OBJETO

En el ámbito de **FMB** y de la **Protección de Infraestructuras Críticas y de la Ciberesiliencia en la Seguridad OT** se determina en el presente documento: requisitos en cuestiones de ciberseguridad de aplicación a los proveedores de servicios para sistemas operacionales de FMB, de acuerdo con la aplicación de las recomendaciones recopiladas en las Normativas: UNE-EN IEC 62443, EN 50701 y el Esquema Nacional de Seguridad (ENS – CCN).

CONSIDERACIONES PREVIAS

Los requisitos de sistema y de componente están previsto en la Norma **UNE IEC 62443 Parte 3-3 requisitos de seguridad del sistema y niveles de seguridad y** en la Norma **UNE IEC 62443 Parte 4-2 requisitos técnicos de seguridad para componentes iacs.,** así como en su aplicación al sector ferroviario, UNE-CLCTS 507012021.

ACRÓNIMOS

Acrónimo	Concepto
BPCS	Sistema básico de control de procesos
BR	Requisito básico
CR	Requisito de componente
D. Req	Documentación requerida
EDR	Requisito para dispositivos integrados
ER	Mejora de los requisitos
EWS	Estaciones de trabajo técnicas
HDR	Requisito para dispositivos host
ID req	Identificación de los requisitos recogida en la UNE 62443-2-4
JTAG	Joint Test Action Group
NDR	Requisito para dispositivos de red
PKI	Clave pública que permite cifrar y firmar datos
SAR	Requisito para aplicaciones de software
SIS	Sistema instrumentado de seguridad
SL	Nivel de seguridad
SP	Programa de seguridad
SR	Requisito de sistema
SuC	Sistema bajo consideración

REQUISITOS ESPECÍFICOS RELACIONADOS CON LA CIBERSEGURIDAD

Las empresas externas deben de tomar una serie de medidas con respecto a la seguridad tanto física como cibernética en los dispositivos con los que trabaja, ya que muchas veces estos dispositivos o está en la infraestructura de FMB o se relacionan con dichas infraestructuras a la hora de realizar operaciones sobre ellas.

Teniendo en cuenta la organización de los requisitos recogidos en la norma UNE 50701 y las descripciones de los mismos, recogidas en la UNE-EN IEC 62443, se clasifica los diferentes requisitos según su obligatoriedad, tema que trata y la necesidad o no de aportar documentación para poder demostrar su cumplimiento.

1. Dotación de personal (SP.01)
2. Garantía (SP.02)
3. Arquitectura (SP.03)
4. Tecnología inalámbrica (SP.04)
5. SIS (SP.05)
6. Gestión de la configuración (SP.06)
7. Acceso remoto (SP.07)
8. Gestión de eventos (SP.08)
9. Gestión de cuentas (SP.09)
10. Protección contra malware (SP.10)
11. Gestión de parches (SP.11)
12. Copia de seguridad/restauración (SP.12)

ANEXO 0: Especificaciones sobre el inventario SuC y la evaluación de riesgo inicial
ANEXO I: Requisitos para nivel SL1
ANEXO II: Requisitos para nivel SL2
ANEXO III: Requisitos para nivel SL3
ANEXO IV: Requisitos para nivel SL4

DOTACIÓN DE PERSONAL (SP.01)

Requisitos relacionados con la asignación del personal de la empresa externa que ejecuta los trabajos en FMB.

ID req	BR/RE	Explicación	D.Req
SP.01.01 Formación - Requisitos 62243	BR	Garantizar que se asigna sólo personal que haya sido informado y que cumpla con las responsabilidades, políticas y procedimientos requeridos por esta especificación.	No
	RE1	Garantizar que se asigna sólo personal del subcontratista o consultor a las actividades relacionadas que haya sido informado y que cumpla con las responsabilidades, políticas y procedimientos requeridos por esta especificación.	No
SP.01.02 Formación - Requisitos propietario del activo	BR	Garantizar que se asigna sólo personal del proveedor de servicios, subcontratista o consultor a las actividades que haya sido informado y que cumpla con las responsabilidades, políticas y procedimientos relacionados con la seguridad requeridos por el propietario de los activos.	No
	RE1	Garantizar que se asigna sólo personal del proveedor de servicios, subcontratista o consultor a las actividades relacionadas que haya sido informado y que cumpla con los procesos de gestión de cambios y con el permiso de trabajo del propietario de los activos para los cambios que involucren dispositivos, estaciones de trabajo y servidores, así como las conexiones entre ellos.	No
SP.01.03 Formación - Datos confidenciales	BR	Garantizar que se asigna sólo personal del proveedor de servicios a las actividades relacionadas que haya sido informado y que cumpla con las políticas, procedimientos y obligaciones contractuales requeridas para proteger la confidencialidad de los datos del propietario de los activos.	No
	RE1	Garantizar que se asigna sólo subcontratistas, consultores y representantes a las actividades relacionadas que haya sido informado y que cumpla con las políticas y procedimientos requeridos para proteger la confidencialidad de los datos del propietario de los activos.	No
SP.01.04 Comprobación antecedentes	BR	Garantizar que se asigna sólo personal del proveedor de servicios a las actividades relacionadas que haya superado con éxito las comprobaciones de antecedentes relacionados con la seguridad en la medida en que lo permita la legislación aplicable.	No
	RE1	Garantizar que se asigna sólo subcontratistas, consultores y representantes a las actividades relacionadas que haya superado con éxito las comprobaciones de antecedentes (siempre que sea posible) relacionados con la seguridad en la medida en que lo permita la ley aplicable.	No
SP.01.05 Asignación laboral -	BR	Tener la capacidad de asignar un contacto de seguridad en su organización, que será responsable de las siguientes actividades: 1) Actuar como enlace con el propietario de los activos. 2) Comunicar el punto de vista del proveedor de servicios sobre la seguridad del IACS al personal del propietario de los activos. 3) Asegurarse de que las ofertas presentadas al propietario de los activos están de acuerdo y cumplen con los requisitos de la Parte2-4 especificados por el propietario de los activos y con los	No

Contacto de seguridad		requisitos de seguridad internos del IACS del proveedor de servicios. 4) Comunicar al propietario de los activos las desviaciones de asuntos que no se ajusten a los requisitos.	
SP.01.06 Asignación laboral - Encargado de seguridad	BR	Tener documentadas las cualificaciones mínimas en seguridad cibernética para los puestos de jefe de seguridad y asignar jefes de seguridad que cumplan con estas cualificaciones.	No
SP.01.07 Asignación laboral - Cambios	BR	Contar con la capacidad de notificar al propietario de los activos sobre los cambios en el personal del proveedor de servicios, subcontratista o consultor que tenga acceso a las actividades.	No

GARANTÍA (SP.02)

Requisitos relacionados con la generación de confianza en la aplicación de las políticas de seguridad.

ID req	BR/RE	Explicación	D.Req
SP.02.01 Componentes de la solución - Verificación	BR	Proporcionar documentación que verifique que los componentes identificados por el propietario de los activos (por ejemplo, como resultado de una evaluación de seguridad, análisis de amenazas y/o ensayos de seguridad) tengan la seguridad adecuada para su nivel de riesgo.	Si
SP.02.02 Herramientas y software de seguridad	BR	Recomendar herramientas de análisis de seguridad. 1) Proporcionar instrucciones sobre cómo utilizarlas. 2) Identificar cualquier efecto adverso conocido que puedan tener en el funcionamiento.3) Proporcionar recomendaciones sobre cómo evitar los efectos adversos.	Si
	RE1	Garantizar que obtiene la aprobación del propietario de los activos antes de utilizar las herramientas de análisis de seguridad (por ejemplo, el análisis de red) en el emplazamiento del propietario de los activos.	No
	RE2	Programar y utilizar herramientas de análisis de seguridad para descubrir sistemas indocumentados y/o no autorizados o vulnerabilidades. Esta capacidad debe incluir la capacidad de utilizar estas herramientas de acuerdo con los procedimientos operativos estándar del propietario de los activos.	No

	RE3	Garantizar que los componentes del sistema de control utilizados tengan la capacidad de mantener la operación de las funciones esenciales del sistema de control en presencia de análisis del sistema y/o de la red durante el funcionamiento normal.	No
SP.02.03 Directrices de protección	BR	Proporcionar documentación al propietario de los activos que describa cómo proteger (hardening) los activos.	Si
	RE1	Verificar que se siguen las directrices (hardening) y procedimientos de protección de la seguridad durante las actividades.	No

ARQUITECTURA (SP.03)

Requisitos relacionados con el diseño de los activos.

ID req	BR/RE	Explicación
SP.03.01 Evaluación de riesgos	BR	Realizar una evaluación de riesgos de seguridad o participar en una evaluación de riesgos de seguridad realizada por el propietario de los activos o su agente. *Aunque no se requiera documentación en este requisito, se podrá requerir la evaluación de riesgo (ver Anexo 0).
	RE1	Informar al propietario de los activos de los resultados de las evaluaciones de riesgos de seguridad a las que someta los activos, incluidos los mecanismos y procedimientos de reducción de riesgos.
	RE2	Verificar que un tercero haya realizado las revisiones de la arquitectura de seguridad y/o la evaluación de la seguridad y/o los análisis de amenazas del sistema de control utilizado.
SP.03.02 Diseño de redes - Conectividad	BR	Garantizar que la arquitectura física de segmentación de red utilizada en los activos, incluido el uso de dispositivos de seguridad de red o mecanismos equivalentes, se implemente de acuerdo con el diseño aprobado por el propietario de los activos.
	RE1	Identificar y documentar los segmentos de red de los activos y sus interfaces con otros segmentos, incluyendo redes externas, y se debe designar si cada interfaz es fiable o no.
	RE2	Garantizar que las interfaces que se hayan identificado como no fiables estén protegidas por dispositivos de seguridad de red o mecanismos equivalentes, con normas de seguridad documentadas y mantenidas.
SP.03.03 Vulnerabilidades	BR	Manejar las vulnerabilidades que afectan a los componentes, incluyendo sus políticas y procedimientos relacionados. Estas capacidades deben abarcar los siguientes puntos: 1) el manejo de vulnerabilidades recientemente descubiertas o en sus políticas y procedimientos relacionados de los cuales es responsable el proveedor de servicios, y 2) el manejo de vulnerabilidades reveladas públicamente que afectan.
	RE1	Proporcionar documentación al propietario de los activos que describa cómo mitigar las debilidades de seguridad inherentes al diseño y/o implementación de protocolos de comunicación utilizados que se conocían antes de las actividades de integración o mantenimiento.

