4 Capacitación del personal y concientización de seguridad 4.3.3.2 Seguridad del personal
A.8.3 Seguridad de los recursos humanos: terminación o cambio de empleo	4.3.3.2 Seguridad del personal
A.9.1 Áreas seguras	4.3.2.5 Plan de continuidad del negocio 4.3.3.3 Seguridad física y ambiental.
A.9.2 Seguridad del equipo	4.3.2.5 Plan de continuidad del negocio 4.3.3.3 Seguridad física y ambiental.
A.10.1 Procedimientos y responsabilidades operacionales	4.3.3.2 Seguridad del personal 4.3.3.4 Segmentación de red 4.3.4.3 Desarrollo y mantenimiento del sistema. 4.4.2 Conformidad
Requisito ISO / IEC 27001	**IEC 62443 - 2 - 1 referencias relacionadas**

A.10.2 Gestión de prestación de servicios de terceros.	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.3 Planificación y aceptación del sistema.	4.3.3.4 Segmentación de red 4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.4 Protección contra códigos maliciosos y móviles	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.5 Copia de seguridad	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.6 Gestión de seguridad de la red.	4.3.3.4 Segmentación de red 4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.7 Manejo de medios	4.3.3.3 Seguridad física y ambiental. 4.3.4.4 Gestión de información y documentos.
A.10.8 Intercambio de información	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.9 Servicios de comercio electrónico.	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.10.10 Monitoreo	4.3.4.3 Desarrollo y mantenimiento del sistema. 4.4.2 Conformidad
A.11.1 Requisito comercial para el control de acceso.	4.3.3.5 Control de acceso: administración de la cuenta
A.11.2 Gestión de acceso de usuarios	4.3.3.5 Control de acceso: administración de la cuenta
A.11.3 Responsabilidades del usuario	4.3.3.6 Control de acceso: autenticación
A.11.4 Control de acceso a la red.	4.3.3.4 Segmentación de red 4.3.3.6 Control de acceso: autenticación
A.11.5 Control de acceso al sistema operativo	4.3.3.6 Control de acceso: autenticación
A.11.6 Aplicación y control de acceso a la información.	4.3.3.7 Control de acceso: autorización
A.11.7 Computación móvil y teletrabajo	4.3.3.7 Control de acceso: autorización

Requisito ISO / IEC 27001	IEC 62443 - 2 - 1 referencias relacionadas
A.12.1 Requisitos de seguridad de los sistemas de información.	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.12.2 Procesamiento correcto en aplicaciones	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.12.3 Controles criptográficos	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.12.4 Seguridad de los archivos del sistema	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.12.5 Seguridad en los procesos de desarrollo y soporte.	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.12.6 Gestión de vulnerabilidades técnicas	4.3.4.3 Desarrollo y mantenimiento del sistema.
A.13.1 Informe de eventos de seguridad de la información y debilidades	4.3.4.5 Planificación y respuesta a incidentes
A.13.2 Gestión de incidentes y mejoras de seguridad de la información.	4.3.4.5 Planificación y respuesta a incidentes 4.4.3 Revisar, mejorar y mantener el CSMS
A.14.1 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.	4.3.2.5 Plan de continuidad del negocio
A.15.1 Cumplimiento de los requisitos legales.	4.4.2 Conformidad
A.15.2 Cumplimiento de políticas y normas de seguridad, y cumplimiento técnico	4.4.2 Conformidad
A.15.3 Consideraciones de auditoría de sistemas de información.	4.4.2 Conformidad

Bibliografía

NOTA Esta bibliografía incluye referencias a fuentes utilizadas en la creación de esta norma, así como referencias a fuentes que pueden ayudar al lector a desarrollar una mayor comprensión de la seguridad cibernética en su conjunto y desarrollar un sistema de gestión. No todas las referencias en esta bibliografía se mencionan en todo el texto de esta norma. Las referencias se han desglosado en diferentes categorías según el tipo de fuente que sean.

Referencias a otras partes, tanto existentes como anticipadas, de la serie IEC 62443:

NOTA Algunas de estas referencias son referencias normativas (ver Cláusula 2), documentos publicados, en desarrollo o anticipados. Todos se enumeran aquí para completar las partes anticipadas de la serie IEC 62443.

