SISTEMAS DE CONTROL INDUSTRIAL

Índice

Lista de figuras

1.0 ALCANCE

Esta ficha técnica contiene recomendaciones para la prevención de siniestros relacionados con los sistemas de control industrial (SCI). Utilizando un enfoque basado en sistemas, se evalúan todos los SCI de la planta, incluidas sus redes de comunicación, y los ciberriesgos. El objetivo de este documento es facilitar soluciones que reduzcan los riesgos desde el punto de vista de la protección de los bienes y la continuidad del negocio.

A efectos del presente documento, los SCI se definen como la combinación de sistemas de hardware y programas de software que controlan, protegen y supervisan los procesos, la producción, la fabricación y las actividades relacionadas, tanto en plantas industriales como no industriales. La siguiente lista, que no es exhaustiva, ofrece ejemplos de activos de hardware que podrían conectarse a la red de los SCI:

- sistema de supervisión, control y adquisición de datos (SCADA);
- sistemas de control distribuido (DCS), incluidos los sistemas para el almacenamiento de datos históricos;
- controladores lógicos programables (PLC);
- controladores de automatización programables;
- pasarela de dispositivos externos;
- unidad terminal remota (RTU);
- dispositivos de redes, incluidos conmutadores, cortafuegos, enrutadores, etc.;
- dispositivos de campo inteligentes (p. ej., medidores inteligentes, válvulas, relés y transmisores de procesos);
- bus de instrumentos;
- interfaces de usuario;
- estación de trabajo de ingeniería;
- paneles de control industrial, incluidos armarios de equipos e instrumentos, armarios de entrada/salida (E/S), etc.;
- sistema de automatización o gestión de edificios;
- dispositivos inteligentes o Internet de las cosas industrial (IIoT).

Esta ficha técnica contiene directrices generales sobre los SCI. En caso de haber fichas técnicas más detalladas para equipos o procesos específicos, estas prevalecerán sobre cualquier directriz incluida en el presente documento.

Esta ficha técnica no aborda lo siguiente:

- el diseño y el funcionamiento detallados de equipos, comunicaciones y redes de los SCI;
- el rendimiento, la compatibilidad y la funcionalidad del software;
- el diseño, el funcionamiento, las inspecciones, las pruebas y el mantenimiento de sistemas instrumentados de seguridad (véase la ficha técnica 7-45, *Safety Controls, Alarms, and Interlocks*);
- los sistemas informáticos empleados en actividades corporativas generales (p. ej., sistemas de envío o recepción de correos electrónicos, sistemas con acceso a Internet).

1.1 Riesgos

Si los SCI no se gestionan y mantienen correctamente, los errores de funcionamiento leves podrían transformarse en averías graves, lo que afectaría a la producción y podría llegar a provocar daños materiales graves. Existen numerosos factores que pueden contribuir al fallo de los sistemas de control, tales como actos cibernéticos destinados a interrumpir los procesos o la falta de un plan de respuesta y recuperación tras un incidente de ciberseguridad.

1.2 Cambios

Julio de 2024. Revisión parcial. Se llevaron a cabo cambios de redacción.

2.0 RECOMENDACIONES PARA LA PREVENCIÓN DE DAÑOS Y PÉRDIDAS

2.1 Introducción

Los SCI funcionan de manera diferente dependiendo de la industria en la que se utilicen, por lo que dos SCI nunca serán iguales. Los SCI son sistemas complejos formados por controladores, controladores lógicos, motores, bombas, accionadores, dispositivos de supervisión y detección y otros elementos, conectados mediante redes de comunicación.

Garantizar que el personal responsable de los SCI de la planta comprenda por completo el sistema general y los requisitos operativos y de protección, así como las necesidades de las redes de comunicación y el software, es fundamental para determinar colectivamente los riesgos relacionados con los SCI de la planta.

2.2 Construcción y ubicación

2.2.1 Ubique las salas de control de procesos y las salas de equipos relacionados relevantes fuera de zonas expuestas a riesgos de explosión. Si esto no fuese posible, habilite una construcción resistente a la presión diseñada de acuerdo con la ficha técnica 1-44, *Damage-Limiting Construction*, asumiendo que el exceso de presión se aplica en la superficie exterior de la sala de control. Se recomienda instalar en las ventanas vidrio laminado que cumpla con la norma ANSI Z97.1 (otras opciones aceptables son las normas ASTM E1886 y E1996, o FBC TAS 201 y 203), sobre la resistencia contra impactos, y la norma ASTM E1300, sobre el exceso de presión requerido.

2.2.2 Ubique las salas de control de procesos y las salas de equipos relacionados de modo que no estén expuestas a daños provocados por líquidos que arden, líquidos corrosivos, vapores inflamables o equipos mecánicos, tales como grúas.

2.2.3 En las salas de control de procesos y las salas de equipos relacionados que estén elevadas y expuestas a riesgo de incendio, instale protección ignífuga adecuada para el riesgo (de una hora, como mínimo) para el acero de soporte estructural.

2.2.4 Construya las salas de control de procesos, los centros de control y las salas de los equipos e instrumentos de control industrial asociados (como las salas de entrada/salida), así como los paneles de control industriales con materiales no combustibles. Esta construcción incluye, entre otros elementos, los falsos techos, falsos suelos, tabiques, muebles, materiales de aislamiento de tuberías y sistemas de climatización y filtros de climatización.

Si se utilizan materiales de plástico, instale materiales homologados por FM o que hayan superado pruebas para cumplir con las especificaciones de uso de acuerdo con las siguientes directrices:

A. norma de homologación de FM Approvals 4882, *Class 1 Interior Wall and Ceiling Materials or Systems for Smoke Sensitive Occupancies;*

B. norma de homologación de FM Approvals 4884, *Panels Used in Data Processing Center Hot and Cold Aisle Containment Systems;*

C. norma ANSI/4910 de FM Approvals, *Cleanroom Materials Flammability Test Protocol*.

2.2.5 Instale una separación con una resistencia al fuego mínima de una hora entre las salas de control de procesos y las zonas contiguas, incluidas las salas de los equipos y las salas de los equipos de distribución de baja tensión. Esta recomendación no se aplica a los equipos independientes ubicados fuera de la sala de control de procesos.

2.2.6 Siempre que haya sistemas de control de procesos redundantes, ubique los controles, equipos y cables de cada sistema en una zona resistente al fuego independiente.

2.2.7 Habilite zonas independientes para los vestuarios, comedores, cocinas, salas de reuniones, oficinas, etc.

2.2.8 Selle las aberturas de los suelos y paredes resistentes al fuego que sirven como paso para tuberías y cables con un sellante homologado por FM o por otro organismo cuya resistencia al fuego sea equivalente a la del suelo o la pared.

2.2.9 Dirija los desagües de la cubierta, los conductos de agua para uso doméstico y otros conductos de líquidos alrededor de las salas de control de procesos y las salas de equipos relacionados. En edificios con varias plantas, selle el piso superior de modo que sea estanco. Si no es posible desviar las tuberías de estas zonas, instale un sistema de contención (p. ej., tuberías concéntricas) o un recipiente de recogida; es instale un sistema de detección de fugas homologado por FM cuya alarma se transmita a una ubicación con presencia constante de personal. Consulte información adicional en la ficha técnica 1-24, *Protection Against Liquid Damage*.

2.2.10 Instale desagües de suelo debajo de los falsos suelos en caso de que pueda acumularse agua u otros líquidos.

2.2.11 Construya los paneles de control industrial, incluidas las puertas y los paneles de acceso, con materiales de construcción no combustibles. Respete las normativas internacionales vigentes.

2.3 Protección

2.3.1 Proteja las salas de control de procesos, las salas de equipos relacionados y los paneles de control industrial contra el riesgo de incendio de acuerdo con la ficha técnica 1-20, *Protection Against Exterior Fire Exposure*.

2.3.2 Instale un sistema de detección de humo homologado por FM en las salas de control de procesos, los centros de control de procesos y las salas de los equipos asociados de forma que envíe una alarma a una estación de trabajo o ubicación con presencia constante de personal.

2.3.3 Allí donde se desee contar con un nivel superior de detección, debido a la presencia de sistemas estratégicos para las actividades o de sistemas de seguridad, instale un sistema de detección de incendios de alerta muy temprana en la sala de los equipos o bien dentro del cuadro de mando industrial que envíe la alarma a una ubicación con atención constante de personal. Utilice sistemas de detección de incendios de alerta muy temprana por aspiración de aire o de detección puntual inteligente y de alta sensibilidad homologados por FM apropiados para la configuración del recinto.

2.3.4 Instale sistemas de detección de humo homologados por FM debajo de los falsos suelos y sobre las zonas del techo en las que haya cables.

2.3.5 Instale un sistema de detección de incendios de acuerdo con la ficha técnica 5-48, *Automatic Fire Detection*.

2.3.6 Habilite protección contra incendios en las salas de control de procesos, los centros de control o las salas de los equipos e instrumentos de control industrial de la siguiente manera:

2.3.6.1 Salas de construcción combustible

A. Instale un sistema de rociadores automáticos de tubería húmeda o de acción previa con rociadores automáticos de respuesta rápida. Use las demandas de diseño, las demandas para mangueras y la duración del suministro estipuladas en la ficha técnica 3-26, *Protección contra incendios para actividad sin almacenamiento*.

B. Instale un sistema automático de protección por agua nebulizada homologado por FM diseñado específicamente para salas de equipos de tratamiento de datos de acuerdo con la ficha técnica 4-2, *Water Mist Systems*, y las directrices de diseño, instalación, uso y mantenimiento del fabricante que se incluyen en el documento de homologación de FM Approvals. Habilite un suministro de agua para el sistema de protección por agua nebulizada con una duración de 60 minutos.

Para los puntos A y B anteriores:

- Utilice la categoría de riesgo 1 (HC-1) para las salas de control de procesos y los centros de control con techos de hasta 9 m (30 ft) de altura.
- Utilice la categoría de riesgo 2 (HC-2) para las salas de equipos de instrumentación de control industrial o salas de control de procesos y centros de control con techos de más de 9 m (30 ft) de altura.

2.3.6.2 Salas de construcción no combustible

Habilite un sistema de extinción de incendios de halocarburos o gas inerte (agente limpio) diseñado e instalado de acuerdo con las instrucciones del fabricante y la ficha técnica 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*. Los sistemas de rociadores automáticos de tubería húmeda o de acción previa o los de agua nebulizada también son aceptables, de acuerdo con la sección 2.3.6.1 de esta ficha técnica.