SP.03.04 Diseño de redes – Tiempo de red	BR	Garantizar que la distribución/sincronización de tiempo se realiza desde una fuente segura y precisa que utilice un protocolo comúnmente aceptado tanto por las comunidades dedicadas a la seguridad como por aquellas dedicadas a la automatización industrial.
SP.03.05 Funcionalidad mínima	BR	Garantizar que sólo las características de software y hardware requeridas o aprobadas por el propietario de los activos estén habilitadas en los activos. 1) se desactiven o eliminen las aplicaciones y servicios de software innecesarios y sus puntos de acceso de comunicación asociados, dispositivos USB, comunicaciones Bluetooth e inalámbricas, a menos que lo requiera los activos; 2) estén autorizadas las direcciones de red en uso; 3) el acceso físico y lógico a los puertos de diagnóstico y configuración esté protegido contra el acceso y uso no autorizados; 4) los puertos no utilizados de los dispositivos de red se configuran para evitar el acceso no autorizado a la infraestructura de red; 5) los procesos de mantenimiento mantengan el estado de protección (hardening) durante su vida útil.
	RE1	Las directrices y procedimientos de protección (hardening) del proveedor de servicios deben garantizar que sólo se instalen los certificados digitales necesarios, autorizados y documentados por las entidades de certificación.
SP.03.06 Estaciones de trabajo – Bloqueo de sesión	BR	Garantizar que las estaciones de trabajo bajo la responsabilidad del proveedor de servicios soportan el uso de bloqueo de la sesión, 1) impidiendo que se visualice la información en el dispositivo y 2) bloqueando la entrada de otro usuario que no sea el propio o un administrador que desbloquee.
SP.03.07 Estaciones de trabajo – Control de acceso	BR	Garantizar que las estaciones de trabajo por cable e inalámbricas, incluidos los dispositives portátiles, utilizadas para el mantenimiento y la ingeniería no eluden: 1) los controles de acceso y 2) protecciones de Seguridad de la red en el límite con el nivel 3. Se prohíbe el acceso directo de un dispositivo portàtil a un dispositivo inalámbrico de nivel 3 que se salte el dispotivo de seguridad de red de nivel 2/3.
	RE1	Capacidad de soportar el uso de autenticación multifactor según lo requiera el propietario del activo.
SP.03.08 Dispositivos - Red	BR	Garantizar que se utilizan los privilegios mínimos para la administración de los dispositives.
	RE1	Garantizar que los controles de acceso están basados en roles de usuario.
	RE2	Garantizar que se utiliza cifrado para proteger los datos, ya sea en tránsito o en reposo.
	RE3	Garantizar que los controles de acceso utilizados para la administración de los dispositivos de red incluyan la autenticación mutua.

SP.03.09 Protección de datos – Comunicaciones	BR	Asegurar que todas las acciones de control y flujos de datos, incluyendo los cambios de configuración: 1) sea válidos; 2) los haya iniciado o aprobado un usuario, y 3) se hayan transferido a través de una conexión aprobada en la dirección aprobada.
SP.03.10 Protección de datos – Datos confidenciales	BR	Garantizar que los puntos de almacenamiento de datos y los flujos de datos, según lo definido o aprobado por el propietario del activo, están documentados, incluyendo los requisitos de seguridad para su protección.
	RE1	Garantizar que los datos estén protegidos contra la divulgación o modificación no autorizada, ya sea en reposo o en tránsito.
	RE2	Proporcionar documentación al propietario del activo que describa las capacidades de retención proporcionadas para el almacenamiento / archivo de datos confidenciales.
	RE3	Garantizar que los mecanismos criptográficos utilizados, incluidos los algoritmos y la gestión / distribución / protección de claves, sean los comúnmente aceptados por las comunidades de seguridad y de automatización industrial.
	RE4	Garantizar que cuando se retire un componente, todos los datos del componente que requieran protección, se destruirán / eliminarán de forma permanente.

TECNOLOGÍA INALÁMBRICA (SP.04)

Requisitos relacionados con el uso de la tecnología inalámbrica en los activos.

ID req	BR/RE	Explicación	D.Req
SP.04.01 Diseño de la red – Descripción técnica	BR	Garantizar que la documentación de la arquitectura de los activos que describe los sistemas inalámbricos esté actualizada en lo que se refiere a la descripción de lo siguiente: 1) intercambio de datos entre una red de nivel 1 e instrumentación inalámbrica; 2) intercambio de datos entre una red de nivel 2 y una red de nivel 3 a través de un enlace inalámbrico seguro; 3) mecanismos de seguridad que impiden que un intruso acceda a los activos a través del sistema inalámbrico; 4) mecanismos de seguridad que restringen el acceso dentro de los activos por parte de los trabajadores con dispositivos inalámbricos portátiles; 5) cuando sea necesario, mecanismos de seguridad que proporcionen protección para la gestión remota de los sistemas inalámbricos.	No
SP.04.02 Diseño de la red	BR	Garantizar que el acceso a los dispositivos inalámbricos esté protegido por mecanismos de autenticación y control de acceso comúnmente aceptados por las comunidades de seguridad y de automatización industrial.	No
	RE1	Garantizar que las comunicaciones inalámbricas estén protegidas por mecanismos criptográficos comúnmente aceptados por las comunidades de seguridad y de automatización industrial.	No
SP.04.03	BR	Garantizar que los protocolos inalámbricos utilizados en los activos cumplen con las normas y con las regulaciones aplicables utilizadas dentro de la comunidad de seguridad industrial.	No

Diseño de la red	RE1	Garantizar que se utilizan identificadores únicos y específicos de los activos para las redes inalámbricas y que todos los identificadores inalámbricos son acrónimos descriptivos que no están obviamente asociados con el sitio del propietario de los activos.	No
	RE2	Asegurar que los dispositivos inalámbricos de los activos que tengan direcciones IP utilicen un direccionamiento estático y tengan desactivados los mecanismos de asignación de direcciones dinámicas (por ejemplo, DHCP).	No

SIS (SP.05)

Requisitos relacionados con un sistema de integración de un sistema instrumentado de seguridad (SIS) en los activos.

ID req	BR/RE	Explicación	D.Req
SP.05.01 Evaluación de riesgos - Verificación	BR	Verificar que se han realizado y abordado las revisiones de la arquitectura de seguridad y/o las evaluaciones de los riesgos de seguridad de las comunicaciones del SIS utilizadas en los activos.	No
SP.05.02 Diseño de la red	BR	Garantizar que las comunicaciones críticas de seguridad del SIS y las funciones de seguridad del SIS estén protegidas de las comunicaciones del BPCS (sistema básico de control de procesos) o de cualquier otro activo.	No
SP.05.03 Diseño de la red	BR	Garantizar que las comunicaciones externas a los activos, incluyendo las comunicaciones de acceso remoto, no puedan interferir con el funcionamiento del SIS.	No
SP.05.04 Diseño de la red	BR	Garantizar que las aplicaciones externas al SIS no puedan participar en las comunicaciones del SIS que son críticas para las funciones de seguridad, o bien interrumpirlas o interferirlas de alguna otra manera.	No
SP.05.05 Estaciones de trabajo	BR	Garantizar que las EWS del SIS que residen fuera del SIS (externas a la interfaz del SIS con el sistema de control) no pueden verse comprometidas por las comunicaciones de nivel 3 (Normas ISA95 e IEC62264-1) o superior.	No
	RE1	Garantizar que las EWS de los activos que residen dentro del SIS (internas a la interfaz del SIS con el sistema de control) no puedan verse comprometidas por el acceso remoto (por ejemplo, RDP).	No

SP.05.06 Estaciones de trabajo	BR	Garantizar que todos los accesos al SIS sean: 1) a través de una pasarela de nivel 2 dedicada al SIS y conectada físicamente a él; y/o 2) desde una EWS del SIS que está físicamente conectada al SIS. Si la EWS del SIS no está conectada físicamente al SIS; su única opción es comunicarse con el SIS a través de pasarela.	No
SP.05.07 Estaciones de trabajo	BR	Garantizar que la EWS se limita a realizar funciones del SIS.	No
SP.05.08 Dispositivos - Inalámbricos	BR	Verificar que no se permitan dispositivos inalámbricos como parte integral de las funciones de seguridad del SIS.	No
SP.05.09 Interfaz de usuario	BR	Garantizar que se proporciona una interfaz de usuario para activar y desactivar el modo de configuración del SIS. Mientras esté bloqueada, esta interfaz debe prohibir la configuración del SIS.	No
	RE1	Garantizar que se proporciona una implementación de hardware de la interfaz que sea capaz de ser bloqueada físicamente mientras el modo de configuración está deshabilitado.	No
	RE2	Capacidad de hacer que una tercera parte independiente verifique que noes posible cambiar la configuración del SIS cuando la interfaz de hardware está bloqueda en le modo de configuración “deshabilitar”.	No

GESTIÓN DE LA CONFIGURACIÓN (SP.06)

Requisitos relacionados con el control de configuración de los activos.

ID req	BR/RE	Explicación	D.Req
SP.06.01 Diseño de la red	BR	Proporcionar gráficos/documentación precisos de la infraestructura lógica y física de los activos, incluyendo sus dispositivos de red, interfaces internas e interfaces externas. La documentación y los gráficos deben mantenerse como una representación exacta.	No
	RE1	Mantener actualizados los documentos de conexión y configuración de los equipos instalados y en funcionamiento.	No
SP.06.02 Registro de inventario	BR	Crear y mantener un registro de inventario SuC (ver anexo 0), incluyendo los números de versión y los números de serie, de todos los dispositivos y sus componentes de software de que es responsable el proveedor de servicios.	No

SP.06.03 Verificación	BR	Verificar que los dispositivos por cable e inalámbricos utilizados para el control y la instrumentación se han configurado correctamente con sus valores aprobados.	No

ACCESO REMOTO (SP.07)

Requisitos relacionados con el acceso remoto a los activos.

ID req	BR/RE	Explicación	D.Req
SP.07.01 Herramientas y software de seguridad	BR	Garantizar que todas las aplicaciones de acceso remoto utilizadas en los activos sean las comúnmente aceptadas por las comunidades de seguridad y de automatización industrial.	No
SP.07.02 Herramientas y software de seguridad	BR	Proporcionar instrucciones detalladas para la instalación, configuración, operación y terminación de las aplicaciones de acceso remoto utilizadas en los activos.	No
SP.07.03 Herramientas y software de seguridad	BR	Proporcionar información sobre todas las conexiones de acceso remoto propuestas al propietario de los activos que incluya, para cada conexión: 1) su propósito; 2) la aplicación de acceso remoto a utilizar; 3) cómo se establecerá la conexión (por ejemplo, a través de Internet mediante una VPN); y 4) la ubicación e identidad del cliente remoto.	No
SP.07.04 Herramientas y software de seguridad	BR	Asegurarse de obtener la aprobación del propietario de los activos antes de utilizar todas y cada una de las conexiones de acceso remoto.	No
	RE1	Garantizar que todas las conexiones de acceso remoto a los activos por parte del proveedor de servicios (por ejemplo, desde una instalación del proveedor de servicios) están autenticadas y cifradas.	No

GESTIÓN DE EVENTOS (SP.08)

Requisitos relacionados con la gestión de eventos en los activos.

ID req	BR/RE	Explicación	D.Req
SP.08.01 Fallos de seguridad	BR	Manejar incidentes de ciberseguridad que afecten a los activos que incluyan: 1) la detección de fallos e incidentes de ciberseguridad; 2) la notificación de los incidentes de ciberseguridad al propietario de los activos; 3) la respuesta a los compromisos e incidentes de ciberseguridad, incluyendo el apoyo a un equipo de respuesta a incidentes.	No
	RE1	Garantizar que los fallos de seguridad que se hayan detectado automáticamente puedan notificarse a través de una interfaz de comunicaciones que sea accesible para el propietario de los activos y que sea comúnmente aceptada por las comunidades de seguridad y de automatización industrial.	No
SP.08.02 Relacionados con la seguridad	BR	Garantizar que los activos estén configurados para registrar todos los eventos relacionados con la seguridad, incluidas las actividades de usuario y las actividades de gestión de cuentas, en un registro de auditoría que se mantiene durante el número de días especificado por el propietario de los activos.	No
	RE1	Garantizar que se pueda acceder a los datos y eventos relacionados con la seguridad a través de una o más interfaces.	No
	RE2	Verificar que, mediante un evento simulado relacionado con la seguridad aprobado por el propietario de los activos, los eventos relacionados con la seguridad pueden recogerse en un registro de auditoría.	No
SP.08.03 Alarmas y eventos	BR	Garantizar que los activos estén configurados para registrar y notificar al operador los eventos relacionados con el proceso según lo requiera el propietario de los activos.	No
	RE1	Garantizar que se pueda informar de las alertas/eventos de manera segura a través de una interfaz.	No
SP.08.04 Alarmas y eventos	BR	Asegurar que los activos sean capaces de soportar la ocurrencia casi simultánea de un gran número de eventos (tormenta de eventos).	Si

GESTIÓN DE CUENTAS (SP.09)

Requisitos relacionados con la administración de cuentas de usuario en los activos.