[1] IEC / TS 62443 - 1 - 1 [2] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 1-1: Terminología, conceptos y modelos*

[2] IEC / TR 62443 - 1 - 2 [4] , *Redes de comunicación industrial - Red y sistema seguridad - Parte 1-2: Glosario maestro de términos y abreviaturas*

[3] IEC / TR 62443 - 1 - 3, *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 1-3: Métricas de cumplimiento de seguridad del sistema*

NOTA Esta norma es IEC 62443 - 2 - 1, *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 2 1: Establecimiento de un programa de seguridad del sistema de automatización y control industrial*

[4] IEC 62443 - 2 - 2 [5] , *Redes de comunicación industrial. Seguridad de redes y sistemas. Parte 2-2: Operación de un programa de seguridad de sistemas de control y automatización industrial.*

[5] IEC / TR 62443 - 2 - 3 [4] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 2-3: Gestión de parches en el entorno IACS*

[6] IEC / TR 62443 - 3 - 1, *Redes de comunicación industrial. Seguridad de redes y sistemas. Parte 3-1: Tecnologías de seguridad para sistemas de control y automatización industrial.*

[7] IEC 62443 - 3 - 2 [4] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 3-2: Objetivos de niveles de garantía de seguridad para zonas y conductos*

[8] IEC 62443 - 3 - 3 [4] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 3-3: Requisitos de seguridad del sistema y niveles de garantía de seguridad*

[9] IEC 62443 - 3 - 4 [4] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 3-4: Requisitos de desarrollo de productos*

[10] IEC 62443 - 4 - 1 [4] , *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 4-1: Dispositivos integrados*

[11] IEC 62443 - 4 - 2 [4], *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 4-2: Dispositivos host*

[12] IEC 62443 - 4 - 3 [4], *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 4-3: Dispositivos de red*

---

4 En desarrollo.

5 Planeado para esta norma internacional.

[13] IEC 62443 - 4 - 4 [4], *Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 4-4: Aplicación, datos y funciones*

Otras referencias de normas:

[14] IEC 61131-3, *Controladores programables. Parte 3: Lenguajes de programación.*

[15] IEC 61512-1, *Control de lotes, Parte 1: Modelos y terminología.*

[16] IEC 62264-1, *Integración del sistema de control empresarial, Parte 1: Modelos y terminología.*

[17] Directivas ISO / IEC, Parte 2, *Reglas para la estructura y redacción de Normas Internacionales.*

[18] ISO / IEC 10746-1, *Tecnología de la información - Procesamiento distribuido abierto - Modelo de referencia: Descripción general*

[19] ISO / IEC 10746-2, *Tecnología de la información - Procesamiento distribuido abierto - Modelo de referencia: Fundamentos*

[20] ISO / IEC 15408-1: 2008, *Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad de TI - Parte 1: Introducción y modelo general*

[21] ISO / IEC 15408-2: 2008, *Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad de TI - Parte 2: Componentes funcionales de seguridad*

[22] ISO / IEC 15408-3: 2008, *Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad de TI - Parte 3: Componentes de garantía de seguridad*

[23] ISO / IEC 17799, *Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información*

[24] ISO / IEC 27001: 2005, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*

[25] 29 CFR 1910.119 - *Normas de seguridad y salud ocupacional de EE . UU. - Materiales peligrosos - Gestión de seguridad de procesos de productos químicos altamente peligrosos*

Referencias específicas de la industria y del sector:

[26] Orientación para abordar la seguridad cibernética en el sector químico, versión 3.0, mayo de 2006, Centro de Tecnología de la Información Química (ChemITC) del Consejo Estadounidense de Química, disponible en
< http://www.chemicalcybersecurity.com/ >

[27] Informe sobre metodologías de evaluación de vulnerabilidades de seguridad cibernética, versión 2.0,
Noviembre de 2004, ChemITC, disponible en
< http://www.chemicalcybersecurity.com/ >

[28] Modelo de referencia de la arquitectura de seguridad cibernética, versión 1.0, agosto de 2004, ChemITC, disponible en < http://www.chemicalcybersecurity.com/ >

[29] Informe sobre la evaluación de las herramientas y métodos de autoevaluación de ciberseguridad, Noviembre de 2004, ChemITC, disponible en < http://www.chemicalcybersecurity.com/ > [30] Estrategia de seguridad cibernética del sector químico estadounidense, septiembre de 2006, disponible en
< http://www.chemicalcybersecurity.com/ >