En cuanto a los sistemas de extinción de incendios de halocarburos o gas inerte (agente limpio), garantice que se cumplen las siguientes condiciones:

1. El sistema de detección de incendios de alerta muy temprana corta automáticamente la alimentación de la sala y los equipos (excepto las luces de emergencia) al detectarse humo, siempre y cuando un análisis de riesgos en procesos o una evaluación equivalente demuestre que el corte de la alimentación no produce daños en los equipos controlados (es decir, los equipos de proceso) ni crea ningún riesgo.
   a. En caso de instalar sistemas de corte automático de la alimentación eléctrica, hágalo de acuerdo con las directrices sobre el aislamiento de la corriente de los equipos de tratamiento de datos y sistemas de climatización de la ficha técnica 5-32.
   b. Ajuste el tiempo de retardo del corte de la alimentación de modo que no supere el tiempo de retención del sistema de extinción de incendios de halocarburos o gas inerte (agente limpio) con un factor de seguridad de dos a fin de llevar el proceso hasta un estado seguro.
2. Disponer de un sistema de detección de incendios de alerta muy temprana con una señal de supervisión que deje el tiempo suficiente para que el operador o el personal de respuesta investigue la causa antes de la descarga del sistema de agente limpio.
3. Asegurarse de que los cerramientos de los equipos estén hechos de metal.
4. Reducir al mínimo el uso de papel y otros materiales combustibles en la sala.
5. No almacenar materiales de embalaje ni cartuchos de plástico en la sala. **Nota:** Este requisito incluye todos los medios combustibles (como las cintas de carrete).
6. Se ha instalado un sistema de parada o de compuerta en los sistemas de ventilación que reponen o hacen recircular aire.

2.3.7 Habilite un sistema de protección para los equipos de control de procesos de la planta. Base esta protección en la importancia del proceso físico y el impacto que podría tener un siniestro del sistema de control de procesos debido a un incendio. Consulte en la sección 3.1 Protección contra incendios de los equipos de control industrial. Instale una de las siguientes opciones (A o B):

A. armarios no combustibles con subdivisiones para limitar los daños a la sección más pequeña posible;

B. un sistema de extinción de incendios de halocarburo o gas inerte (agente limpio), siempre y cuando los armarios estén ventilados o el sistema esté dispuesto de tal modo que descargue directamente en el interior de los armarios. Siga las directrices de la sección 2.3.6.2 de esta ficha técnica.

2.3.8 Instale protección por rociadores automáticos de acuerdo con la ficha técnica 3-26, *Protección contra incendios para actividades sin almacenamiento*, en todos los espacios del edificio contiguos a las salas y centros de control (incluidos, entre otros, las oficinas, las zonas de descanso, las salas de archivos, las zonas de permisos, las salas de conferencias y de formación o los cuartos de baño), de acuerdo con la clasificación de riesgo adecuada asociada con esta actividad.

2.3.9 Instale sistemas de protección contra incendios de acuerdo con la ficha técnica 2-0, *Directrices para la instalación de rociadores automáticos*, y la ficha técnica que sea de aplicación al sistema de protección especial.

2.3.10 Proteja los centros de datos relacionados con las salas de control de procesos de acuerdo con la ficha técnica 5-32, *Data Centers and Related Facilities*. Efectúe un análisis de riesgos en procesos de los controles antes de habilitar la parada automática.

2.3.11 Proteja los grupos electrógenos de acuerdo con la ficha técnica 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.3.12 Proteja los grupos de cables y las bandejas de cables de acuerdo con la ficha técnica 5-31, *Cables and Bus Bars*.

2.3.13 A fin de proteger los equipos electrónicos, habilite extintores portátiles de dióxido de carbono o agentes limpios (clase C) indicados para riesgos eléctricos sometidos a tensión de acuerdo con la ficha técnica 4-5, *Portable Fire Extinguishers*.

2.3.13.1 No use extintores químicos secos en zonas que alberguen equipos electrónicos.

2.3.13.2 Para materiales combustibles ordinarios, instale extintores portátiles del tipo o la combinación de tipos adecuados que corresponda de acuerdo con la ficha técnica 4-5, *Portable Extinguishers*.

2.3.14 Desarrolle un plan de coordinación con el cuerpo de bomberos para responder ante un incendio o una emergencia eléctrica en las salas de control de procesos, los centros de control, las salas de los equipos e instrumentos de control industrial asociados y los paneles de control industrial.

2.3.14.1 Verifique que el personal de mantenimiento eléctrico sea capaz de responder al mismo tiempo que el personal de lucha contra incendios y que cuente con la formación para cortar la electricidad o aislar de forma segura los paneles de control de procesos afectados y emprender las actividades de lucha contra incendios.

2.3.14.2 Cuando no resulte práctico cortar la electricidad de todos los equipos eléctricos de las salas de equipos e instrumentos de control industrial y los paneles de control industrial, asegúrese de que la respuesta a la notificación de la alarma de incendio involucre a personal formado que sea capaz de diagnosticar el estado del fuego y humo de la zona afectada e implantar el plan de coordinación con el cuerpo de bomberos a fin de aislar manualmente estos equipos de la corriente de manera puntual, parcial o completa.

2.4 Factor humano

2.4.1 Programa de gestión de cambios

2.4.1.1 Administre los programas de gestión y seguridad de los SCI junto con el programa de gestión de cambios.

2.4.2 Gestión de los SCI

Para que los programas de supervisión y gestión de los SCI tengan éxito, es fundamental el compromiso de la dirección. Un compromiso firme de la dirección contribuye a que todos los aspectos relativos a los SCI reciban la atención, la financiación y la dotación de personal necesarios.

2.4.2.1 Equipo de supervisión de los SCI

2.4.2.1.1 Las organizaciones deberían crear un equipo de supervisión de los SCI conformado por personal de los niveles corporativo y local que se encargue de supervisar la implementación de las políticas de ciberseguridad relacionadas con los SCI.

2.4.2.2 Programa de gestión de activos

2.4.2.2.1 Establezca y ponga en marcha un programa de inspección, pruebas y mantenimiento de los SCI. Consulte directrices para desarrollar un programa de integridad de activos en la ficha técnica 9-0, *Asset Integrity*. Incluya los siguientes elementos en un programa de gestión de activos, cuando corresponda:

A. Mantenga un inventario de los sistemas de hardware que estén conectados a la red de SCI que incluya el fabricante, el número de modelo y el firmware, software y aplicaciones instalados, incluidos los números de las versiones.

B. Asegúrese de que el inventario incluya una evaluación de la importancia de los activos de los SCI a fin de priorizar las labores de seguridad y disponer de las actualizaciones de seguridad pertinentes.

C. Guarde los planos y la documentación de los SCI (p. ej., esquemas eléctricos y de control, planos de las redes y, cuando sea pertinente, diagramas de las tuberías y la instrumentación). Mantenga actualizados estos documentos a medida que se modifiquen los SCI.

D. Guarde en una ubicación controlada y restringida el inventario de activos, los planos y los documentos que detallen el diseño y el funcionamiento de los SCI. Otorgue acceso solamente en la medida en que sea necesario. Si dichos documentos fueran digitales, protéjalos con contraseña, haga copias de seguridad y almacénelas en una red segura. Estos archivos deberían cifrarse cuando sea posible. Todas las redes que estén fuera del entorno de los SCI y la red operativa deben considerarse como inseguras, incluida la red informática local.

2.4.2.3 Programa de gestión de la cadena de suministro

2.4.2.3.1 Incluya los siguientes elementos en un programa de gestión de la cadena de suministro, cuando corresponda:

A. Introduzca requisitos de ciberseguridad para los sistemas, las aplicaciones o los dispositivos dentro de la documentación de licitaciones para los proveedores. Antes de firmar o renovar ningún contrato, vuelva a evaluar las políticas y los procedimientos de seguridad de los proveedores que disponen de acceso a la planta, incluidos los proveedores de servicios externos.

2.4.3 Seguridad de los SCI

La disponibilidad de los SCI es fundamental en cualquier proceso. Una estrategia de seguridad de los SCI efectiva puede desempeñar una función esencial en el mantenimiento de dicha disponibilidad.

2.4.3.1 Programa de gestión de los accesos

2.4.3.1.1 Incluya los siguientes elementos en un programa de gestión de los accesos, cuando corresponda:

A. Utilice las credenciales de los SCI para controlar el acceso a estos sistemas (es decir, dar acceso a las estaciones de operador o interfaces de usuario y estaciones de ingeniería en función de los permisos asignados). Asimismo, limite el acceso a las estaciones de ingeniería a aquellas personas que tengan la autoridad para cambiar el proceso. Para respaldar el acceso controlado a los SCI, respete las siguientes recomendaciones:

1. Las estaciones de operador o interfaces de usuario (que no tengan capacidad para modificar los puntos de ajuste de las alarmas ni de los enclavamientos de los dispositivos de seguridad) pueden usar credenciales de acceso compartidas.
2. Las estaciones de ingeniería requieren utilizar unas credenciales de usuario y contraseña únicas siempre que se acceda al sistema y establecer un cierre de sesión automático cuando la estación esté inactiva durante un periodo de aproximadamente 30 minutos o menos.
3. Las credenciales empleadas para acceder a los SCI se gestionan de manera independiente de las utilizadas para acceder a los sistemas informáticos Las credenciales de los usuarios de los SCI deberían guardarse en un repositorio de usuarios actualizado en el entorno de la red operativa. Además, los permisos de acceso deberían revisarse periódicamente y se debería eliminar el acceso de las personas que ya no lo necesitan. Otra opción aceptable sería utilizar credenciales de acceso locales, no conectadas a la red.

B. Cambie el nombre de usuario y la contraseña que vienen por defecto en todos los sistemas, dispositivos de hardware y programas de software. Actualice las contraseñas de manera periódica o cuando se produzcan cambios significativos o cruciales en el personal o los proveedores. Evite usar nombres de usuario genéricos y contraseñas poco seguras.

C. Proteja las comunicaciones inalámbricas mediante autenticación y cifrado.

D. Adopte las siguientes precauciones al conectar dispositivos portátiles a los SCI:

1. Antes de permitir su acceso a la planta, se debería facilitar formación sobre la ciberseguridad de los SCI a los contratistas y otras personas que visiten la planta temporalmente, en la que debería incluirse la familiarización con las reglas y los procedimientos de la planta de acuerdo con las partes D.2 a D.5 de la sección 2.4.3.1.1.
2. Para los dispositivos que se empleen en el entorno de los SCI, como ordenadores portátiles, tabletas, etc. (incluidos los de personal externo), se deberían desactivar las conexiones inalámbricas, mantener los parches de seguridad y programas antivirus y comprobar si hay otros más recientes y verificar mediante análisis la presencia de virus siempre que se vaya a conectar un dispositivo a los SCI.

3. Para tarjetas de memoria, dispositivos de memoria USB, discos duros portátiles, etc., lleve a cabo un análisis de seguridad siempre que se vayan a conectar a los SCI.
4. No conecte teléfonos móviles ni otros dispositivos con acceso a la red móvil a los SCI.
5. Desactive siempre que sea posible los puertos (USB, RJ45, en serie, etc.) de los equipos conectados a los SCI que no se utilicen.