ID req	BR/RE	Explicación	D.Req
SP.09.01	BR	Garantizar que los activos soporten: 1) la utilización de una base de datos única e integrada, para definir y gestionar las cuentas de usuario y de servicio; 2) la gestión restringida de cuentas a los usuarios autorizados; 3) el acceso descentralizado	No

Cuentas de usuario y de servicio		a esta base de datos para la gestión de cuentas; 4) la aplicación descentralizada de la configuración de las cuentas definidas en esta base de datos.	
SP.09.02 Cuentas de usuario y de servicio	BR	Asegurar que se pueden crear y mantener cuentas únicas para los usuarios.	No
	RE1	Proporcionar documentación al propietario de los activos que: 1) identifique todas las cuentas de usuario y de servicio predeterminadas; 2) describa las herramientas y procedimientos utilizados para establecer/restablecer las contraseñas de todas las cuentas de usuario y de servicio predeterminadas.	Si
	RE2	Garantizar que si se genera automáticamente una cuenta/contraseña para un usuario tanto la cuenta como la contraseña generadas serán únicas.	No
	RE3	Asegurar que las cuentas de servicio, organizadas según lo que requiera el propietario de los activos, se han configurado de manera que nunca caduquen ni se deshabiliten automáticamente.	No
	RE4	Asegurar que la cuenta de administrador incorporada se deshabilite y, si esto no es posible, que se le cambie el nombre o que se dificulte su explotación.	No
SP.09.03 Cuentas predeterminadas	BR	Garantizar que las cuentas predeterminadas no utilizadas en el sistema hayan sido eliminadas o desactivadas.	No
SP.09.04 Usuario	BR	Garantizar que todas las cuentas de usuario se eliminen una vez que ya no se necesiten y notificar al propietario de los activos sobre la eliminación de éstas.	No
	RE1	Generar un informe de registro de auditoría después de la finalización de las actividades de integración/mantenimiento que muestre que las cuentas se han eliminado si ya no son necesarias.	No
SP.09.05 Contraseñas	BR	Garantizar que las políticas de contraseñas puedan establecerse para lograr una complejidad mínima comúnmente aceptada por las comunidades de seguridad y de automatización industrial.	No
SP.09.06 Contraseñas	BR	Garantizar que las contraseñas de las cuentas de usuario locales y de todo el sistema se configuran para que caduquen automáticamente después de haber estado en uso durante un periodo de tiempo especificado por el propietario de los activos.	No
	RE1	Garantizar que las políticas de contraseñas se establezcan para solicitar a los usuarios que cambien las contraseñas N días antes de que caduquen, estando N especificado por el propietario de los activos. Este requisito no se aplica a las contraseñas que no están configuradas para caducar.	No

SP.09.07 Contraseñas	BR	Asegurar que las contraseñas predeterminadas se cambien según lo requiera el propietario de los activos.	No
SP.09.08 Contraseñas	BR	Asegurar que las políticas de contraseñas se establecen para evitar que los usuarios reutilicen sus últimas N contraseñas, estando N especificada por el propietario de los activos.	No
	RE1	Asegurar que las políticas de contraseñas se establecen para evitar que los usuarios cambien sus contraseñas más de una vez cada N días, donde N es especificado por el propietario de los activos.	No
SP.09.09 Contraseñas	BR	Asegurar que las cuentas cuyas contraseñas hayan sido aprobadas por el propietario de los activos para ser compartidas con el proveedor de servicios se encuentran documentadas y se mantienen de manera segura.	No
	RE1	Informar al propietario de los activos sobre las contraseñas que se hayan compartido, divulgado o se hayan visto comprometidas.	No

PROTECCIÓN CONTRA MALWARE (SP.10)

Requisitos relacionados con el uso de software antimalware en los activos.

ID req	BR/RE	Explicación	D.Req
SP.10.01 Proceso manual – Mecanismos protección contra malware	BR	Proporcionar al propietario de los activos instrucciones documentadas para la correcta instalación, configuración y actualización de los mecanismos de protección contra el malware que se prueban y verifican para los activos.	No
SP.10.02 Herramientas y software de seguridad	BR	Garantizar que: 1) los mecanismos de protección contra el malware se han instalado/actualizado y configurado correctamente; 2) los archivos de definición de malware se instalan dentro del período de tiempo acordado con el propietario de los activos; 3) las configuraciones de malware se mantienen y se actualizan.	No
	RE	Crear y mantener la documentación que describe el uso de los mecanismos de protección contra el malware. Esta documentación incluirá: 1) el estado de instalación; 2) los ajustes de configuración; 3) el estado actual de los archivos de definición de malware; 4) el uso de otras características y funciones atenuantes de infecciones.	No
SP.10.03	BR	Verificar que los mecanismos de protección contra el malware instalado pueden detectar y manejar adecuadamente el malware que no sea de día cero.	No

Herramientas y software de seguridad			
SP.10.04 Proceso manual – Archivos de definición de malware	BR	Proporcionar al propietario de los activos la documentación que describa: 1) cómo se evalúan y aprueban los archivos de definición de malware; 2) cómo informar del estado de los archivos de definición de malware al propietario de los activos. Este estado incluye la aplicabilidad y el estado de aprobación.	Si
SP.10.05 Dispositivos	BR	Garantizar que todos los dispositivos, incluidas las estaciones de trabajo, suministrados a los activos por el proveedor de servicios estén libres de malware conocido antes de su uso.	No
	RE1	Garantizar que los medios portátiles que utilice para el ensayo, puesta en marcha y/o mantenimiento del sistema, solo se utilizan para este propósito.	No
	RE2	Garantizar que todos los dispositivos portátiles de almacenamiento y transferencia de datos utilizados o conectados a los activos por el proveedor de servicios estén libres de malware conocido antes de su uso.	No

GESTIÓN DE PARCHES (SP.11)

Requisitos relacionados con los aspectos de seguridad de la aprobación e instalación de parches de software.

ID req	BR/RE	Explicación	D.Req
SP.11.01 Proceso manual – Calificación de parches	BR	Proporcionar documentación al propietario de los activos que describa cómo se evalúan y aprueban los parches de seguridad del software de los activos que es responsable.	Si
	RE1	Revisar, como resultado de los cambios en los riesgos de seguridad, la forma en que evalúa y aprueba los parches de seguridad para el software de los activos del que es responsable.	No
SP.11.02 Lista de parches	BR	Poner a disposición del propietario de los activos la documentación que describe los parches/actualizaciones de seguridad. Debe incluir: 1) parches de seguridad que son aplicables a los componentes; 2) el estado de aprobación/estado del ciclo de vida de cada uno; 3) una advertencia si la aplicación de un parche aprobado requiere o provoca un reinicio del sistema; 4) la razón por las que determinados parches no están aprobados o no son aplicables; 5) un plan de corrección para los que son aplicables, pero no están aprobados.	Si

	RE1	Poner a disposición del propietario de los activos, a través de una interfaz comúnmente aceptada, una lista de parches que identifique: 1) parches de seguridad aprobados aplicables al software de los activos; 2) cuáles de estos han sido aprobados para su uso en los activos; 3) los números de versión del software al que se aplican los parches aprobados.	No
	RE2	El proveedor de servicios debe tener la capacidad de: 1) recomendar un plan de mitigación cuando lo solicite el propietario de los activos para los parches de seguridad que no fueron aprobados por el propietario de los activos, por ejemplo, porque podrían afectar las operaciones o el rendimiento (véase el requisito básico SP 11.05 BR); 2) implementar el plan de mitigación después de la aprobación del propietario de los activos.	No
SP.11.03 Parche de seguridad	BR	Gestionar: 1) parches que el propietario de los activos obtendrá directamente del fabricante del parche; y/o 2) redistribución de parches por parte del proveedor de servicios solo si está aprobado por el propietario de los activos y permitido por el fabricante del parche.	No
SP.11.04 Parche de seguridad	BR	Proporcionar documentación de las instrucciones de como instalar el parche manualmente o cómo utilizar el servidor de gestión de parches.	Si
SP.11.05 Parche de seguridad	BR	El proveedor de servicios debe tener la capacidad de asegurarse de obtener la aprobación del propietario de los activos para instalar todos y cada uno de los parches de seguridad.	No
SP.11.06 Parche de seguridad	BR	Garantizar que el proceso de actualización asegure la autenticidad e integridad del software o firmware de los dispositivos en los que se ejecute.	No
	RE1	Garantizar que el nivel de protección (hardening) de la seguridad de los activos se mantiene después de la instalación del parche, por ejemplo, mediante la reinstalación del software o cambiando los ajustes de configuración del sistema.	No
	RE2	Garantizar que, en el caso de los dispositivos que admiten la instalación de software o firmware en la red, el proceso de actualización asegure la autenticidad e integridad del software o firmware de los dispositivos.	No
	RE3	Determinar el estado de la instalación de todos los parches de seguridad aplicables a los activos de la que es responsable el proveedor de servicios.	No

COPIA DE SEGURIDAD/RESTAURACIÓN (SP.12)

Requisitos relacionados con los aspectos de seguridad de las copias de seguridad y la restauración.

ID req	BR/RE	Explicación	D.Req
SP.12.01 Proceso manual – Descripción técnica	BR	Proporcionar la documentación para los procedimientos de copia de seguridad recomendados para los activos que incluyan: 1) Instrucciones sobre cómo realizar una copia de seguridad completa y seguridad parciales si procede, utilizando al menos uno de los siguientes métodos en las arquitecturas de las copias de seguridad a) patentada en medios extraíbles, b) de un solo sistema en medios extraíbles; c) distribuida d) centralizada. 2) Disposiciones para hacer una copia de seguridad de los siguientes tipos de datos: a)archivos del sistema operativo y datos criptográficos, aplicaciones, datos de configuración, archivos de la base de datos, archivos de registro, libro de registro electrónico, tipos de archivos no convencionales, parámetros de la instrumentación de campo, información de directorio, otros archivos identificados por el proveedor de servicios que se requieran para crear una copia de seguridad completa de los activos. 3) Recomendaciones para el almacenamiento externo de los medios de copia de seguridad. 4) Disposiciones para garantizar que los cambios en los activos que puedan afectar a la integridad de una copia de seguridad no se realicen mientras se esté realizando una copia de seguridad.	Si
SP.12.02 Restauración	BR	Proporcionar instrucciones documentadas al propietario de los activos para restaurar los activos o sus componentes a su funcionamiento normal.	Si
SP.12.03 Dispositivos de almacenamiento portátil	BR	Proporcionar documentación al propietario de los activos que describa cómo controlar y gestionar de forma segura los medios de copia de seguridad extraíbles.	Si
SP.12.04 Copia de seguridad	BR	Proporcionar documentación al propietario de los activos que describa cómo verificar la copia de seguridad del sistema con éxito.	Si
SP.12.05 Restauración	BR	Verificar que: 1) es posible realizar una copia de seguridad completa de los activos; y 2) es posible restablecer los activos completamente funcionales a partir de esta copia de seguridad.	No
SP.12.06 Copia de seguridad	BR	Realizar una copia de seguridad de los activos de acuerdo con los programas de copia de seguridad del propietario de los activos y los objetivos de restauración de datos y recuperación ante desastres.	No