Otros documentos y recursos publicados:

[31] Carlson, Tom, *Information Security Management: Understanding ISO 17799* , 2001, disponible en < http://www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf >

[32] Purdue Research Foundation, un modelo de referencia para la fabricación integrada por computadora, 1989, ISBN 1-55617-225-7

[33] Publicación especial NIST 800-30, *Guía de gestión de riesgos para sistemas de tecnología de la información* , julio de 2002

[34] Publicación especial NIST 800-37, *Guía para la Certificación de Seguridad y Acreditación de Sistemas de Información Federal* , mayo de 2004

[35] Publicación especial NIST 800-55, *Guía de métricas de seguridad para sistemas de tecnología de la información* , julio de 2003

[36] Publicación especial NIST 800-61, *Guía de manejo de incidentes de seguridad informática* , enero de 2004

[37] Publicación especial NIST 800-82, *Guía de control de supervisión y adquisición de datos (SCADA) y seguridad del sistema de control industrial* , marzo de 2006, borrador

[38] Foro de requisitos de seguridad de control de procesos NIST (PCSRF), Sistema de control industrial - Perfil de protección del sistema (ICS-SPP)

[39] Instituto de Ingeniería de Software Carnegie Mellon, *Integración del Modelo de Madurez de Capacidades (CMMI) para Ingeniería de Software* , v1.1, agosto de 2002

Sitios web:

[40] NASA / Oficina de Ciencia de Normas y Tecnología (NOST), disponible en < http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html >

[41] Modelo de referencia empresarial de Zachmann, disponible en < http://www.zifa.com/ >

[42] Sarbanes - Sitio web de Oxley, disponible en < http://www.sarbanes-oxley.com/ >

[43] Sitio web de Sans, disponible en < http://www.sans.org/ >

[44] Instituto de Capacitación MIS, disponible en < http://www.misti.com/ >

[45] Instituto Nacional de Normas y Tecnología de EE . UU., Disponible en < http://www.nist.gov/ >

[46] Programas de auditoría de tecnología de sistemas de información, disponibles en < http://www.auditnet.org/asapind.htm >

[47] NIST eScan Security Assessment, disponible en < https://www.mepcenters.nist.gov/escan/ >

[48] American National Standards Institute, disponible en < http://www.ansi.org/ >

[49] Modelo IDEAL, disponible en < http://www.sei.cmu.edu/ideal/ideal.html >

[50] Objetivos de control de la información y la tecnología relacionada (COBIT), disponible en < http://www.isaca.org/ >

[51] Grupo de trabajo sobre gobierno corporativo “Gobierno de seguridad de la información: un llamado a la acción”, disponible en < http://www.cyberpartnership.org/InfoSecGov4_04.pdf >

[52] Definiciones de ciberseguridad del estado de Michigan, disponibles en < http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html >

[53] The Free Internet Encyclopedia - Wikipedia, disponible en < http://www.wikipedia.org/ >

[54] Glosario de Bridgefield Group, disponible en < http://www.bridgefieldgroup.com/ >

[55] Información Six Sigma, disponible en < http://www.onesixsigma.com/ >

[56] Instituto de Ingeniería de Software Carnegie Mellon, disponible en < http://www.sei.cmu.edu/ >

[57] Instituto de Ingeniería de Software Carnegie Mellon, Equipo de Respuesta a Emergencias Informáticas (CERT), disponible en < http://www.cert.org/ >

[58] SCADA y Proyecto de Adquisición de Sistemas de Control, disponible en
< http://www.msisac.org/scada/ >

[59] Centro de intercambio de información sobre interoperabilidad, disponible en < http://www.ichnet.org/ >

[60] Terminología financiera del estado de Nueva York, disponible en
< http://www.budget.state.ny.us/citizen/financial/glossary_all.html >

[61] Busque Seguridad de Windows, disponible en < http://www.searchwindowssecurity.com/ >

[62] Programa de seguridad cibernética del sector químico, disponible en
< http://www.chemicalcybersecurity.com/ >

[63] TechEncyclopedia, disponible en < http://www.techweb.com/encyclopedia/ >