2.4.3.2 Programa de gestión de configuración

2.4.3.2.1 Incluya los siguientes elementos en un programa de gestión de la configuración, cuando corresponda:

A. Limite las características y las funciones de todos los dispositivos digitales conectados a los SCI solo a las necesarias para el funcionamiento de los SCI. Esto incluye los dispositivos de campo que tengan múltiples configuraciones y se comuniquen digitalmente; los controladores que efectúen tanto controles de procesos básicos como de seguridad; los dispositivos de supervisión, las interfaces de usuario y las estaciones de ingeniería; los sistemas para el almacenamiento de datos históricos; los servidores; los equipos de conexión en red como las pasarelas, los conmutadores y los enrutadores; y equipos de protección de redes como los cortafuegos, incluidos todos los dispositivos instalados en el interior de la red perimetral de los SCI.

B. Antes de la implantación de modificaciones en cualquier dispositivo digital conectado a los SCI, compruebe que, como parte del programa de gestión de cambios, el equipo de supervisión de los SCI haya analizado, validado y aprobado los posibles efectos sobre la seguridad.

C. Utilice la supervisión de sistemas para comprobar que no se produzcan cambios no autorizados en los equipos de control básicos, los equipos de control de seguridad y los equipos de la red operativa.

D. Antes de activar un sistema de seguridad y de operar los SCI, asegúrese de que los controladores lógicos, PLC y controladores que formen parte del sistema de control de procesos básicos y del sistema de seguridad tengan seleccionado el modo de funcionamiento recomendado por el fabricante (es decir, en funcionamiento, programado, remoto, etc.). Incluya las modificaciones al modo de funcionamiento incluidas en la recomendación anterior relativa a la supervisión de los sistemas.

2.4.3.3 Programa de gestión de instalación de parches

2.4.3.3.1 Incluya los siguientes elementos en un programa de gestión de instalación de parches, cuando corresponda:

A. Asegúrese de que el programa de gestión de parches incluya equipos de soporte y comunicación como, entre otros, servidores de salto, sistemas para el almacenamiento de datos históricos, protección antivirus, redes privadas virtuales y otros componentes de conexión en red, incluidos los cortafuegos. Incluya también todos los equipos que se empleen en el mantenimiento de los SCI, como ordenadores portátiles o dispositivos de mano, así como equipos de escaneo que se usen para comprobar dispositivos portátiles, como terminales de USB, etc.

B. Debería estarse al corriente de posibles vulnerabilidades de ciberseguridad mediante la consulta de los boletines y las alertas de los fabricantes de los sistemas y dispositivos, los integradores de los SCI, organismos gubernamentales, etc.

C. Al recibir una notificación de ciberseguridad, haga que el equipo de supervisión de los SCI determine las medidas necesarias para proteger a los SCI de la planta en función de su importancia y el riesgo. Puede que sea necesario tomar medidas de protección adicionales contra vulnerabilidades del sistema hasta que pueda instalarse un parche de software.

D. Verifique que el equipo de supervisión de los SCI consulta a los proveedores de los SCI antes de instalar los parches. En la medida de lo posible, pruébelo en una simulación o un sistema virtual antes de la instalación.

E. Habilite medidas de protección adicionales para los equipos o el software obsoletos contra vulnerabilidades de ciberseguridad para los que el fabricante ya no facilite asistencia.

2.4.3.4 Sistemas de seguridad de redes

2.4.3.4.1 Establezca un acceso remoto seguro al entorno de la red operativa y los SCI. Todas las redes que estén fuera del entorno de los SCI y la red operativa deben considerarse como inseguras, incluida la red informática local. Ponga en marcha las siguientes precauciones, cuando corresponda:

A. Verifique el acceso remoto a los SCI de la siguiente manera:

1. Desde una red interna (cuya conexión se inicie en la red corporativa), como la red informática local, use autenticación de varios factores a través de un servidor de salto ubicado en una red perimetral industrial (consulte la sección 2.4.3.4.2 B).
2. Desde una red externa (cuya conexión se inicie fuera de la red corporativa), use una red privada virtual (VPN) segura y autenticación de varios factores a través de una ruta exclusiva para ello usando los sistemas corporativos hasta un sistema intermedio (huésped de salto de la red perimetral industrial) antes de acceder al entorno de los SCI y las tecnologías operativas.
3. Asegúrese de que no se utilicen ordenadores personales ni otros dispositivos personales externos para acceder remotamente al entorno de los SCI y la red operativa.

B. No permita conexiones remotas a los sistemas de seguridad dedicados.

C. No permita conexiones remotas persistentes en el entorno de los SCI y la red operativa. La supervisión a distancia, la recopilación de datos y los diagnósticos con flujo de datos restringido en una dirección son adecuados y no es necesario establecer límites de tiempo en su conexión a los SCI.

D. Sustituya los módems telefónicos por métodos de comunicación modernos y seguros. Si esto no resulta posible, realice las siguientes acciones:

1. Apague o desenchufe los módems telefónicos cuando no estén en uso.
2. Habilite medidas de protección adicionales para los módems telefónicos activos (p. ej., configurar la devolución de la llamada a un número telefónico determinado, filtrar la identidad de las llamadas entrantes, desactivar las respuestas automáticas).

2.4.3.4.2 Establezca las siguientes medidas de protección de redes, cuando corresponda:

A. Separe con una red perimetral industrial las redes de los sistemas de control industrial y operativas de las redes de tecnologías de la información u otras redes corporativas y dirija todas las comunicaciones hacia y desde los SCI a través de dicha red perimetral.

B. Habilite una separación entre la red del sistema básico de control de procesos y la de seguridad mediante segregación (arquitectura *air-gapped* o de interfaces) o segmentación (arquitectura integrada o común). Consulte directrices adicionales sobre los sistemas de seguridad en la ficha técnica 7-45, *Safety Controls, Alarms, and Interlocks*.

C. Verifique que las reglas del cortafuegos (puertos abiertos, protocolos permitidos, etc.) se revisen periódicamente por personal con experiencia en redes y ciberseguridad. Los cambios en las reglas del cortafuegos deberían implantarse desde el entorno de los SCI y la red operativa y gestionarse mediante un programa de gestión de cambios bajo la dirección del equipo de supervisión de los SCI.

D. Elabore ″listas blancas″ de las aplicaciones del entorno de los SCI siempre que sea posible. Implante esta solución con cautela.

E. Supervise las redes de los SCI y registre las actividades de estas (es decir, utilice un sistema de detección de intrusiones), utilizando un software de gestión de eventos e información de seguridad siempre que sea posible para detectar actividades no autorizadas. Cuando sea posible, supervise el entorno de la red operativa desde un centro de seguridad de operaciones.

F. Utilice programas antivirus de protección en el entorno de los SCI y la red operativa, incluidos los sistemas de supervisión, control y adquisición de datos (SCADA). Se debería colaborar con el vendedor o proveedor de servicios de los SCI y decidir cuidadosamente la selección y el establecimiento de soluciones antivirus.

2.5 Operación y mantenimiento

Es esencial tener certeza de que los SCI funcionan según lo previsto para evitar que se produzcan daños importantes a los equipos y bienes que puedan resultar en paradas largas. La posibilidad de que se produzcan fallos e interrupciones duraderas relacionados con los SCI puede minimizarse mediante procedimientos de supervisión y notificación, así como planes viables de respuesta y recuperación ante emergencias y de contingencia de los SCI, y operadores que cuenten con la formación y los conocimientos necesarios y que sigan procedimientos de funcionamiento generales y de emergencia documentados.

2.5.1 Funcionamiento de los SCI

2.5.1.1 Programa de gestión de alarmas

2.5.1.1.1 Incluya la supervisión de los sistemas de los equipos de los SCI y de las redes operativas, siempre que esto sea posible de acuerdo con la recomendación de gestión de la configuración 2.4.3.2.1 C:

A. Mediante la supervisión de los sistemas, disponga que se dispare una alerta si se produce un cambio no autorizado en la configuración de los equipos de los SCI, incluidos los sistemas de seguridad y los equipos de la red operativa.

Nota: Las alertas indicadas anteriormente no deberían ser gestionadas por los operadores de proceso, sino que deberían hacerse llegar al personal responsable de supervisar los equipos de las redes operativas y de los SCI.

Consulte directrices adicionales sobre la gestión de alarmas en la ficha técnica 10-8, *Operators*.

2.5.1.2 Procedimientos operativos en caso de emergencia

2.5.1.2.1 La planificación y la preparación son fundamentales para que un procedimiento de actuación en caso de emergencia cibernética o relativa a los SCI tenga éxito. Esto incluye identificar a los trabajadores y, si fuera necesario, consultores u otros especialistas externos que cuentan con las habilidades necesarias para responder ante una ciberintrusión.

A. Verifique que se hayan establecido funciones y responsabilidades para gestionar los ciberincidentes.

B. Guarde la información sobre qué proveedores tienen autorización o están obligados contractualmente a facilitar asistencia durante un incidente cibernético.

2.5.1.2.2 Incluya los siguientes elementos en el procedimiento de actuación en caso de emergencia cibernética o relativa a los SCI, cuando corresponda:

A. Asegúrese de que se disponga de un procedimiento para mitigar el impacto sobre los SCI y la producción en caso de siniestro de un sistema de planificación de recursos empresariales (ERP) o un sistema de ejecución de fabricación (MES).

B. Asegúrese de que se hayan facilitado directrices sobre cómo detener el sistema o proceso (es decir, llevarlo hasta un estado seguro) cuando el comportamiento del sistema de control de los SCI sea sospechoso o deje de funcionar. Estas deberían contemplar ciberincidentes conocidos o sospechados, incluidos, entre otros, los siguientes:

- la congelación o el apagado de la pantalla de una estación de operador;
- un disparo inexplicable de la unidad;
- la aparición de mensajes de ransomware en las estaciones de operador;
- el movimiento inesperado de los cursores en las estaciones de operador sin la orden del operador;
- un cambio no reconocido de las configuraciones;
- problemas a la hora de configurar o calibrar parte de los SCI.

C. Compruebe que existan procedimientos para accionar los equipos estratégicos en modo manual.

D. Verifique que los procedimientos de actuación en caso de emergencia se practiquen (como mínimo) en ejercicios de gabinete periódicos.

2.5.1.3 Plan de contingencia

2.5.1.3.1 Plan de contingencia para los equipos

Desarrolle y mantenga un plan de contingencia por escrito para los SCI según lo estipulado en la ficha técnica 9-0, *Integridad de los activos*. Consulte las directrices sobre el proceso de desarrollo y mantenimiento de un plan de contingencia viable para los SCI en el Anexo C de dicha ficha técnica, en la que también se incluyen directrices sobre estrategias de mitigación para equipos de recambio, en alquiler y redundantes.

Asimismo, incluya los siguientes elementos en el plan de contingencia para los SCI:

A. Como parte del programa de respuesta y recuperación ante incidentes, se deberían estudiar las medidas necesarias para gestionar las paradas imprevistas y recuperarse de la parada de un SCI (véase la sección 2.5.1.4).

B. Pruebe y ejercite el plan con la frecuencia que determine el propietario del activo y que sea proporcional a los riesgos.

C. De acuerdo con el inventario de hardware (véase la sección 2.4.2.2.1), y teniendo en cuenta la importancia del componente y los planes de gestión del ciclo de vida, se debería evaluar la necesidad y la envergadura de la dotación de componentes de recambio de los SCI para averías.