SP.12.07 Copia de seguridad	BR	Garantizar que los activos puedan seguir funcionando normalmente durante una copia de seguridad.	No
SP.12.08 Proceso manual - Registro	BR	Proporcionar documentación al propietario de los activos que describa cómo generar y mantener registros de auditoría de todas las actividades de copia de seguridad y restauración.	Si
SP.12.09 Proceso manual - Recuperación	BR	Documentar un plan recomendado de recuperación ante desastres que incluya, pero no se limite a lo siguiente: 1) Descripción de varios escenarios de desastre y su impacto en los activos. 2) Instrucciones paso a paso para restaurar y reiniciar componentes con fallos e integrarlos en los activos. 3) Requisito mínimo de arquitectura para restaurar los activos al completo.	Si

ANEXO 0: ESPECIFICACIONES SOBRE EL INVENTARIO SuC Y LA EVALUACIÓN DE RIESGO INICIAL

Entregables	**Especificaciones**	
Identificar los activos del SuC	Establecer un perímetro de seguridad y puntos de acceso: - Inventario de sistema - Diagrama de arquitectura de red y flujo de los datos	
Evaluación inicial de los riesgos cibernéticos *Identificar riesgos no reducidos y el impacto que puede tener sobre diferentes aspectos como el impacto para la seguridad/salud, pérdida de producción, interrupción del servicio, entre otros.*	División de las zonas en zonas y conductos	- Agrupar los activos según diferentes criterios como la evaluación de riesgos, criticidad de los activos, ubicación física o lógica, el acceso requerido o la organización responsable. Prestar atención a los sistemas inalámbricos, los dispositivos con puntos de conexión de Internet, los que interactúan con la IACS gestionados por otras entidades y dispositivos móviles. - Separar en zonas lógicas y/o físicas los activos de la IACS de los de la empresa. - Intentar separar los activos de la IACS que están relacionados con la seguridad de los que no, cuando sea posible, si no lo es, identificar todo el conjunto como activo de seguridad, ya que necesita un nivel mayor de protección. - Separar los activos conectados temporalmente de los que no, si estos activos se usan con otros dispositivos, no se aplica a dispositivos que no se utilizan fueran de estos sistemas. - Separar dispositivos inalámbricos de los que funcionan por cable, por ejemplo, a través de un firewall. -Separar los dispositivos que están conectados al sistema a través de conexiones externas.
	Comparación de riesgos	- Si el riesgo inicial sobrepasa el riesgo tolerable se debe realizar una evaluación detallada. -Se pueden agrupar zonas que tengan amenazas compartidas y aplicar diseños que se hayan utilizado con anterioridad para ese nivel de amenaza y que las haya mitigado.
	Identificar las amenazas	- Identificar las vulnerabilidades y los puntos de acceso - Determinar el impacto y consecuencias ▪ Analizar el coste y beneficios de los controles de seguridad, medición cualitativa o cuantitativa.

	Listar de forma detallada y realista las amenazas (describir la fuente, la capacidad de la fuente, vectores y activos afectados)	- Determinar la probabilidad no mitigada ▪ Probabilidad de que las amenazas se materialicen teniendo en cuenta el historial, la motivación de la fuente, las vulnerabilidades conocidas, etc. - Determinar el riesgo no mitigado ▪ Determinar combinando la probabilidad no mitigada el impacto. - Determinar el nivel de seguridad objetivo. ▪ El método para determinarlo es a elección. - Comparar el riesgo no mitigado con el riesgo no tolerable ▪ Determinar si el riesgo se transfiere, mitiga o acepta. - Identificar y evaluar las contramedidas existentes ▪ Evaluar la eficacia de las mismas en el impacto. - Reevaluar la probabilidad y el impacto - Determinar el riesgo residual ▪ Se determina combinando la probabilidad mitigada y el impacto mitigado actual - Comparar el riesgo actual con el riesgo tolerable. - Identificar contramedidas adicionales de seguridad cibernéticas - Documentar y comunicar los resultados ▪ Diagramas de arquitectura del sistema, las evaluaciones de la vulnerabilidad y fuentes de información de las amenazas

	Documentar los requisitos, las hipótesis y las restricciones de seguridad cibernética	- Especificación de los requisitos de seguridad cibernética ▪ Descripción del SUC ▪ Diagramas de zonas y conductos ▪ Características de las zonas y conductos a) Nombre y/o identificador único b) Organización/es responsable/s c) Definición del límite lógico y físico, si corresponde d) Designación de seguridad e) Lista de todos los puntos de acceso lógicos y físicos f) Lista de flujo de datos asociados a cada punto de acceso g) Zonas o conductos conectados h) Lista de activos y su clasificación, criticidad y valor de negocio i) Nivel de seguridad objetivo j) Requisitos de seguridad aplicables k) Políticas de seguridad aplicables l) Hipótesis y dependencias externas ▪ Hipótesis del entorno de funcionamiento ▪ Entorno de amenazas ▪ Políticas de seguridad de la organización ▪ Riesgo tolerable ▪ Requisitos reglamentarios - Entorno de amenaza ▪ Incluir amenazas actuales como futuras, por ejemplo, clima geopolítico, entorno físico y sensibilidad del sistema. - Políticas de seguridad de la organización ▪ Contramedidas y elementos de seguridad implementados - Riesgo tolerable - Requisitos reglamentarios ▪ Importante para el cumplimiento de la normativa.

ANEXO I: REQUISITOS PARA NIVEL SL1

Requisitos de seguridad del sistema

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
SR 1.1	BR	Todos los usuarios que accedan al sistema han de ser identificados y autenticados tanto a nivel de sistemas como de aplicación puede ser a través de contraseñas, dispositivos de acceso o multifactor (combinación de las anteriores).
SR 1.3	BR	El sistema de control debe tener la capacidad de gestionar cuentas de usuarios (agregar, eliminar, modificar o desactivar) estableciendo condiciones para pertenecer a un grupo y la asignación de autorizaciones. Sólo se admitirán cuentas compartidas, cuando por condiciones del sistema se establezca en el análisis de riesgo, aunque deberán de establecerse contramedidas y documentarlas.
SR 1.4	BR	El sistema de control debe proporcionar la capacidad de admitir la gestión de los identificadores (permite operar dentro de un dominio o zona de control específico del sistema) por usuario, grupo, rol o interfaz del sistema de control.
SR 1.5	BR	El sistema de control debe proporcionar la capacidad de: 1) iniciar el contenido del autenticador; 2) cambiar todos los autenticadores predeterminados; 3) cambiar/actualizar los autenticadores; 4) protegerlos contra la divulgación y modificación no autorizada. Ejemplos de autenticadores son claves físicas, tarjetas de acceso, claves privadas, entre otras.
SR 1.6	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar a todos los usuarios que participen en una comunicación inalámbrica. Ejemplos de tecnologías inalámbricas son Bluetooth, infrarrojos, enrutadores móviles, etc.
SR 1.7	BR	En los sistemas de control que utilicen la contraseña como medio de autenticación debe aplicar una fortaleza configurable en base a la longitud mínima y la variedad de caracteres. Se aplicará vigencia máxima para las contraseñas y se notificará cuando esta expire. Esta protección se puede mejorar limitando la reutilización de las contraseñas.
SR 1.10	BR	El sistema de control debe proporcionar la capacidad de ocultar la retroalimentación de la información de autenticación durante el proceso. No debe dar pistas sobre los fallos de autenticación como, por ejemplo, “nombre de usuario desconocido”
SR 1.11	BR	El sistema de control debe proporcionar la capacidad de aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por cualquier usuario dentro de un periodo configurable de tiempo.
SR 1.12	BR	El sistema de control debe proporcionar la capacidad de mostrar un mensaje de aviso del sistema antes de la autenticación. El personal autorizado debe poder configurar el mensaje de aviso de uso del sistema.
SR 1.13	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza. Debe permitir el acceso sólo cuando se esté autorizado y restringir el acceso desde conexiones telefónicas o no autorizadas. Es posible que los procedimientos requieran la autenticación multifactor para permitir el acceso remoto.

FR2. Control de uso		
SR 2.1	BR	El sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control a fin de admitir el reparto de tareas y el privilegio mínimo. Verificar que las acciones del usuario están permitidas según el rol asignado y permitir que solo las personas cualificadas y autorizadas realicen cambios en los componentes del sistema.
SR 2.2	BR	El sistema de control debe proporcionar la capacidad de autorizar, supervisar y aplicar las restricciones de uso para las conexiones inalámbricas al sistema de control con arreglo a las prácticas comúnmente aceptadas en el sector de la seguridad.
SR 2.3	BR	El sistema de control debe proporcionar la capacidad de aplicar automáticamente las restricciones de uso configurables, que incluyen: a) prevenir el uso de dispositivos portátiles y móviles; b) requerir autorización basada en un contexto específico; y c) restringir la transferencia de códigos y datos a/de dispositivos portátiles y móviles.
SR 2.4	BR	El sistema de control debe proporcionar la capacidad de aplicar restricciones de uso para las tecnologías de código móvil basadas en la posibilidad de que causen daños al sistema de control, incluyendo: a) prevenir la ejecución del código móvil; b) requerir procesos de autenticación y autorización adecuados para el origen del código; c) restringir la transferencia del código móvil a/del sistema de control; y d) supervisar el uso del código móvil.
SR 2.5	BR	El sistema de control debe proporcionar la capacidad de evitar un acceso posterior iniciando un bloqueo de la sesión tras un período de tiempo configurable de inactividad o mediante iniciación manual. La sesión debe continuar bloqueada hasta que el usuario autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados. En los casos en los que el sistema de control no pueda admitir el bloqueo de la sesión, la entidad responsable debería emplear las contramedidas compensatorias que se consideren adecuadas como mayores medidas de seguridad física y auditorias.
SR 2.8	BR	El sistema de control debe proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de copias de seguridad y restauración, cambios en la configuración, actividad potencial de reconocimiento y eventos del registro de auditoría. Los registros individuales de auditoría deben incluir la marca de tiempo, fuente (dispositivo, proceso de software o cuenta de usuario humano de origen), categoría, tipo, identificador del evento y resultado del evento.
SR 2.9	BR	El sistema de control debe asignar una capacidad suficiente de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocida para la gestión de registros y la configuración del sistema. El sistema de control debe proporcionar mecanismos de auditoría para reducir la posibilidad de que se exceda dicha capacidad.
SR 2.10	BR	El sistema de control debe proporcionar la capacidad de alertar al personal y evitar la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de auditorías. El sistema de control debe proporcionar la capacidad de admitir las acciones apropiadas en respuesta a un fallo en el procesamiento de auditorías de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.

FR3. Integridad del sistema		
SR 3.1	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el sistema para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
SR 3.2	BR	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección para prevenir, detectar, mitigar e informar de los efectos de un código malicioso o de software no autorizado. El sistema de control debe proporcionar la capacidad de actualizar los mecanismos de protección.
SR 3.3	BR	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad (medidas de antivirus, identificación, detección de intrusos y auditorias) e informar de las anomalías que se produzcan durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado. Las funciones de seguridad deben incluir todas las funciones que sean necesarias para cumplir con los requisitos de seguridad especificados en esta norma.
SR 3.5	BR	El sistema de control debe validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que tengan un impacto directo en la acción del sistema de control. Las directrices a tener en cuenta deberían incluir la Code Review Guide del Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control debe proporcionar la capacidad de establecer el valor de salida a un estado predeterminado si no se puede mantener el funcionamiento normal como resultado de un ataque.
FR4. Confidencialidad de los datos		
SR 4.1	BR	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información (especialmente en dispositivos portátiles) para la que se admite la autorización explícita de lectura, ya esté en reposo o en tránsito. La técnica elegida tenga en cuenta las posibles ramificaciones en el rendimiento del sistema de control y la capacidad de recuperarse tras un fallo del sistema o un ataque.
SR 4.3	BR	Si se requiere el uso de criptografía, el sistema de control debe usar algoritmos criptográficos, tamaños de clave y mecanismos para el establecimiento y gestión de claves con arreglo a las prácticas y recomendaciones de seguridad comúnmente aceptadas en el sector que se encuentran en documentos como la Publicación Especial NIST SP800-57
FR5. Flujo de datos restringidos		
SR 5.1	BR	El sistema de control debe proporcionar la capacidad de segmentar de manera lógica las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de otras redes del sistema de control.
SR 5.2	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas y conductos de riesgo. Como parte de una estrategia de protección de defensa total, se deberían dividir los sistemas de control de mayor impacto en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red con arreglo a las políticas y procedimientos de seguridad y a una evaluación de riesgos.

SR 5.3	BR	Un sistema de control debe proporcionar la capacidad de evitar la recepción de mensajes de propósito general (correo electrónico, redes sociales o cualquier otro sistema de mensajería) entre personas recibidos de usuarios o sistemas externos al sistema de control.
SR 5.4	BR	El sistema de control debe proporcionar la capacidad de admitir la partición de datos (por medios físicos o lógicos), aplicaciones y servicios en base a su criticidad para facilitar la implementación de un modelo de zonificación.
FR6. Respuesta oportuna a los incidentes		
SR 6.1	BR	El sistema de control debe proporcionar la capacidad de que las personas y/o las herramientas autorizadas accedan a los registros de auditoría en modo de lectura.
FR7. Disponibilidad de los recursos		
SR 7.1	BR	El sistema de control debe proporcionar la capacidad de funcionar en modo degradado durante un evento de denegación de servicio. Un evento de denegación de servicio en el sistema de control no debería afectar negativamente a ningún sistema relacionado con la seguridad.
SR 7.2	BR	El sistema de control debe proporcionar la capacidad de limitar el uso de recursos por parte de las funciones de seguridad para evitar el agotamiento de los recursos.
SR 7.3	BR	El sistema de control debe facilitar la identidad y ubicación de los archivos críticos y la capacidad de llevar a cabo copias de seguridad de la información a nivel del usuario y del sistema (incluyendo información sobre el estado del sistema) sin que esto afecte a las operaciones habituales.
SR 7.4	BR	El sistema de control debe proporcionar la capacidad de recuperarse y reconstituirse hasta un estado seguro conocido después de una interrupción o fallo. Un estado seguro conocido significa que se atribuyen a todos los parámetros del sistema (ya sean predeterminados o configurables) valores seguros, se reinstalan los parches críticos para la seguridad, se restablecen los ajustes de configuración relacionados con la seguridad, se dispone de la documentación y los procedimientos operativos del sistema, se reinstala y configura la aplicación y el software del sistema con ajustes seguros, se carga la información de las copias de seguridad más recientes y conocidas y se somete a ensayo y se comprueba el funcionamiento del sistema en su totalidad.
SR 7.5	BR	El sistema de control debe proporcionar la capacidad de cambiar de y a una fuente de alimentación de emergencia sin que esto afecte el estado de seguridad existente o un modo degradado documentado.
SR 7.6	BR	El sistema de control debe proporcionar la capacidad de ser configurado de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El sistema de control debe proporcionar una interfaz a los ajustes de configuración de red y seguridad desplegados actualmente.
SR 7.7	BR	El sistema de control debe proporcionar la capacidad de prohibir y/o restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.

Requisitos de seguridad del componente generales

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
CR 1.1	BR	Los componentes deben proporcionar la capacidad de identificar y autenticar a todos los usuarios en todas las interfaces que permita el reparto de tareas y los privilegios mínimos. Se puede proporcionar a nivel componente o a nivel sistema.
CR 1.3	BR	Los componentes deben proporcionar la capacidad de permitir la gestión de todas las cuentas de forma directa o integrándose en un sistema que gestione las cuentas.
CR 1.4	BR	Los componentes deben proporcionar la capacidad de integrarse en un sistema que soporte la gestión de identificadores y/o la capacidad de permitir la gestión de identificadores.
CR 1.5	BR	Los componentes deben proporcionar la capacidad de: a) permitir el uso del contenido inicial del autenticador; b) permitir el reconocimiento de los cambios en los autenticadores predeterminados realizados en el momento de la instalación; c) funcionar correctamente con operaciones periódicas de modificación/actualización de los autenticadores; y d) proteger a los autenticadores de la divulgación y modificación no autorizada cuando se almacenan, utilizan y transmiten.
CR 1.7	BR	Los componentes que utilicen autenticación basada en contraseña, deben proporcionar o integrarse en un sistema que proporcione la capacidad de aplicar la fortaleza de las contraseñas configurables de acuerdo con directrices de contraseñas reconocidas y probadas internacionalmente.
CR 1.10	BR	Cuando un componente ofrezca la capacidad de autenticación, el componente debe ofrecer la capacidad de ocultar la retroalimentación de la información del autenticador durante el proceso de autenticación.
CR 1.11	BR	Cuando un componente ofrezca una capacidad de autenticación, el componente debe proporcionar la capacidad de: a) aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por parte de cualquier usuario durante un período de tiempo configurable; b) denegar el acceso durante un período de tiempo específico o hasta que un administrador lo desbloquee cuando se haya alcanzado este límite. Un administrador puede desbloquear una cuenta antes de la caducidad del período de tiempo de espera.
CR 1.12	BR	Cuando un componente proporcione un acceso de usuario humano local/IHM, debe proporcionar la capacidad de mostrar un mensaje de notificación de uso del sistema antes de la autenticación. Personal autorizado debe poder configurar el mensaje de notificación de uso del sistema.
FR2. Control de uso		
CR 2.1	BR	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios identificados y autenticados en función de las responsabilidades que se les hayan asignado.

CR 2.2	BR	Si un componente soporta el uso a través de interfaces inalámbricas, debe proporcionar la capacidad de integrarse en el sistema que soporta la autorización de uso, la supervisión y las restricciones de acuerdo con las prácticas industriales comúnmente aceptadas.
CR 2.5	BR	Si un componente proporciona una interfaz para un usuario humano, tanto si se accede localmente como a través de una red, el componente debe proporcionar la capacidad de: a)protegerse contra el acceso posterior iniciando un bloqueo de sesión después de un período de tiempo configurable de inactividad o mediante la iniciación manual por parte del usuario y b)mantener el bloqueo de la sesión hasta que el usuario propietario de la sesión, u otro usuario humano autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados.
CR 2.8	BR	Los componentes deben proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: a) control de acceso; b) errores de solicitud; c) eventos del sistema de control; d) evento de copia de seguridad y restauración; e) cambios de configuración; y f) eventos de registro de auditoría. Los registros de auditoría individuales deben incluir: a) marca de tiempo; b) fuente (dispositivo de origen, proceso de software o cuenta de usuario humano); c) categoría; d) tipo; e) ID del evento; y f) resultado del evento.
CR 2.9	BR	Los componentes deben: a) proporcionar la capacidad de asignar una capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros; y b) proporcionar mecanismos para proteger contra un fallo del componente cuando alcance o supere la capacidad de almacenamiento de datos de auditoría.
CR 2.10	BR	Los componentes deben: a) proporcionar la capacidad de proteger contra la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de una auditoría; y b) proporcionar la capacidad para permitir las acciones apropiadas en respuesta a un fallo en el procesamiento de una auditoría de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
CR 2.11	BR	Los componentes deben proporcionar la capacidad de crear marcas de tiempo (incluyendo fecha y hora) para su uso en los registros de auditoría.
CR 2.12	BR	Si un componente proporciona una interfaz para un usuario humano, el componente debe proporcionar la capacidad de determinar si un determinado usuario humano ha realizado una determinada acción. Los elementos de control que no puedan permitir tal capacidad se deben enumerar en los documentos de los componentes.
FR3. Integridad del sistema		
CR 3.1	BR	Los componentes deben proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el componente para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
CR 3.3	BR	Los componentes deben proporcionar la capacidad de permitir la verificación de la operación prevista de las funciones de seguridad de acuerdo con el requisito del sistema.

CR 3.4	BR	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de integridad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de integridad.
CR 3.5	BR	Los componentes deben validar la sintaxis, la longitud y el contenido de cualquier dato de entrada que se utilice como entrada de control de procesos industriales o entrada a través de interfaces externas que tengan un impacto directo en la acción del componente.
CR 3.6	BR	Los componentes que se conectan física o lógicamente a un proceso de automatización deben proporcionar la capacidad de establecer salidas a un estado predeterminado si no se puede mantener el funcionamiento normal definido por el proveedor de componentes.
CR 3.7	BR	Los componentes deben identificar y tratar las condiciones de error de manera que no proporcionen información que pueda ser aprovechada por adversarios para atacar el sistema de control.
FR4. Confidencialidad de los datos		
CR 4.1	BR	Los componentes deben: a proporcionar la capacidad de proteger la confidencialidad de la información en reposo para la que se admite la autorización explícita de lectura; y b) permitir la protección de la confidencialidad de la información en tránsito, como se define en el requisito del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.3	BR	Si se requiere el uso de criptografía, el componente debe utilizar mecanismos de seguridad criptográfica de acuerdo con prácticas y recomendaciones de seguridad internacionalmente reconocidas y probadas.
FR5. Flujo de datos restringidos		
CR 5.1	BR	Los componentes deben permitir una red segmentada que admitan zonas y conductos, según sea necesario, para permitir una arquitectura de red más amplia basada en la segmentación lógica y la criticidad.
FR6. Respuesta oportuna a los incidentes		
CR 6.1	BR	Los componentes deben proporcionar la capacidad para que las personas y/o las herramientas autorizadas puedan acceder a los registros de auditoría de solo lectura.
FR7. Disponibilidad de los recursos		
CR 7.1	BR	Los componentes deben proporcionar la capacidad de mantener las funciones esenciales cuando operen en modo degradado como resultado de un evento de denegación de servicio.
CR 7.2	BR	Los componentes deben proporcionar la capacidad de limitar el uso de recursos en las funciones de seguridad para proteger contra el agotamiento de los recursos.
CR 7.3	BR	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.

CR 7.4	BR	Los componentes deben proporcionar la capacidad de poder ser recuperados y reconstituidos hasta un estado de seguridad conocido después de una interrupción o fallo.
CR 7.6	BR	Los componentes deben proporcionar la capacidad de poder ser configurados de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El componente debe proporcionar una interfaz con los ajustes de configuración de red y seguridad actualmente desplegados.
CR 7.7	BR	Los componentes deben proporcionar la capacidad de restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.

Requisitos de seguridad del componente a nivel de software

ID req	BR/RE	Explicación
SAR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
SAR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.