2.5.1.3.2 Revise los planes de contingencia de los SCI anualmente.

2.5.1.4 Programa de recuperación tras incidentes

2.5.1.4.1 Incluya los siguientes elementos en un programa de respuesta y recuperación ante incidentes como parte del plan de contingencia de los SCI, cuando corresponda:

A. Determine la causa raíz de cualquier parada imprevista antes de probar a reiniciar los SCI.

B. Cuando se produzca una parada imprevista, mantenga registros electrónicos para su evaluación posterior, siempre que sea posible.

C. Debería mantenerse una copia actualizada y viable de todos los archivos de configuración de los SCI (por ejemplo, la última configuración fiable conocida, la configuración de referencia) y la documentación necesaria para un sistema totalmente funcional. Mantenga un historial de archivos de respaldo en una ubicación con control de accesos.

1. Si las copias de seguridad son archivos inmutables (por ejemplo, de escritura única/muchas lecturas o que no puedan sobrescribirse), entonces:
    a. Almacene los archivos inmutables de las copias de seguridad en un disco de red seguro e independiente de la red donde se originaron los datos.
    b. Cree nuevos archivos de copias de seguridad cuando se produzcan cambios en el sistema y después de una actualización de este.
    c. Deberían crearse nuevos archivos de copias de seguridad antes de que acabe el periodo de retención del último archivo inmutable.
2. Si las copias de seguridad no son archivos inmutables (por ejemplo, si se pueden sobrescribir), entonces:
    a. Almacene al menos una copia de todos los archivos de las copias de seguridad fuera de línea, en una ubicación con control de accesos.
    b. Cree nuevos archivos de copias de seguridad cuando se produzcan cambios en el sistema y después de una actualización de este.

D. Revise los contratos de servicio con los fabricantes y proveedores para identificar cuánto tardarían en entregarse los componentes a fin de determinar la estrategia óptima de recuperación y dotación de piezas de recambio para los equipos.

E. Revise periódicamente el programa de respuesta y recuperación ante incidentes con una frecuencia que sea acorde con el riesgo, pero al menos una vez al año. Actualice el programa según sea necesario para mantener su eficacia.

Consulte directrices adicionales sobre la planificación previa al incidente y la respuesta de recuperación en la ficha técnica 9-1, *Supervision of Property*, la ficha técnica 10-1, *Planes de coordinación con el cuerpo de bomberos y de respuesta ante emergencias*, y la ficha técnica 10-5, *Disaster Recovery Planning*.

Consulte directrices adicionales sobre la investigación de incidentes en la ficha técnica 10-8, *Operators*, y la ficha técnica 7-43, *Process Safety*.

2.6 Formación

2.6.1 Implante un programa de formación y concienciación de las políticas y los procedimientos de seguridad de los SCI como parte del programa de formación de los operadores de la planta. Este programa debería incluir las normas y prácticas recomendadas sobre ciberseguridad de la industria.

2.6.2 Proporcione a los operadores y al personal esencial de la planta que vaya a interactuar con los SCI formación especializada antes de que se les otorgue acceso a los SCI. Imparta formación adicional a los administradores de los sistemas o al personal con niveles de acceso privilegiados o aumentados (es decir, imparta la formación de acuerdo con las funciones) para realizar las tareas de su puesto.

2.6.3 Imparta formación inicial y de actualización sobre la ciberseguridad de los SCI a todos los trabajadores de los SCI de manera continua y con una frecuencia anual.

2.6.4 Imparta formación al personal de respuesta ante emergencias por incendio sobre cómo luchar contra incendios en equipos de control de procesos. Consulte la sección 2.7.1 de la ficha técnica 5-32, *Data Centers and Related Facilities*.

Consulte directrices adicionales sobre los operadores en la ficha técnica 10-8, *Operators*.

2.7 Sistemas de suministro

2.7.1 Instale sistemas de alimentación ininterrumpida (SAI) y sistemas de alimentación de emergencia que permitan a los SCI seguir funcionando hasta que sea posible apagarlos de manera segura. Incluya sistemas SAI en todos los sistemas auxiliares, como los de aire de los instrumentos (cuando se use) y de climatización, que puedan resultar necesarios hasta que se complete el apagado seguro.

2.7.2 Realice actividades de inspección y mantenimiento en los sistemas de suministro y auxiliares de los SCI (p. ej., baterías, sistemas de alimentación ininterrumpida [SAI], grupos electrógenos y climatización) como parte del programa de integridad de activos. Consulte directrices adicionales en la ficha técnica 5-28, *DC Battery Systems*, y la ficha técnica 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.7.3 Siempre que se utilicen controles neumáticos, habilite un sistema fiable de aire para instrumentos (p. ej., un compresor de aire de instrumentos independiente con respaldo N+1 o un receptor de aire diseñado adecuadamente).

2.7.4 Instale un sistema fiable de calefacción, ventilación y aire acondicionado que mantenga las condiciones ambientales necesarias en los espacios que alberguen a los equipos de los SCI para que estos funcionen normalmente. Esta recomendación se centra en los equipos de los SCI considerados como estratégicos para las operaciones.

3.0 FUNDAMENTO DE LAS RECOMENDACIONES

3.1 Protección contra incendios de los equipos de control industrial

Tenga en cuenta que la instalación de protección por rociadores automáticos está destinada principalmente a proteger la estructura de la sala y la actividad contigua. En una sala pequeña, pueden perderse todos los equipos, incluso en un incendio controlado por un sistema de rociadores o de protección por agua nebulizada. Por tanto, los sistemas de extinción de incendios de halocarburos o gas inerte (agente limpio) pueden constituir una mejor opción a fin de proteger los equipos en sí.

En caso de haber un incendio en armarios bien subdivididos que alberguen equipos de control de procesos, este probablemente causaría daños en el armario en el que se haya originado el incendio y daños menores en los contiguos. Por el contrario, se espera que un incendio que se declare en un armario que albergue equipos de control de procesos y que no disponga de subdivisiones afecte al recinto en toda su longitud. El impacto del siniestro de los equipos de control de procesos depende de la gravedad de los daños por fuego, la importancia del proceso, la disponibilidad de repuestos, etc.

3.2 Gestión de los SCI

El propietario de los activos o el individuo identificado deberían disponer de una estrategia de ciberseguridad que proteja todos los SCI de la planta.

3.2.1 Supervisión de los SCI

Además de la complejidad de la automatización, la interconexión de diferentes sistemas y redes y la recopilación de datos con fines analíticos y empresariales, los SCI se ven afectados por una nueva amenaza: los ciberriesgos. Para que el proceso de la planta siga funcionando, los SCI necesitan que se haya identificado a una persona concreta que proteja los SCI frente a los ciberriesgos y comprenda cómo los métodos, productos y sistemas de ciberseguridad pueden afectar a su rendimiento.

3.2.2 Programa de gestión de activos

Para mantener la resiliencia cibernética de los SCI, las organizaciones deben saber qué está conectado a su red. Sin esta información, no podrá identificar los dispositivos que expongan al SCI a ciberriesgos.

Los activos que deben formar parte del programa de gestión de activos son los dispositivos digitales que están conectados a la red de los SCI. Contemple la posibilidad de incluir las estaciones de operador, las estaciones de trabajo de ingeniería, los conmutadores de red, los módems, los enrutadores, los cortafuegos, los servidores de aplicaciones, las impresoras, los DCS, los PLC y otros controladores lógicos, y los dispositivos de campo inteligentes conectados en red. Los sistemas operativos (p. ej., los equipos empleados en el nivel 3 del modelo de Purdue de una red operativa) también deberían incluirse en la supervisión de activos. Algunos elementos que se suelen encontrar en este nivel son sistemas para el almacenamiento de datos históricos agregados de la planta, sistemas de planificación de la producción, servidores de alarmas y de otras aplicaciones, servicios informáticos específicos de las operaciones (como DHCP, LDAP o DNS) y servidores de archivos. Además, plantéese incluir dispositivos del Internet de las cosas industrial (IIoT) e incluso dispositivos básicos de Internet de las cosas (IoT) que puedan estar conectados de manera incorrecta a la red de los SCI.

Un buen programa de gestión de activos es capaz de identificar los dispositivos conectados a la red de los SCI. Entre estos se incluyen los controladores lógicos programables, las interfaces de usuario, las estaciones de trabajo de ingeniería, los equipos de redes o los servidores. Es fundamental identificar el firmware, el software y las aplicaciones de todos los dispositivos. Sin esta información complementaria, no es posible determinar las funciones y los servicios disponibles para cada dispositivo, lo que pone a los SCI en situación de vulnerabilidad.

El mercado cuenta con muchos proveedores que ofrecen soluciones automáticas, activas y pasivas, de detección de activos y de mapeo de redes. Siempre que sea posible, se prefiere el uso de soluciones pasivas de detección de activos en lugar de técnicas manuales de gestión de activos.

3.2.3 Programa de gestión de la cadena de suministro

Un buen programa de gestión de la cadena de suministro ayuda a garantizar que los equipos y el software estén configurados de forma segura por los proveedores a fin de cumplir los requisitos de seguridad de la organización.

Antes de instalar cualquier controlador u otro dispositivo digital, software o aplicación en el SCI, la organización debe tener la certeza de que el dispositivo proviene de una cadena de custodia fiable, desde el desarrollador, el fabricante, el proveedor, los procesos de envío y almacenamiento hasta las pruebas de puesta en marcha y aceptación.

3.3 Seguridad de los SCI

3.3.1 Programa de gestión de los accesos

Los puntos de acceso no seguros son unos de los canales de ataque más vulnerables de los SCI, que pueden sufrir ciberintrusiones tanto deliberadas como involuntarias. Los ciberdelincuentes saben que siempre puede accederse remotamente a los SCI y buscarán los puntos de acceso más sencillos para poner en riesgo al sistema. En el peor de los casos, un punto de acceso puede resultar afectado durante un periodo prolongado, lo que permitiría acceder a los SCI a terceros sin autorización, obtener información valiosa sobre estos y los procesos de la planta y disponer del tiempo necesario para planear y lanzar un ciberataque.

3.3.2 Programa de gestión de configuración

En su firmware y software, los dispositivos digitales o electrónicos disponen de muchas opciones y funciones de rendimiento y comunicaciones. Para reducir la superficie que podría verse afectada por un ciberataque, se utiliza el «bastionado» de estos equipos (en función, por ejemplo, de la importancia de los activos o un análisis de ciberriesgos en procesos) para limitar las opciones y funciones de los dispositivos digitales o electrónicos a solo aquellas que sean necesarias para que los SCI funcionen correctamente.

Una vez establecida la configuración deseada y cuando el sistema funcione adecuadamente, dicha configuración debería guardarse como referencia o como última configuración fiable. Esta referencia se usaría para intentar restablecer el sistema en caso de que este se haya visto afectado, ya sea por daños físicos o del firmware o software.