Requisitos de seguridad para los dispositivos integrados (PLCs, IED)

ID req	BR/RE	Explicación
EDR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
EDR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.
EDR 3.10	BR	El dispositivo integrado debe admitir la capacidad de ser actualizado y someterse a una subida de nivel.
EDR 3.14	BR	Los dispositivos integrados deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el arranque del componente y los procesos en tiempo de ejecución antes de su uso.

Requisitos de seguridad para los dispositivos Host

ID req	BR/RE	Explicación
HDR 2.4	BR	En caso de que un dispositivo host utilice tecnologías de código móvil, dicho dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo host: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a cargar código móvil en el dispositivo host; y c) controlar la ejecución del código basándose en comprobaciones de integridad en el código móvil y antes de que el código se ejecute.
HDR 3.2	BR	Los dispositivos host deben contar con mecanismos homologados por el proveedor de productos del sistema de control que garanticen la protección contra códigos maliciosos. El proveedor del producto del sistema de control debe documentar cualquier requisito especial de configuración relacionado con la protección contra el código malicioso.
HDR 3.10	BR	Los dispositivos host deben contar con la capacidad de ser actualizados y someterse a una subida de nivel.
HDR 3.14	BR	Los dispositivos host deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos de red

ID req	BR/RE	Explicación
NDR 1.6	BR	Un dispositivo de red que permita la gestión de acceso inalámbrico debe proporcionar la capacidad de identificar y autenticar a todos los usuarios (personas, procesos de software o dispositivos) que participan en la comunicación inalámbrica.
NDR 1.13	BR	El dispositivo de red que permita el acceso de dispositivos a una red debe poder supervisar y controlar todos los métodos de acceso al dispositivo de red a través de redes que no son de confianza.
NDR 2.4	BR	En caso de que un dispositivo de red utilice tecnologías de código móvil, el dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo de red: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil hacia/desde el dispositivo de red; y c) controlar la ejecución del código basándose en verificaciones de integridad antes de que el código se ejecute
NDR 3.2	BR	El dispositivo de red debe proporcionar protección contra códigos maliciosos.
NDR 3.10	BR	Los dispositivos de red deben admitir la capacidad de ser actualizados y someterse a una subida de nivel.

NDR 3.14	BR	Los dispositivos de red deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
NDR 5.2	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas de riesgo y conductos.
NDR 5.3	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de proteger contra la recepción de mensajes de propósito general entre personas recibidos de usuarios o sistemas externos al sistema de control.

ANEXO II: REQUISITOS PARA NIVEL SL2

Requisitos de seguridad del sistema

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
SR 1.1	BR	Todos los usuarios que accedan al sistema han de ser identificados y autenticados tanto a nivel de sistemas como de aplicación puede ser a través de contraseñas, dispositivos de acceso o multifactor (combinación de las anteriores).
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios humanos.
SR 1.2	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar todos los procesos de software y dispositivos. Esta capacidad debe hacer cumplir dicha identificación y autenticación en todas las interfaces que proporcionen acceso al sistema de control para permitir los privilegios mínimos, de conformidad con las políticas y procedimientos de seguridad aplicables.
SR 1.3	BR	El sistema de control debe tener la capacidad de gestionar cuentas de usuarios (agregar, eliminar, modificar o desactivar) estableciendo condiciones para pertenecer a un grupo y la asignación de autorizaciones. Sólo se admitirán cuentas compartidas, cuando por condiciones del sistema se establezca en el análisis de riesgo, aunque deberán de establecerse contramedidas y documentarlas.
SR 1.4	BR	El sistema de control debe proporcionar la capacidad de admitir la gestión de los identificadores (permite operar dentro de un dominio o zona de control específico del sistema) por usuario, grupo, rol o interfaz del sistema de control.
SR 1.5	BR	El sistema de control debe proporcionar la capacidad de: 1) iniciar el contenido del autenticador; 2) cambiar todos los autenticadores predeterminados; 3) cambiar/actualizar los autenticadores; 4) protegerlos contra la divulgación y modificación no autorizada. Ejemplos de autenticadores son claves físicas, tarjetas de acceso, claves privadas, entre otras.
SR 1.6	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar a todos los usuarios que participen en una comunicación inalámbrica. Ejemplos de tecnologías inalámbricas son Bluetooth, infrarrojos, enrutadores móviles, etc.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios personas, procesos de o dispositivos) que participen en la comunicación inalámbrica.
SR 1.7	BR	En los sistemas de control que utilicen la contraseña como medio de autenticación debe aplicar una fortaleza configurable en base a la longitud mínima y la variedad de caracteres. Se aplicará vigencia máxima para las contraseñas y se notificará cuando esta expire. Esta protección se puede mejorar limitando la reutilización de las contraseñas.
SR 1.8	BR	En los casos en los que se utilice una PKI, el sistema de control debe proporcionar la capacidad de que una PKI funcione con arreglo a las mejores prácticas comúnmente aceptadas u obtener certificados de clave pública de una PKI existente. El registro de esta debe

		incluir la autorización de un supervisor que verifique la identidad del titular del certificado y que garantice que se emite al usuario previsto.
SR 1.9	BR	En el caso de los sistemas de control que utilicen autenticación de clave pública (PKI), el sistema de control debe proporcionar la capacidad de: l) validar los certificados comprobando la validez de la firma de un certificado determinado; m) validar los certificados a través de una ruta de certificación a una CA aceptada o, en el caso de los certificados autofirmados, desplegando certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; n)validar los certificados comprobando el estado de revocación de un certificado determinado; o)establecer el control del usuario sobre la clave privada correspondiente; y p)asignar la identidad autenticada a un usuario.
SR 1.10	BR	El sistema de control debe proporcionar la capacidad de ocultar la retroalimentación de la información de autenticación durante el proceso. No debe dar pistas sobre los fallos de autenticación como, por ejemplo, "nombre de usuario desconocido"
SR 1.11	BR	El sistema de control debe proporcionar la capacidad de aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por cualquier usuario dentro de un periodo configurable de tiempo.
SR 1.12	BR	El sistema de control debe proporcionar la capacidad de mostrar un mensaje de aviso del sistema antes de la autenticación. El personal autorizado debe poder configurar el mensaje de aviso de uso del sistema.
SR 1.13	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza. Debe permitir el acceso sólo cuando se esté autorizado y restringir el acceso desde conexiones telefónicas o no autorizadas. Es posible que los procedimientos requieran la autenticación multifactor para permitir el acceso remoto.
	RE1	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza.
FR2. Control de uso		
SR 2.1	BR	El sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control a fin de admitir el reparto de tareas y el privilegio mínimo. Verificar que las acciones del usuario están permitidas según el rol asignado y permitir que solo las personas cualificadas y autorizadas realicen cambios en los componentes del sistema.
	RE1	En todas las interfaces, el sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios (personas, procesos de software y dispositivos) para controlar el uso del sistema de control con el fin de admitir el reparto de tareas y el privilegio mínimo.
	RE2	El sistema de control debe proporcionar de que un usuario o rol autorizado defina y modifique la asignación de permisos a roles para todos los usuarios humanos.

SR 2.2	BR	El sistema de control debe proporcionar la capacidad de autorizar, supervisar y aplicar las restricciones de uso para las conexiones inalámbricas al sistema de control con arreglo a las prácticas comúnmente aceptadas en el sector de la seguridad.
SR 2.3	BR	El sistema de control debe proporcionar la capacidad de aplicar automáticamente las restricciones de uso configurables, que incluyen: a) prevenir el uso de dispositivos portátiles y móviles; b) requerir autorización basada en un contexto específico; y c) restringir la transferencia de códigos y datos a/de dispositivos portátiles y móviles.
SR 2.4	BR	El sistema de control debe proporcionar la capacidad de aplicar restricciones de uso para las tecnologías de código móvil basadas en la posibilidad de que causen daños al sistema de control, incluyendo: a) prevenir la ejecución del código móvil; b) requerir procesos de autenticación y autorización adecuados para el origen del código; c) restringir la transferencia del código móvil a/del sistema de control; y d) supervisar el uso del código móvil.
SR 2.5	BR	El sistema de control debe proporcionar la capacidad de evitar un acceso posterior iniciando un bloqueo de la sesión tras un período de tiempo configurable de inactividad o mediante iniciación manual. La sesión debe continuar bloqueada hasta que el usuario autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados. En los casos en los que el sistema de control no pueda admitir el bloqueo de la sesión, la entidad responsable debería emplear las contramedidas compensatorias que se consideren adecuadas como mayores medidas de seguridad física y auditorias.
SR 2.6	BR	El sistema de control debe proporcionar la capacidad de terminar una sesión remota, ya sea automáticamente después de un período de inactividad configurable o manualmente por parte del usuario que inició la sesión.
SR 2.8	BR	El sistema de control debe proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de copias de seguridad y restauración, cambios en la configuración, actividad potencial de reconocimiento y eventos del registro de auditoría. Los registros individuales de auditoría deben incluir la marca de tiempo, fuente (dispositivo, proceso de software o cuenta de usuario humano de origen), categoría, tipo, identificador del evento y resultado del evento.
SR 2.9	BR	El sistema de control debe asignar una capacidad suficiente de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros y la configuración del sistema. El sistema de control debe proporcionar mecanismos de auditoría para reducir la posibilidad de que se exceda dicha capacidad.
SR 2.10	BR	El sistema de control debe proporcionar la capacidad de alertar al personal y evitar la pérdida de servicios y funciones esenciales en caso de que falle procesamiento auditorías. El sistema de control debe proporcionar la capacidad de admitir las acciones apropiadas en respuesta a un fallo en el procesamiento de auditorías de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
SR 2.11	BR	El sistema de control debe proporcionar marcas de tiempo (fecha y hora) para la generación de registros de auditoría. Evitar que las fuentes horarias sufran alteraciones no autorizadas.

FR3. Integridad del sistema		
SR 3.1	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el sistema para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
SR 3.2	BR	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección para prevenir, detectar, mitigar e informar de los efectos de un código malicioso o de software no autorizado. El sistema de control debe proporcionar la capacidad de actualizar los mecanismos de protección.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección contra códigos maliciosos en todos los puntos de entrada y salida.
SR 3.3	BR	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad (medidas de antivirus, identificación, detección de intrusos y auditorias) e informar de las anomalías que se produzcan durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado. Las funciones de seguridad deben incluir todas las funciones que sean necesarias para cumplir con los requisitos de seguridad especificados en esta norma.
SR 3.4	BR	El sistema de control debe proporcionar la capacidad de detectar, registrar, informar y proteger contra cambios no autorizados en el software y en la información en reposo.
SR 3.5	BR	El sistema de control debe validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que tengan un impacto directo en la acción del sistema de control. Las directrices a tener en cuenta deberían incluir la Code Review Guide del Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control debe proporcionar la capacidad de establecer el valor de salida a un estado predeterminado si no se puede mantener el funcionamiento normal como resultado de un ataque.
SR 3.7	BR	El sistema de control debe identificar y tratar las condiciones de error de manera tal que se pueda aplicar un remedio efectivo. Esto se debe hacer sin proporcionar información que pueda ser aprovechada por adversarios para atacar el sistema de control, a no ser que sea necesario para resolver los problemas de manera oportuna.
SR 3.8	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de las sesiones. El sistema de control debe rechazar cualquier uso por parte de identificadores de sesión no válidos.
SR 3.9	BR	El sistema de control debe proteger la información y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
SR 4.1	BR	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información (especialmente en dispositivos portátiles) para la que se admite la autorización explícita de lectura, ya esté en reposo o en tránsito. La técnica elegida

		tenga en cuenta las posibles ramificaciones en el rendimiento del sistema de control y la capacidad de recuperarse tras un fallo del sistema o un ataque.
	RE1	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información en reposo y en sesiones con acceso remoto a través de una red que no es de confianza.
SR 4.2	BR	El sistema de control debe proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura de los componentes que vayan a ser liberados del servicio activo y/o puestos fuera de servicio.
SR 4.3	BR	Si se requiere el uso de criptografía, el sistema de control debe usar algoritmos criptográficos, tamaños de clave y mecanismos para el establecimiento y gestión de claves con arreglo a las prácticas y recomendaciones de seguridad comúnmente aceptadas en el sector que se encuentran en documentos como la Publicación Especial NIST SP800-57
FR5. Flujo de datos restringidos		
SR 5.1	BR	El sistema de control debe proporcionar la capacidad de segmentar de manera lógica las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de otras redes del sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de segmentar físicamente las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de las redes no críticas del sistema de control.
SR 5.2	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas y conductos de riesgo. Como parte de una estrategia de protección de defensa total, se deberían dividir los sistemas de control de mayor impacto en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red con arreglo a las políticas y procedimientos de seguridad y a una evaluación de riesgos.
	RE1	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
SR 5.3	BR	Un sistema de control debe proporcionar la capacidad de evitar la recepción de mensajes de propósito general (correo electrónico, redes sociales o cualquier otro sistema de mensajería) entre personas recibidos de usuarios o sistemas externos al sistema de control.
SR 5.4	BR	El sistema de control debe proporcionar la capacidad de admitir la partición de datos (por medios físicos o lógicos), aplicaciones y servicios en base a su criticidad para facilitar la implementación de un modelo de zonificación.
FR6. Respuesta oportuna a los incidentes		
SR 6.1	BR	El sistema de control debe proporcionar la capacidad de que las personas y/o las herramientas autorizadas accedan a los registros de auditoría en modo de lectura.

SR 6.2	BR	El sistema de control debe proporcionar la capacidad de supervisar continuamente el rendimiento del mecanismo de seguridad utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
SR 7.1	BR	El sistema de control debe proporcionar la capacidad de funcionar en modo degradado durante un evento de denegación de servicio. Un evento de denegación de servicio en el sistema de control no debería afectar negativamente a ningún sistema relacionado con la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar las cargas de comunicación (por ejemplo, limitando la tasa) para mitigar los efectos de los tipos de desbordamiento de información de los eventos de denegación de servicio.
SR 7.2	BR	El sistema de control debe proporcionar la capacidad de limitar el uso de recursos por parte de las funciones de seguridad para evitar el agotamiento de los recursos.
SR 7.3	BR	El sistema de control debe facilitar la identidad y ubicación de los archivos críticos y la capacidad de llevar a cabo copias de seguridad de la información a nivel del usuario y del sistema (incluyendo información sobre el estado del sistema) sin que esto afecte a las operaciones habituales.
	RE1	El sistema de control debe proporcionar la capacidad de verificar la fiabilidad de los mecanismos de copias de seguridad.
SR 7.4	BR	El sistema de control debe proporcionar la capacidad de recuperarse y reconstituirse hasta un estado seguro conocido después de una interrupción o fallo. Un estado seguro conocido significa que se atribuyen a todos los parámetros del sistema (ya sean predeterminados o configurables) valores seguros, se reinstalan los parches críticos para la seguridad, se restablecen los ajustes de configuración relacionados con la seguridad, se dispone de la documentación y los procedimientos operativos del sistema, se reinstala y configura la aplicación y el software del sistema con ajustes seguros, se carga la información de las copias de seguridad más recientes y conocidas y se somete a ensayo y se comprueba el funcionamiento del sistema en su totalidad.
SR 7.5	BR	El sistema de control debe proporcionar la capacidad de cambiar de y a una fuente de alimentación de emergencia sin que esto afecte el estado de seguridad existente o un modo degradado documentado.
SR 7.6	BR	El sistema de control debe proporcionar la capacidad de ser configurado de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El sistema de control debe proporcionar una interfaz a los ajustes de configuración de red y seguridad desplegados actualmente.
SR 7.7	BR	El sistema de control debe proporcionar la capacidad de prohibir y/o restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
SR 7.8	BR	El sistema de control debe proporcionar la capacidad de informar de la lista actual de componentes instalados y de sus propiedades asociadas.

Requisitos de seguridad del componente generales

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
CR 1.1	BR	Los componentes deben proporcionar la capacidad de identificar y autenticar a todos los usuarios en todas las interfaces que permita el reparto de tareas y los privilegios mínimos. Se puede proporcionar a nivel componente o a nivel sistema.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios humanos.
CR 1.2	BR	Los componentes deben proporcionar la capacidad de identificarse a sí mismos y autenticar a cualquier otro componente de acuerdo con el requisito del sistema SR 1.2 de la Norma IEC62443-3-3.Si el componente, como en el caso de una aplicación, se ejecuta en el contexto de un usuario humano, además, la identificación y autenticación del usuario humano de acuerdo con el requisito del sistema SR1.1 de la Norma IEC62443-3-3 puede formar parte del proceso de identificación y autenticación del componente hacia los demás componentes.
CR 1.3	BR	Los componentes deben proporcionar la capacidad de permitir la gestión de todas las cuentas de forma directa o integrándose en un sistema que gestione las cuentas.
CR 1.4	BR	Los componentes deben proporcionar la capacidad de integrarse en un sistema que soporte la gestión de identificadores y/o la capacidad de permitir la gestión de identificadores.
CR 1.5	BR	Los componentes deben proporcionar la capacidad de: a) permitir el uso del contenido inicial del autenticador; b) permitir el reconocimiento de los cambios en los autenticadores predeterminados realizados en el momento de la instalación; c) funcionar correctamente con operaciones periódicas de modificación/actualización de los autenticadores; y d) proteger a los autenticadores de la divulgación y modificación no autorizada cuando se almacenan, utilizan y transmiten.
CR 1.7	BR	Los componentes que utilicen autenticación basada en contraseña, deben proporcionar o integrarse en un sistema que proporcione la capacidad de aplicar la fortaleza de las contraseñas configurables de acuerdo con directrices de contraseñas reconocidas y probadas internacionalmente.
CR 1.8	BR	Cuando se utilice una infraestructura de clave pública (PKI), el componente debe proporcionar o integrarse en un sistema que ofrezca la capacidad de interactuar y funcionar de conformidad con el requisito del sistema SR 1.8 de la Norma IEC62443-3-3.
CR 1.9	BR	Los componentes que utilicen autenticación basada en clave pública deben suministrarse directamente o integrarse en un sistema que ofrezca la capacidad en el mismo entorno del sistema de control para: a)validar los certificados comprobando la validez de la firma de un certificado determinado; b)validar la cadena de certificados o, en el caso de los certificados autofirmados, desplegar certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; c)validar los certificados comprobando el estado de revocación de un certificado determinado; d)establecer el control del usuario sobre la clave privada correspondiente; e)asignar la

		identidad autenticada a un usuario y f)garantizar que los algoritmos y claves utilizados para la autenticación de clave pública cumplen con los requisitos establecidos.
CR 1.10	BR	Cuando un componente ofrezca la capacidad de autenticación, el componente debe ofrecer la capacidad de ocultar la retroalimentación de la información del autenticador durante el proceso de autenticación.
CR 1.11	BR	Cuando un componente ofrezca una capacidad de autenticación, el componente debe proporcionar la capacidad de: a) aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por parte de cualquier usuario durante un período de tiempo configurable; b) denegar el acceso durante un período de tiempo específico o hasta que un administrador lo desbloquee cuando se haya alcanzado este límite. Un administrador puede desbloquear una cuenta antes de la caducidad del período de tiempo de espera.
CR 1.12	BR	Cuando un componente proporcione un acceso de usuario humano local/IHM, debe proporcionar la capacidad de mostrar un mensaje de notificación de uso del sistema antes de la autenticación. Personal autorizado debe poder configurar el mensaje de notificación de uso del sistema.
CR 1.14	BR	Para los componentes que utilicen claves simétricas, el componente debe proporcionar la capacidad de: a) establecer la confianza mutua utilizando la clave simétrica; b) almacenar de forma segura el secreto compartido; c) restringir el acceso al secreto compartido; y d) garantizar que los algoritmos y claves utilizados para la autenticación de clave simétrica cumplen con los requisitos establecidos.
FR2. Control de uso		
CR 2.1	BR	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios identificados y autenticados en función de las responsabilidades que se les hayan asignado.
	RE1	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios en función de las responsabilidades que se les asignen y del privilegio mínimo.
	RE2	Los componentes, directamente o a través de un mecanismo de compensación de seguridad, deben proporcionar un rol autorizado para definir y modificar la asignación de permisos a roles para todos los usuarios humanos. Los roles no deberían limitarse a jerarquías fijas anidadas en las que un rol de nivel superior sea un superconjunto de un rol menos privilegiado. Por ejemplo, un administrador de sistema no debería incluir necesariamente privilegios de operador.
CR 2.2	BR	Si un componente soporta el uso a través de interfaces inalámbricas, debe proporcionar la capacidad de integrarse en el sistema que soporta la autorización de uso, la supervisión y las restricciones de acuerdo con las prácticas industriales comúnmente aceptadas.
CR 2.5	BR	Si un componente proporciona una interfaz para un usuario humano, tanto si se accede localmente como a través de una red, el componente debe proporcionar la capacidad de: a)protegerse contra el acceso posterior iniciando un bloqueo de sesión después de un período de tiempo configurable de inactividad o mediante la iniciación manual por parte del usuario y b)mantener el bloqueo de la sesión hasta que el usuario propietario de la sesión, u otro usuario humano autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados.

CR 2.6	BR	Si un componente soporta sesiones remotas, el componente debe proporcionar la capacidad de terminar una sesión remota automáticamente después de un período de inactividad configurable, manualmente por parte de una autoridad local, o manualmente por parte del usuario que inició la sesión.
CR 2.8	BR	Los componentes deben proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: a) control de acceso; b) errores de solicitud; c) eventos del sistema de control; d) evento de copia de seguridad y restauración; e) cambios de configuración; y f) eventos de registro de auditoría. Los registros de auditoría individuales deben incluir: a) marca de tiempo; b) fuente (dispositivo de origen, proceso de software o cuenta de usuario humano); c) categoría; d) tipo; e) ID del evento; y f) resultado del evento.
CR 2.9	BR	Los componentes deben: a) proporcionar la capacidad de asignar una capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros; y b) proporcionar mecanismos para proteger contra un fallo del componente cuando alcance o supere la capacidad de almacenamiento de datos de auditoría.
CR 2.10	BR	Los componentes deben: a) proporcionar la capacidad de proteger contra la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de una auditoría; y b) proporcionar la capacidad para permitir las acciones apropiadas en respuesta a un fallo en el procesamiento de una auditoría de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
CR 2.11	BR	Los componentes deben proporcionar la capacidad de crear marcas de tiempo (incluyendo fecha y hora) para su uso en los registros de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de crear marcas de tiempo que estén sincronizadas con una fuente de tiempo de todo el sistema.
CR 2.12	BR	Si un componente proporciona una interfaz para un usuario humano, el componente debe proporcionar la capacidad de determinar si un determinado usuario humano ha realizado una determinada acción. Los elementos de control que no puedan permitir tal capacidad se deben enumerar en los documentos de los componentes.
FR3. Integridad del sistema		
CR 3.1	BR	Los componentes deben proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el componente para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardware adecuados para el contexto en el que se encuentran.
	RE1	Los componentes deben proporcionar la capacidad de verificar la autenticidad de la información recibida durante la comunicación.
CR 3.3	BR	Los componentes deben proporcionar la capacidad de permitir la verificación de la operación prevista de las funciones de seguridad de acuerdo con el requisito del sistema.