Una vez establecida la configuración de los PLC de seguridad u otros controladores, estos dispositivos deberían ponerse en el modo de funcionamiento recomendado por el fabricante (ejecución, programación, remoto, etc.). Esta configuración, incluidos los ajustes y el modo de funcionamiento, se bloquearía mediante la necesidad de disponer de una llave física o estableciendo una clave digital. Este método respalda el programa de gestión de accesos, al permitir el acceso solamente a aquellas personas que cuenten con permiso para modificar la configuración de seguridad.

Mediante la supervisión de los ajustes de configuración se identificará cuándo se realizan cambios no autorizados en los SCI. Esta supervisión resulta útil para identificar y, en algunos casos prevenir, amenazas internas o externas a los SCI.

3.3.3 Programa de gestión de instalación de parches

La gestión de parches es el proceso de aplicar actualizaciones a software, firmware y controladores para proteger contra vulnerabilidades. Los parches deberían evaluarse para determinar cómo pueden afectar al proceso.

Antes de instalar cualquier parche, autentique y verifique la integridad del software a fin de garantizar que se encuentre en su estado original y no haya sido modificado. El origen del software también es fundamental; antes de descargar cualquier programa de software, debe confirmarse que su origen es de confianza.

Si un parche no ofrece ninguna ventaja de ciberseguridad o rendimiento, puede que no sea necesario. Para instalar los parches en el entorno de los SCI y la red operativa, el propietario de los activos debería colaborar con los proveedores de los SCI.

3.3.4 Sistemas de seguridad de redes

El entorno de los SCI y la redes operativas están más conectados que nunca gracias a avances tecnológicos como Industria 4.0; este incremento en la conectividad, al mismo tiempo, los expone a ciberamenazas que en el pasado no existían.

Desde hace un tiempo, es habitual que los proveedores externos ofrezcan asistencia mediante acceso remoto, algo que resulta un medio de acceso cómodo al entorno de los SCI y la red operativa para los empleados. Las comunicaciones provenientes del exterior y que deseen acceder al entorno de los SCI y la red operativa deberían llevarse a cabo a través de una red privada virtual segura, con autenticación de varios factores a través de una red perimetral, para llegar a un servidor de salto con acceso al entorno de los SCI y la red operativa. Las comunicaciones provenientes del entorno de la empresa y que deseen

acceder al entorno de los SCI y la red operativa deberían usar autenticación de varios factores y atravesar una red perimetral para acabar en un servidor de salto con acceso al entorno de los SCI y la red operativa.

Una red perimetral industrial es una red perimetral que añade una capa adicional de seguridad a la red operativa interna de una organización frente a tráfico no fiable. Una red perimetral es una zona que se encuentra en el límite de una red de confianza y que proporciona recursos accesibles a redes que no son de confianza, como Internet. De esta manera, los recursos que consumen los usuarios de zonas que no son de confianza no pueden acceder a la red que esté considerada como segura. Una red perimetral industrial proporciona servicios que requieren conectividad con los entornos tanto informático como operativo, tales como acceso remoto, gestión de parches y antivirus, sistemas para el almacenamiento de datos históricos o de ejecución de fabricación (MES) y transferencia de archivos.

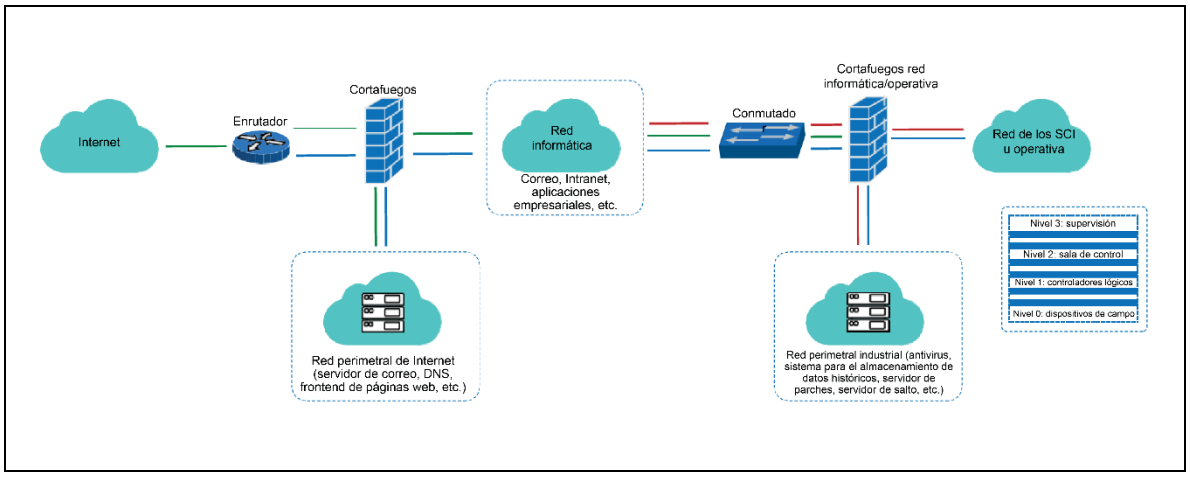

Figura 3.3.4. Ejemplo de ruta de comunicación que muestra la red perimetral corporativa y de Internet y la red perimetral industrial y de los SCI

Los sistemas de detección de intrusiones son una herramienta de seguridad de red que supervisa el tráfico y los dispositivos de red para detectar actividades maliciosas. Las alertas de los SCI deberían transmitirse a un centro de seguridad de las operaciones para efectuar una investigación más detallada.

Los sistemas de detección de intrusiones basados en firmas se centran en la búsqueda de firmas (patrones) para detectar una intrusión. Estas firmas deben actualizarse periódicamente para que sean capaces de identificar los patrones de ataque más novedosos.

Los sistemas de detección de intrusiones basados en anomalías se centran en localizar patrones inesperados de actividad para detectar una intrusión; por ejemplo, un pico en la actividad de la red, varios intentos fallidos de inicio de sesión o actividades inusuales en los puertos de la red que se marcan como sospechosas. Estas alertas se transmiten periódicamente al centro de seguridad de las operaciones.

3.4 Ejemplos de siniestros

3.4.1 Red eléctrica de Ucrania

Malware Crash Override. El 23 de diciembre de 2015, se produjo en Ucrania una de las vulneraciones no autorizadas de un SCI más destacables, cuando varios apagones eléctricos imprevistos afectaron a unos 225.000 clientes. Los apagones fueron causados por ciberintrusiones remotas en tres empresas de distribución eléctrica regionales. Mientras se restauraba el servicio, las operaciones de las empresas afectadas continuaron con limitaciones.

Según se informó, el ciberataque se sincronizó y coordinó después de un exhaustivo reconocimiento de las redes afectadas y algunos informes apuntan a que este ataque se produjo a lo largo de un periodo de seis meses. Los informes indican, además, que los ciberataques que sufrieron las diferentes empresas ocurrieron en intervalos de 30 minutos entre ellos y afectaron a varias plantas. Durante el suceso, múltiples atacantes externos accionaron varios disyuntores de manera remota y sin autorización, utilizando herramientas de administración remota existentes en el nivel del sistema operativo o el software remoto del

cliente del SCI mediante conexiones de redes privadas virtuales (VPN). Al parecer, los atacantes externos obtuvieron credenciales válidas antes del ciberataque para facilitar el acceso remoto.

Las tres compañías eléctricas informaron al concluir el ciberataque que se borraron varios sistemas utilizando el malware Kill Disk. Este malware borra ciertos archivos de los sistemas y corrompe el registro de arranque principal, lo que imposibilita utilizar estos sistemas. Además, las interfaces de usuario que utiliza Windows, incrustadas en unidades terminales remotas, también fueron sobrescritas mediante Kill Disk. Se inutilizaron varios conversores de serie a Ethernet de las subestaciones al corromper su firmware. Se desconectaron los sistemas de alimentación ininterrumpida (SAI) a través de su interfaz de gestión remota, lo que interfirió con las labores de restauración previstas.

Las tres empresas informaron de que habían sido infectadas por el malware Black Energy, pero no está claro si esto influyó de algún modo en el ciberataque. Según se informó, el malware se entregó mediante correos electrónicos de *phishing* que adjuntaban archivos malintencionados. No se ha confirmado, pero se sospecha que se utilizó Black Energy para obtener credenciales válidas. Sin embargo, se podría haber usado cualquier troyano para acceder remotamente.

Tras los ataques, las empresas no pudieron restaurar remotamente los disyuntores, por lo que el personal de operaciones tuvo que desplazarse físicamente para conmutarlos manualmente. Esto provocó que la duración del apagón se alargase entre cuatro y seis horas. Cabe observar que no se informó acerca de ningún daño en ninguna planta de generación eléctrica debido a este incidente.

3.4.2 TRISIS

En diciembre de 2017, unos investigadores de seguridad descubrieron un ataque de malware en sistemas instrumentados de seguridad y sistemas de control distribuido (DCS) de una gran planta industrial de Oriente Medio. Las organizaciones de ciberseguridad han denominado a este malware tanto TRITON como TRISIS, y el equipo de SCI y de respuesta ante emergencias comunitarias del Departamento de Seguridad Nacional de los EE. UU. se refiere a él como HATMAN. Este malware afectó a los controladores de seguridad y la interfaz de usuario Triconex Tricon de Schneider Electric, y permitió al atacante leer y modificar el contenido de la memoria de estos controladores (es decir, sobrescribir los programas existentes mediante una conexión de red remota).

Gracias a la información disponible, los atacantes accedieron a distancia a una estación de trabajo de ingeniería de los sistemas instrumentados de seguridad e instalaron el malware: un archivo ejecutable para ordenadores con sistema operativo Windows para comunicarse con el controlador de seguridad (Triconex) y un componente binario malintencionado que se descargó en el controlador. Mandiant, la empresa de ciberseguridad de FireEye responsable de investigar el incidente, explicó en su informe [1] que «el malware podía leer y escribir programas y consultar el estado del controlador. Asimismo, tenía la capacidad de comunicarse con el controlador mediante TriStation, un protocolo patentado que utiliza el software TriStation (software de programación de Tricon) para comunicarse con los sistemas de seguridad de Triconex. Parece que el atacante conocía el sistema Triconex y había probado el malware antes del ataque».

Basándose en el análisis de Mandiant, existen pruebas de que los atacantes también accedieron al DCS de la planta, pero decidieron ir contra el sistema de seguridad. Los atacantes provocaron la parada accidental del sistema mientras intentaban reprogramar los controladores para causar daños físicos. El sistema entró en un estado a prueba de fallos debido a una comprobación de validación fallida entre los procesadores, lo que detuvo el sistema y alertó al propietario. Según lo expresado por Mandiant: «Si el atacante hubiera tomado el control tanto del DCS como del sistema instrumentado de seguridad, el impacto podría haber sido mayor».

El Departamento de Seguridad Nacional de EE. UU. y Dragos han declarado que el protocolo TriStation utilizado en controladores antiguos, como el que sufrió este incidente, no cuenta con un mecanismo de autenticación o cifrado para cuentas que acceden por la puerta trasera del sistema, un aspecto esencial para acceder y controlar el dispositivo al nivel de administrador durante una emergencia. Sin embargo, las versiones más recientes de los sistemas de Triconex contienen un factor de autenticación para estas cuentas y son menos vulnerables a estos ataques. Schneider Electric confirmó esta vulnerabilidad mediante una notificación de seguridad y ha desarrollado una herramienta para detectar y eliminar el malware de los controladores Tricon. La empresa también indicó que el hardware de conmutación mediante llave que habilita el control físico de las operaciones se dejó en modo «Programación», una práctica que no se considera segura cuando no se está programando el controlador.

Los sistemas de seguridad de Triconex están entre los más seguros del mercado. Tricon utiliza la tecnología Triple Modular Redundant (TMR), que integra en un solo sistema tres sistemas de control aislados en paralelo y un exhaustivo proceso de diagnóstico. El sistema de Tricon proporciona una gran integridad en el funcionamiento de los procesos, sin errores ni interrupciones y sin puntos únicos de fallo. La tecnología TMR se aplica a entradas, salidas y lógica. Debido al impacto y el coste del sistema, se utiliza principalmente en aplicaciones estratégicas como controles de turbinas (control de sobrevelocidad) y, a veces, como DCS. Aunque este malware fue diseñado especialmente para sistemas de Triconex, las organizaciones de ciberseguridad creen que los malhechores pueden adaptar la capacidad y metodología de dicho malware con el fin de atacar a sistemas de seguridad de proveedores diferentes. Este incidente ha puesto en cuestión la creencia de que, incluso si el sistema de control de procesos resulta afectado, el sistema de seguridad evitará que se produzcan daños.

4.0 REFERENCIAS

4.1 FM

Ficha técnica 1-20, *Protection Against Exterior Fire Exposure*
Ficha técnica 1-44, *Damage-Limiting Construction*
Ficha técnica 2-0, *Directrices sobre la instalación de rociadores automáticos*
Ficha técnica 3-26, *Protección contra incendios para actividades sin almacenamiento*
Ficha técnica 4-5, *Portable Extinguishers*
Ficha técnica 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*
Ficha técnica 5-11, *Lightning and Surge Protection for Electrical Systems*
Ficha técnica 5-23, *Design and Protection for Emergency and Standby Power Systems*
Ficha técnica 5-28*, DC Battery Systems*
Ficha técnica 5-31, *Cables and Bus Bars*
Ficha técnica 5-32, *Data Centers and Relating Facilities*
Ficha técnica 7-43, *Process Safety*
Ficha técnica 7-45, *Safety Controls, Alarms, and Interlocks*
Ficha técnica 9-0, *Integridad de los activos*
Ficha técnica 9-1, *Supervision of Property*
Ficha técnica 10-1, *Planes de coordinación con el cuerpo de bomberos y de respuesta ante emergencias*
Ficha técnica 10-5, *Disaster Recovery Planning*
Ficha técnica 10-8, *Operators*

4.2 Otras referencias

International Society for Automation (ISA). Normas ISA/IEC 62443 y serie de informes técnicos.

National Institute of Standards and Technology (NIST) *Guide to Industrial Control Systems (ICS) Security*. NIST SP 800-82, revisión 2.

North American Electric Reliability Corporation (NERC). Normas de fiabilidad de la protección de infraestructuras críticas (CIP).

Electric Power Research Institute (EPRI), *Generation Cyber Security*.

Departamento de Seguridad Nacional de EE. UU., Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC), Equipo de SCI y de Respuesta ante Emergencias Comunitarias (ICS-CERT).

ANEXO A: GLOSARIO DE TÉRMINOS

Acceso físico: Acceso práctico y desde la planta a un hardware informático o de red o a otras partes de una instalación de red.

Acceso remoto: Acceso externo de usuarios (o sistemas de información) al perímetro de seguridad de un sistema informático (fuente: NIST SP 800-53). Uso de sistemas que se encuentran dentro del perímetro de seguridad desde una ubicación geográfica diferente con los mismos derechos que si el usuario se encontrase presente físicamente. Algunos ejemplos de los equipos utilizados en el acceso remoto son:

1. Los módems modulan los datos al entrar en la caja y los demodulan a su salida. En esencia, transforman señales eléctricas analógicas provenientes del exterior de la red en unos y ceros digitales que se gestionarán por el enrutador, y viceversa.

2. Los enrutadores están instalados aguas abajo del módem. Se conectan a una red de área extensa (WAN) o a Internet con una dirección IP pública. Guían y dirigen los datos de red, al mismo tiempo que los priorizan y eligen la mejor ruta para cada transmisión.
3. Los servidores de acceso remoto facilitan servicios que gestionan las conexiones remotas desde el exterior de la LAN. Suelen denominarse servidores o huéspedes «de salto».

Acceso: La capacidad de comunicarse o interaccionar con un sistema a fin de utilizar sus recursos, así como el medio para hacerlo. El acceso puede ser físico (permiso para estar físicamente en una zona, posesión de una llave física, un código personal o tarjeta de acceso o atributos biométricos que permitan el acceso) o lógico (autorización para iniciar sesión en un sistema y aplicaciones mediante una combinación de medios lógicos y físicos).

Activo: Objeto físico o lógico poseído o custodiado por una organización y que tiene un valor percibido o real para ella.

Actor de amenazas: Entidad que es responsable parcial o totalmente de un incidente que afecta a la seguridad de una organización. Algunos ejemplos de actores de amenazas son los hacktivistas, las amenazas internas, los estados nación y el crimen organizado.

Amenaza interna: Amenazas (tanto malintencionadas como involuntarias) de personas que forman parte de la organización, como empleados descontentos, antiguos empleados, contratistas y socios empresariales, que tengan información privilegiada acerca de las prácticas de seguridad, los datos y los sistemas informáticos de la organización.

Archivos de copias de seguridad inmutables: Un archivo de copias de seguridad inmutable es aquel que no puede alterarse ni modificarse por ningún medio (escritura única, muchas lecturas) y no puede borrarse hasta que haya finalizado el periodo de retención (la fecha de finalización de este periodo debe configurarse en el momento de crear el archivo inmutable). Puesto que los archivos inmutables no pueden alterarse ni borrarse, el control de versiones es fundamental.

Atacante: Persona que crea o modifica programas informáticos y hardware para cometer delitos o a cambio de beneficios económicos. Los atacantes suelen intentar acceder a los sistemas informáticos para obtener credenciales de usuario y contraseñas.

Autenticación multifactor: La autenticación multifactor entraña dos o más factores de autenticación (es decir, algo que el usuario conoce, como una contraseña; algo que el usuario tiene, como un testigo digital temporal o estático; o algo que forma parte del usuario, como una huella digital). La autenticación de dos factores es un caso especial de autenticación multifactor que involucra a exactamente dos factores.

Autenticación: Acto de demostrar una afirmación, como la identidad de un usuario de un sistema informático. A diferencia de la identificación, que es el acto de indicar la identidad de una persona o cosa, la autenticación es el proceso de verificar dicha identidad. Un medio común de autenticación es una contraseña facilitada por un usuario para iniciar la sesión.

Bastionado: Medida de seguridad que incluye la eliminación o desactivación de características, funciones, puertos y servicios no necesarios y la aplicación de controles de ciberseguridad para evitar el uso no autorizado. Existen dos tipos de bastionado:

1. Bastionado físico: La desactivación mediante medios físicos, la eliminación de puertos de comunicación innecesarios, el bloqueo de acceso a los puertos y unidades, etc.
2. Bastionado lógico: La desactivación de los protocolos de red y comunicación que no se utilicen, *drivers* de los periféricos no utilizados, servidores web, etc., y la aplicación de controles de ciberseguridad, como protección por contraseñas, para actualizar el firmware y cargar programas; la habilitación de registros y alertas; y la habilitación de tecnologías de seguridad como programas antivirus o listas de permisos incluidos en el dispositivo.

Centro de control de procesos: véase «Sala de control de procesos».

Centro de control SCADA: Un centro de control que utiliza ordenadores con software SCADA para supervisar y operar equipos en una o más ubicaciones alejadas geográficamente del centro de control. Los centros de control SCADA suelen situarse en un edificio que no tiene controles de proceso locales, como sistemas de control distribuido o controladores lógicos programables. Estos centros de control SCADA tienen

un tráfico de datos bidireccional y pueden modificar el funcionamiento de equipos situados en otra ubicación a distancia.

Centro de control: véase «Sala de control de procesos».

Centro de seguridad de operaciones (SOC): Solución que engloba a personas, procesos y tecnologías, incluida la solución SIEM, involucradas en la supervisión de los entornos digitales (redes informática y operativa). Da respuesta a sucesos que se convierten en incidentes, investiga la existencia de amenazas conocidas o desconocidas, da respuesta ante incidentes y divulga información, entre otras funciones.

Cifrado: Codificación de los datos de modo que no pueda leerlos nadie que no posea la clave utilizada para descodificarlos. Transformación criptográfica de texto plano en texto cifrado que oculta el significado original de los datos para evitar que estos se usen o conozcan.

Comunicación en un solo sentido: Estrategias empleadas para garantizar comunicaciones unidireccionales seguras desde dispositivos o a través de diferentes redes y zonas de protección, como:

1. el envío solamente de una señal analógica (de corriente o tensión eléctrica) desde o hacia un dispositivo, en lugar de datos digitales;
2. el uso de una pasarela o diodo de datos unidireccional;
3. el uso de reglas en un cortafuegos o red perimetral para transferir datos a través de redes.

Contraseña por defecto: La contraseña estándar incluida en un sistema cuando este se recibe o instala por primera vez. Los usuarios siempre deberían cambiar la contraseña por defecto inmediatamente.

Control de accesos basado en funciones: Método de control de accesos a partir de la identidad de los usuarios y en el que las entidades del sistema identificadas y controladas son puestos funcionales en una organización o proceso.

Controlador lógico programable (PLC): Los PLC son controladores de automatización con la capacidad de controlar procesos complejos, y se usan considerablemente en sistemas de supervisión, control y adquisición de datos (SCADA) y sistemas de control distribuido (DCS). También se usan como controladores principales en sistemas pequeños. Los PLC están muy extendidos en casi todos los procesos industriales.

Cortafuegos: Dispositivo de seguridad de red que supervisa el tráfico entrante y saliente de la red y decide si debe permitir o bloquear tráfico concreto basándose en un conjunto definido de reglas de seguridad.

Credenciales: Como mínimo, las credenciales han de estar formadas por un nombre de usuario y una contraseña, pero también pueden incluir un elemento biométrico físico o humano, como una huella dactilar. Las credenciales se utilizan para autenticar a un usuario cuando este inicia sesión en el SCI. Puede que se vinculen permisos de acceso a las credenciales del usuario. Estas podrían darle acceso solamente a una estación de operador, mientras que un usuario diferente con un nivel de permisos superior podría tener acceso a una estación de trabajo de ingeniería.

Defensa exhaustiva: Práctica de establecer varias capas superpuestas de controles de seguridad para proteger los entornos de las tecnologías de la información u operativas.

Dispositivo de campo: Equipo conectado al lado de campo de un SCI. Entre los tipos de dispositivos de campo se incluyen unidades terminales remotas, controladores lógicos programables (PLC), accionadores, sensores, interfaces de usuario y las comunicaciones relacionadas.

Dispositivo de entrada/salida (E/S): Término general que se aplica a los equipos que se utilizan para comunicarse con un ordenador o sistema de control.

Dispositivo no autorizado: Dispositivo que no cuenta con permiso para acceder y funcionar en la red. Estos dispositivos pueden ser malintencionados y utilizarse para esquivar los sistemas de seguridad.

Enrutador: Pasarela entre dos redes de la capa 3 del modelo de interconexión de sistemas abiertos que transmite y transfiere paquetes de datos a través de este espacio entre redes. El tipo de enrutador más común funciona con paquetes de protocolo de Internet (IP).

Equipos de control industrial: Véase «Paneles de control industrial».

Estación de operador: Una estación de operador proporciona una vista dinámica de todos los procesos de la planta necesarios para accionar los sistemas de control. Muestra gráficos de control, datos de diagnóstico, tendencias, alarmas y estados.

Estación de trabajo de ingeniería: Plataforma de computación usualmente fiable y de alto rendimiento diseñada para configurar, mantener y diagnosticar las aplicaciones y otros equipos del sistema de control. Generalmente, contiene el software del proveedor necesario para programar dispositivos, así como los archivos de proyecto utilizados para programar los dispositivos, incluidos los controladores lógicos programables y las interfaces de usuario.

Fiabilidad: Capacidad de un sistema de realizar una función necesaria bajo las condiciones indicadas durante un periodo especificado.

Gestión de configuración: Políticas y procedimientos para controlar modificaciones en el hardware, el firmware, el software y la documentación a fin de garantizar que el sistema de información esté protegido contra modificaciones inadecuadas antes, durante y después de la implantación del sistema.

Gestión de eventos e información de seguridad (SIEM): Aplicación que proporciona la capacidad de recopilar datos de seguridad de componentes del sistema de información, normaliza los registros de auditoría y registra las pruebas en un conjunto de reglas de correlación que, al activarse, crea eventos para el análisis y presenta esos datos como información práctica mediante una interfaz única.

Integridad: Cualidad de un sistema que refleja la exactitud lógica y la fiabilidad del sistema operativo, la exhaustividad lógica del hardware y el software encargados de implantar los mecanismos de protección, la coherencia de las estructuras de datos y la existencia de los datos almacenados.

1. Dispositivo electrónico inteligente (IED): Cualquier dispositivo que incorpore uno o más procesadores con capacidad para recibir, enviar y controlar datos desde o hacia una fuente externa (p. ej., medidores electrónicos multifunción, relés digitales, controladores).

Interfaz de usuario:

1. Hardware o software a través del cual un operador interactúa con un controlador. Puede ser un panel de control físico con botones y testigos o un ordenador industrial con pantalla a color para la visualización de gráficos que emplea un software especializado.
2. Software y hardware que permite a los usuarios autorizados supervisar y controlar procesos y equipos. Por ejemplo, permite visualizar su estado o tendencias históricas, modificar los ajustes de control y anular manualmente en caso de emergencia.

Lista de permisos: Lista de entidades discretas, como anfitriones o aplicaciones, que se sabe que son benignas y han sido aprobadas para su uso en una organización o sistema informático. Ejemplo: Permitir la ejecución solamente de ciertas aplicaciones y servicios en un anfitrión como parte de su bastionado.

Malware: Término genérico utilizado para describir software malintencionado como virus, archivos troyanos, software espía y contenido activo malintencionado.

Marcación de guerra: Un marcador de guerra es un programa informático utilizado para identificar los números de teléfono que pueden establecer una conexión con el módem de un ordenador. El programa marca automáticamente un intervalo definido de números telefónicos y registra en una base de datos aquellos que se conectan con éxito al módem. Algunos programas también pueden identificar el sistema operativo concreto que esté ejecutando el ordenador y también pueden llevar a cabo pruebas de penetración automatizadas. En tales casos, el marcador de guerra recorre una lista predeterminada de nombres de usuario y contraseñas comunes para intentar acceder al sistema.

Paneles de control industrial (PCI): Conjunto que consta de dos o más componentes de circuitos de control y potencia. Entre los componentes de circuitos de control están los controladores lógicos programables, módulos de entrada y salida, transmisiones de motores y módulos de comunicación. Algunos componentes de circuitos de potencia son fuentes de alimentación, sistemas de alimentación ininterrumpida (SAI), relés, transformadores eléctricos y convertidores de tensión y corriente. En general, los PCI funcionan con una alimentación de 600 voltios o menos, aunque las normativas UL 508A e IEC permiten valores de hasta 1.000 voltios.

Parche: Complemento de software diseñado para arreglar fallos y problemas de seguridad en sistemas operativos o aplicaciones. Los riesgos de seguridad pueden minimizarse instalando todos los parches más recientes del software.

Pasarela: Mecanismo de transmisión que une dos o más redes informáticas con funciones similares, pero implantaciones distintas y que permite a los ordenadores anfitriones de una red comunicarse con los huéspedes de la otra.

Pasarelas de datos unidireccionales o de diodo: Véase la definición de «diodo de datos unidireccional» posterior.

Pasarelas unidireccionales y diodos de datos unidireccionales: Dispositivos basados en hardware con dos nodos o circuitos (uno solamente envía, el otro solamente recibe) que permiten el flujo de datos en una única dirección, desde un origen hasta un destino. Utilizan un LED como transmisor de datos en un lado y un fotorreceptor en el otro, lo que imposibilita que los datos se transmitan físicamente en la otra dirección. Algunas personas pueden considerar que una solución de software (a través de un cortafuegos), o incluso un conmutador o un enrutador, son pasarelas unidireccionales, pero una pasarela unidireccional «real» utiliza diodos de datos de una dirección para crear dicha pasarela. De acuerdo con la norma NIST 800-82: Las pasarelas unidireccionales son una combinación de hardware y software. El hardware permite el flujo de datos de una red a otra, pero es físicamente incapaz de enviar información de vuelta a la red de origen. El software duplica las bases de datos y emula los servidores y dispositivos de protocolo».

Phishing: Tipo de ataque de seguridad que persuade a las víctimas para que revelen información mediante el envío de un correo electrónico falsificado que hace que el destinatario acceda a una página web que parece estar relacionada con una fuente legítima.

Política: Conjunto de reglas que rige cómo se gestionan ciertos procedimientos.

Procedimiento: Pasos necesarios para realizar una tarea determinada.

Programa antivirus: Programa que protege a un ordenador contra virus y malware. Cuando se detecta la presencia de código malintencionado, el programa antivirus intenta limpiar, borrar o aislar los archivos, directorios o discos afectados.

Protocolo: Sistema de reglas utilizado por dos componentes que comparten datos para interpretar los datos que se están compartiendo. No es un «lenguaje», sino que puede describirse de manera más adecuada como la gramática y la sintaxis necesarias para comunicar dicho lenguaje. En el mundo de los SCI, muchos de estos protocolos solo se utilizan por un proveedor y se han diseñado prestando atención a la funcionalidad y la fiabilidad, en lugar de a la seguridad. Suelen transmitirse en texto en claro (sin cifrar). Esto aumenta la necesidad de separar los entornos operativos de la red informática. Algunos ejemplos de protocolos de SCI utilizados en la industria son: Modbus RTU, Modbus TCP, Profibus, Profinet, DNP3 y ControlNet. En el lado informático, es común utilizar protocolos basados en TCP/IP (como FTP, DNS, HTTP, HTTPS).

Ransomware: Un tipo de software malintencionado (malware) que desactiva el funcionamiento o bloquea el acceso a los datos hasta que el propietario o el operador responde a una exigencia económica.

Red de área extensa (WAN): Red informática que abarca superficies grandes, países o incluso el mundo entero. Los datos se transfieren de varias maneras entre redes que se extienden por una ubicación geográfica; los diferentes tipos de conexión crean estas redes WAN. Algunas soluciones cableadas son: MPLS, T1 y circuitos virtuales permanentes. Entre los servicios de comunicación inalámbricos se encuentran 4G, 5G, Wi-Fi y redes satelitales.

Red de área local (LAN): Red de comunicaciones diseñada para conectar ordenadores y otros dispositivos inteligentes situados en una zona geográfica limitada (generalmente de menos de 10 kilómetros).

Red de control: Red cuya rapidez es fundamental y que está conectada normalmente a los equipos que controlan los procesos físicos. La red de control puede dividirse en zonas, y puede haber varias redes de control independientes en una sola empresa y planta.

Red de seguridad: Red que conecta sistemas instrumentados de seguridad para transmitir información de seguridad.

Red de tecnologías de la información: Red que se utiliza generalmente para llevar a cabo actividades empresariales en las que se utilizan ordenadores para crear, manipular, almacenar, recuperar y transmitir datos.

Red de tecnologías operativas (red de OT): El término «red operativa» se suele usar indistintamente con sistema de control industrial (SCI) o redes de control de procesos. Está pensado para distinguir entre la red

de tecnologías de la información de la empresa y la red que controla los activos operativos. Los SCI constan de varios controladores e instrumentos que supervisan y controlan un proceso físico, mientras que la red operativa incluye a los sistemas informáticos y la infraestructura que gestionan las operaciones industriales (incluidos los SCI).

Red perimetral (industrial):

1. Interfaz de un cortafuegos de enrutamiento similar a las que se encuentran en el lado protegido del cortafuegos. El tráfico que se mueve entre la red perimetral y otras interfaces del lado protegido del cortafuegos sigue atravesando el cortafuegos, y pueden aplicarse sobre él políticas de protección por cortafuegos.
2. Un anfitrión o un segmento de red que está insertado como zona neutral entre la red privada de una organización e Internet. La mayoría de las redes perimetrales industriales se encuentran entre los entornos informático y operativo de una organización.
3. Un segmento de una red perimetral vinculado lógicamente entre las redes internas y externas. Su finalidad es hacer cumplir la política de la red interna para el intercambio de información externa y proporcionar a las fuentes externas y no fiables un acceso restringido a la información divulgable mientras protege a las redes internas de ataques externos.

Red privada virtual (VPN): Conexión segura entre una red pública (Internet, generalmente) y una privada.

Referencia: Especificación o producto que se ha revisado y sobre el que se ha llegado a un acuerdo formalmente y que, desde entonces, sirve como base para desarrollos posteriores y puede modificarse solo mediante procedimientos formales de control de cambios.

Repositorio de usuarios: Sistema que almacena información sobre usuarios o miembros para un dominio concreto con el objetivo de garantizar las funciones de autenticación y autorización utilizando un enfoque centralizado. Microsoft Active Directory es un ejemplo habitual de repositorio de usuarios que puede verse comúnmente en redes informáticas y operativas.

Sala de control de procesos: Sala compartimentada o aislada en la que el personal supervisa y controla procesos desde una ubicación central o remota. La sala de control de procesos suele estar separada de las salas de equipos de control industrial, pero integrada con estas a fin de controlar el funcionamiento de los equipos. El control de procesos se usa ampliamente en la industria. Comúnmente, permite ejecutar procesos de producción continua en masa, como papel, fármacos, productos químicos y energía eléctrica, así como otros procesos industriales. En algunas situaciones, algunas salas y espacios técnicos de control de procesos pueden estar desatendidas y operarse a distancia.

Salas de equipos e instrumentos de control industrial: Salas que albergan los equipos de control de procesos, que suelen incluir varios paneles de control industrial y los equipos de redes necesarios para que funcione el proceso físico.

Segmentación: División de una red en secciones más pequeñas y compartimentadas que siguen formando parte de la misma red general. En el ámbito de los SCI, la segmentación suele conseguirse mediante redes de área local virtuales (VLAN) o cortafuegos de hardware. La segmentación ayuda a frenar la propagación de malware o a obstaculizar a un atacante. Sin embargo, el uso de VLAN no es un método aceptable de separación de la red informática y la operativa.

Segregación: Desconexión completa de una red con respecto a otras (*air-gapped*). Los sistemas instrumentados de seguridad (SIS) de plantas grandes suelen estar segregados debido a que no están controlados por la red de SCI que gestiona el sistema básico de control de procesos.

Sensor:

1. Dispositivo que produce una tensión o corriente que representa la medición de una propiedad física (p. ej., velocidad, temperatura o caudal).
2. Dispositivo que mide una cantidad física y la transforma en una señal que puede ser leída por un observador o un instrumento.
3. Dispositivo que responde a una cantidad de entrada mediante la generación de una salida relacionada funcionalmente, generalmente en forma de señal eléctrica u óptica.

Separación: Partición adecuada de redes diferentes consideradas como no fiables entre sí. La separación suele conseguirse mediante cortafuegos (y, de manera ideal, con una red perimetral formal) o una pasarela unidireccional. La separación de la red informática resulta fundamental para las redes de los SCI.

Servidores de acceso remoto: Tipo de servidor que facilita servicios para gestionar una conexión remota desde el exterior de la LAN. Suelen denominarse servidores «de salto».

Sistema básico de control de procesos: Sistema que gestiona los equipos, la producción y los procesos de una planta. A partir de unas condiciones predeterminadas, y utilizando las respuestas de bucles de control, automatiza y mantiene una condición, un parámetro de salida o un proceso deseados. Los sistemas básicos de control de procesos se personalizan para satisfacer cualquier necesidad de los procesos, desde sistemas de gran tamaño y complejidad, como sistemas de generación eléctrica o procesadores de productos químicos, hasta sistemas muy sencillos con una sola entrada y salida, como detectores de movimiento o sistemas de iluminación.

Sistema de control distribuido (DCS): Sistema automatizado que controla los procesos distribuyendo las funciones de control entre múltiples componentes interconectados. Utiliza componentes distribuidos en lugar de un equipo central único. Obsérvese que el término «controlador del DCS» se aplica al componente del controlador físico, mientras que el término «sistema de control distribuido» se aplica al sistema completo, incluidos los servidores de aplicaciones, interfaces de usuario, etc.

Sistema de control industrial (SCI):

1. Término general que abarca varios tipos de sistemas de control, incluidos sistemas de supervisión, control y adquisición de datos (SCADA), sistemas de control distribuido (DCS) y otras configuraciones de sistemas de control, como controladores lógicos programables y controladores lógicos de seguridad, que suelen encontrarse a menudo en sectores industriales e infraestructuras estratégicas. Un SCI consta de varios componentes de control (p. ej. eléctricos, mecánicos, hidráulicos, neumáticos) que actúan en conjunto para alcanzar un objetivo industrial (como fabricación, generación de electricidad o transporte de materia o energía).
2. Conjunto de trabajadores, hardware y software que pueden afectar o influir en el funcionamiento seguro y fiable de un proceso industrial.

Sistema de detección de intrusiones: Servicio de seguridad que supervisa y analiza eventos en la red o el sistema a fin de detectar posibles intentos de acceder a recursos del sistema sin autorización y proporcionar advertencias en tiempo real o cuasireal. Un sistema de detección de intrusiones puede detectar y alertar de tráfico dañino, pero no bloquearlo ni rechazarlo.

Sistema de ejecución de fabricación (MES): Sistema informático que incluye software utilizado en entornos de producción y fabricación para ayudar a rastrear inventarios y otra información de producción. Funciona de manera similar a un sistema ERP, pero con un enfoque más especializado en la fabricación (p. ej., supervisión y documentación de la transformación de materias primas en productos acabados).

Sistema de planificación de recursos empresariales (ERP): Software utilizado en entornos empresariales; algunos ejemplos son SAP y Oracle/PeopleSoft, sistemas que gestionan pedidos de producción, actividades de almacenamiento e información de transporte de los pedidos completados.

Sistema de seguridad: Sistema empleado para implantar una o más funciones con instrumentos de seguridad. Consta de una combinación de sensores, controladores lógicos y accionadores.

Sistema operativo: Software básico que habilita la interacción con un ordenador. Controla el almacenamiento, las comunicaciones y la gestión de las tareas del ordenador.

Sistema para el almacenamiento de datos históricos: Sistema de software especializado que recopila valores puntuales, alarmas, registros por lotes y otra información proveniente de los dispositivos y sistemas industriales y los almacena en una base de datos creada para este fin (es decir, una base de datos centralizada que admite el análisis de datos utilizando técnicas estadísticas de control de procesos).

Soluciones de detección de activos:

1. Supervisión pasiva: Técnica de supervisión silenciosa y no intrusiva empleada para capturar el tráfico de una red mediante la copia de dicho tráfico, a menudo desde un puerto SPAN o espejo o mediante terminal de acceso a la red. Las soluciones de detección de intrusiones basadas en la red operativa utilizan esta técnica para detectar activos y actividades no autorizadas.

2. Supervisión activa: Técnica de supervisión intrusiva que ejecuta consultas en el idioma nativo del controlador correspondiente (protocolo); puede variar ligeramente dependiendo del fabricante. En una estrategia de supervisión activa, se le pregunta al controlador acerca de información detallada (dirección IP y MAC, versión del firmware, configuración de la placa base, etc.).

Supervisión, control y adquisición de datos (SCADA): Se usa para controlar activos dispersos cuando la adquisición centralizada de datos es tan importante como el control. Los sistemas de SCADA se usan en sistemas de distribución como los siguientes:

1. sistemas de distribución de agua y de recogida de aguas residuales;
2. oleoductos y gasoductos;
3. sistemas de transmisión y distribución eléctrica;
4. sistemas ferroviarios u otros medios de transporte público.

Los sistemas de SCADA integran a sistemas de adquisición de datos con sistemas de transmisión de datos e interfaces de usuario para formar un sistema centralizado de supervisión y control para numerosas entradas y salidas de los procesos. Los sistemas de SCADA se diseñan para recopilar información de campo, transferirla a una instalación informática central y mostrarla al operador mediante gráficos o texto, lo que permite a dicho operador supervisar o controlar un sistema completo desde una ubicación central prácticamente en tiempo real. En función de la sofisticación y la configuración del sistema, el control de cualquier sistema, operación o tarea puede ser automático o realizarse mediante comandos del operador.

Unidad terminal remota (RTU): Unidad diseñada para asistir a sistemas de control distribuido (DCS) y estaciones remotas de supervisión, control y adquisición de datos (SCADA). Las RTU son dispositivos de campo utilizados para supervisar parámetros. Se comunican con un controlador de supervisión mediante comunicaciones remotas, como módems, interfaces de telefonía móvil o de radio o cualquier tecnología de comunicación de área extensa. A veces, se utilizan PLC de modo que ejerzan como dispositivos de campo y actúen como RTU; en este caso, suele referirse al PLC como una RTU. Suelen instalarse en ubicaciones que no cuentan con un acceso sencillo a una fuente de electricidad, pero pueden alimentarse mediante energía solar.

Vector de ataque: Método o medio por el que un atacante accede a, o daña, los datos o la red de ordenadores de una organización. Algunos ejemplos de vectores de ataque son la denegación de servicio (DoS), malware, acceso físico, ransomware e ingeniería social.

Vulnerabilidad: Defecto o debilidad en el diseño, la implantación, el funcionamiento o la gestión de un sistema que puede aprovecharse para violar su integridad o la política de seguridad.

ANEXO B: HISTORIAL DE REVISIONES DEL DOCUMENTO

El objetivo de este anexo es recoger los cambios introducidos en este documento en cada una de sus versiones publicadas. Tenga en cuenta que los números de secciones se refieren específicamente a la numeración existente en la versión publicada en esa fecha (es decir, los números de sección no siempre se mantienen idénticos de una versión a otra).

Julio de 2024. Revisión parcial. Se llevaron a cabo cambios de redacción.

Enero de 2024. Revisión provisional. Se llevaron a cabo cambios mínimos de redacción.

Julio de 2023. Revisión parcial. Se han llevado a cabo los siguientes cambios importantes:

A. Se han mejorado y aclarado las recomendaciones relativas a la protección contra incendios.
    1. Se han mejorado las directrices sobre los sistemas de protección contra incendios que afectan a la actividad y a los equipos.
B. Se han actualizado las recomendaciones de seguridad de los SCI.
    1. Se han facilitado directrices sobre las conexiones a centros de control SCADA remotos.
C. Se han añadido términos al anexo A: Glosario de términos.

Enero de 2023. Revisión provisional. Se llevaron a cabo los siguientes cambios:

A. Se han aclarado recomendaciones de protección contra incendios.
B. Se han aclarado recomendaciones para la gestión de los SCI.

C. Se han aclarado y modificado las siguientes recomendaciones relacionadas con la seguridad de los SCI:

1. Se han modificado las recomendaciones relativas a la configuración y la supervisión de los sistemas de control industrial y equipos de redes operativas, incluidos los sistemas de seguridad.
2. Se han aclarado las recomendaciones sobre la gestión de parches.
3. Se han aclarado las recomendaciones relativas a los sistemas de seguridad de redes.

D. Se han aclarado y modificado las recomendaciones relacionadas con las operaciones de los SCI.

1. Se han aclarado las recomendaciones relativas a la gestión de alarmas.
2. Se ha modificado el programa de recuperación tras incidentes, concretamente los tipos de archivos que pueden aceptarse como copias de seguridad.

E. Se han añadido términos al anexo A: Glosario de términos.

Julio de 2022. Revisión parcial. Se llevaron a cabo cambios mínimos de redacción.

Octubre de 2021. Revisión provisional. Se actualizó la referencia a la prueba de baterías (sección 2.7).

Julio de 2021. Revisión parcial. Se actualizó y aclaró lo siguiente:

A. Seguridad de los SCI

i. gestión de accesos;
ii. gestión de configuración;
iii. gestión de instalación de parches;
iv. sistemas de seguridad de redes.

B. Operaciones de los SCI

i. procedimientos operativos en caso de emergencia.

C. Recomendaciones sobre la construcción y la protección contra incendios.

Julio de 2020. Revisión parcial. Se actualizaron el plan de contingencia y las directrices para la gestión de piezas de recambio.

Octubre de 2019. Esta es la primera edición de este documento.