CR 3.4	BR	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de integridad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de integridad.
	RE1	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de autenticidad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de autenticidad.
CR 3.5	BR	Los componentes deben validar la sintaxis, la longitud y el contenido de cualquier dato de entrada que se utilice como entrada de control de procesos industriales o entrada a través de interfaces externas que tengan un impacto directo en la acción del componente.
CR 3.6	BR	Los componentes que se conectan física o lógicamente a un proceso de automatización deben proporcionar la capacidad de establecer salidas a un estado predeterminado si no se puede mantener el funcionamiento normal definido por el proveedor de componentes.
CR 3.7	BR	Los componentes deben identificar y tratar las condiciones de error de manera que no proporcionen información que pueda ser aprovechada por adversarios para atacar el sistema de control.
CR 3.8	BR	Los componentes deben proporcionar mecanismos para proteger la integridad de las sesiones de comunicación, incluyendo: a) la capacidad de invalidar identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación); b) la capacidad de generar un identificador de sesión único para cada sesión y reconocer solo los identificadores de sesión generados por el sistema; y c) la capacidad de generar identificadores de sesión únicos con fuentes de aleatoriedad comúnmente aceptadas.
CR 3.9	BR	Los componentes deben proteger la información de auditoría, los registros de auditoría y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
CR 4.1	BR	Los componentes deben: a) proporcionar la capacidad de proteger la confidencialidad de la información en reposo para la que se admite la autorización explícita de lectura; y b) permitir la protección de la confidencialidad de la información en tránsito, como se define en el requisito del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Los componentes deben proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura, de los componentes que vayan a ser liberados del servicio activo y/o poner fuera de servicio.
CR 4.3	BR	Si se requiere el uso de criptografía, el componente debe utilizar mecanismos de seguridad criptográfica de acuerdo con prácticas y recomendaciones de seguridad internacionalmente reconocidas y probadas.

FR5. Flujo de datos restringidos		
CR 5.1	BR	Los componentes deben permitir una red segmentada que admitan zonas y conductos, según sea necesario, para permitir una arquitectura de red más amplia basada en la segmentación lógica y la criticidad.
FR6. Respuesta oportuna a los incidentes		
CR 6.1	BR	Los componentes deben proporcionar la capacidad para que las personas y/o las herramientas autorizadas puedan acceder a los registros de auditoría de solo lectura.
CR 6.2	BR	Los componentes deben proporcionar la capacidad de ser continuamente supervisados utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
CR 7.1	BR	Los componentes deben proporcionar la capacidad de mantener las funciones esenciales cuando operen en modo degradado como resultado de un evento de denegación de servicio.
	RE1	Los componentes deben proporcionar la capacidad de mitigar los efectos de los tipos de eventos de denegación de servicio de desbordamiento de información y/o mensajes.
CR 7.2	BR	Los componentes deben proporcionar la capacidad de limitar el uso de recursos en las funciones de seguridad para proteger contra el agotamiento de los recursos.
CR 7.3	BR	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
	RE1	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
CR 7.4	BR	Los componentes deben proporcionar la capacidad de poder ser recuperados y reconstituidos hasta un estado de seguridad conocido después de una interrupción o fallo.
CR 7.6	BR	Los componentes deben proporcionar la capacidad de poder ser configurados de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El componente debe proporcionar una interfaz con los ajustes de configuración de red y seguridad actualmente desplegados.
CR 7.7	BR	Los componentes deben proporcionar la capacidad de restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.

CR 7.8	BR	Los componentes deben proporcionar la capacidad de permitir un inventario de componentes del sistema de control de acuerdo con el requisito del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisitos de seguridad del componente a nivel de software

ID req	BR/RE	Explicación
SAR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	La aplicación debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
SAR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.

Requisitos de seguridad para los dispositivos integrados (PLCs, IED)

ID req	BR/RE	Explicación
EDR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	El dispositivo integrado debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
EDR 2.13	BR	Los dispositivos integrados deben proteger contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, depuración JTAG).
EDR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.
EDR 3.10	BR	El dispositivo integrado debe admitir la capacidad de ser actualizado y someterse a una subida de nivel.

	RE1	El dispositivo integrado debe validar la autenticidad e integridad de cualquier actualización o subida de nivel del software antes de la instalación.
EDR 3.11	BR	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
EDR 3.12	BR	Los dispositivos integrados deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
EDR 3.13	BR	Los dispositivos integrados deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
EDR 3.14	BR	Los dispositivos integrados deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el arranque del componente y los procesos en tiempo de ejecución antes de su uso.
	RE1	Los dispositivos integrados deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos Host

ID req	BR/RE	Explicación
HDR 2.4	BR	En caso de que un dispositivo host utilice tecnologías de código móvil, dicho dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo host: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a cargar código móvil en el dispositivo host; y c) controlar la ejecución del código basándose en comprobaciones de integridad en el código móvil y antes de que el código se ejecute.
	RE1	El dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
HDR 2.13	BR	Los dispositivos host deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
HDR 3.2	BR	Los dispositivos host deben contar con mecanismos homologados por el proveedor de productos del sistema de control que garanticen la protección contra códigos maliciosos. El proveedor del producto del sistema de control debe documentar cualquier requisito especial de configuración relacionado con la protección contra el código malicioso.

	RE1	El dispositivo host debe informar automáticamente de las versiones del software y de los archivos de protección contra el código malicioso en uso (como parte de la función de registro general).
HDR 3.10	BR	Los dispositivos host deben contar con la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos host deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
HDR 3.11	BR	Los dispositivos host deben ofrecer la capacidad de admitir mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
HDR 3.12	BR	Los dispositivos host deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
HDR 3.13	BR	Los dispositivos host deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
HDR 3.14	BR	Los dispositivos host deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos host deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos de red

ID req	BR/RE	Explicación
NDR 1.6	BR	Un dispositivo de red que permita la gestión de acceso inalámbrico debe proporcionar la capacidad de identificar y autenticar todos los usuarios (personas, procesos de software o dispositivos) que participan en la comunicación inalámbrica.
	RE1	El dispositivo de red debe proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios (personas, procesos o dispositivos de software) que participen en la comunicación inalámbrica.
NDR 1.13	BR	El dispositivo de red que permita el acceso de dispositivos a una red debe poder supervisar y controlar todos los métodos de acceso al dispositivo de red a través de redes que no son de confianza.
NDR 2.4	BR	En caso de que un dispositivo de red utilice tecnologías de código móvil, el dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo de red: a) controlar la ejecución del código

		móvil; b) controlar qué usuarios están autorizados a transferir código móvil hacia/desde el dispositivo de red; y c) controlar la ejecución del código basándose en verificaciones de integridad antes de que el código se ejecute
	RE1	El dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
NDR 2.13	BR	Los dispositivos de red deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
NDR 3.2	BR	El dispositivo de red debe proporcionar protección contra códigos maliciosos.
NDR 3.10	BR	Los dispositivos de red deben admitir la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos de red deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
NDR 3.11	BR	Los dispositivos de red deben ofrecer mecanismos de detección y resistencia a la manipulación para proteger contra el acceso físico no autorizado al dispositivo.
NDR 3.12	BR	Los dispositivos de red deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
NDR 3.13	BR	Los dispositivos de red deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
NDR 3.14	BR	Los dispositivos de red deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos de red deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.
NDR 5.2	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas de riesgo y conductos.
	RE1	El componente de red debe proporcionar la capacidad de denegar tráfico de red por defecto y permitir tráfico de red por excepción (también denominado "denegar todo, permiso por excepción").
NDR 5.3	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de proteger contra la recepción de mensajes de propósito general entre personas recibidos de usuarios o sistemas externos al sistema de control.

ANEXO III: REQUISITOS PARA NIVEL SL3

Requisitos de seguridad del sistema

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
SR 1.1	BR	Todos los usuarios que accedan al sistema han de ser identificados y autenticados tanto a nivel de sistemas como de aplicación puede ser a través de contraseñas, dispositivos de acceso o multifactor (combinación de las anteriores).
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios humanos.
	RE2	El sistema de control debe proporcionar la capacidad de emplear la autenticación multifactor para permitir el acceso de usuarios humanos al sistema de control a través de una red que no es de confianza.
SR 1.2	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar todos los procesos de software y dispositivos. Esta capacidad debe hacer cumplir dicha identificación y autenticación en todas las interfaces que proporcionen acceso al sistema de control para permitir los privilegios mínimos, de conformidad con las políticas y procedimientos de seguridad aplicables.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única todos los procesos de software y dispositivos.
SR 1.3	BR	El sistema de control debe tener la capacidad de gestionar cuentas de usuarios (agregar, eliminar, modificar o desactivar) estableciendo condiciones para pertenecer a un grupo y la asignación de autorizaciones. Sólo se admitirán cuentas compartidas, cuando por condiciones del sistema se establezca en el análisis de riesgo, aunque deberán de establecerse contramedidas y documentarlas.
	RE1	El sistema de control debe proporcionar la capacidad de admitir la gestión de cuentas unificada.
SR 1.4	BR	El sistema de control debe proporcionar la capacidad de admitir la gestión de los identificadores (permite operar dentro de un dominio o zona de control específico del sistema) por usuario, grupo, rol o interfaz del sistema de control.
SR 1.5	BR	El sistema de control debe proporcionar la capacidad de: 1) iniciar el contenido del autenticador; 2) cambiar todos los autenticadores predeterminados; 3) cambiar/actualizar los autenticadores; 4) protegerlos contra la divulgación y modificación no autorizada. Ejemplos de autenticadores son claves físicas, tarjetas de acceso, claves privadas, entre otras.

	RE1	Para los usuarios de procesos de software y dispositivos, el sistema de control debe proporcionar la capacidad de proteger los autenticadores pertinentes a través de mecanismos de hardware.
SR 1.6	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar a todos los usuarios que participen en una comunicación inalámbrica. Ejemplos de tecnologías inalámbricas son Bluetooth, infrarrojos, enrutadores móviles, etc.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios (personas, procesos de software o dispositivos) que participen en la comunicación inalámbrica.
SR 1.7	BR	En los sistemas de control que utilicen la contraseña como medio de autenticación debe aplicar una fortaleza configurable en base a la longitud mínima y la variedad de caracteres. Se aplicará vigencia máxima para las contraseñas y se notificará cuando esta expire. Esta protección se puede mejorar limitando la reutilización de las contraseñas.
	RE1	El sistema de control debe proporcionar la capacidad de evitar que una cuenta de un usuario humano determinada reutilice una contraseña para un número configurable de generaciones. Además, el sistema de control debe proporcionar la capacidad de aplicar restricciones de vigencia mínimas y máximas de las contraseñas a los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad.
SR 1.8	BR	En los casos en los que se utilice una PKI, el sistema de control debe proporcionar la capacidad de que una PKI funcione con arreglo a las mejores prácticas comúnmente aceptadas u obtener certificados de clave pública de una PKI existente. El registro de esta debe incluir la autorización de un supervisor que verifique la identidad del titular del certificado y que garantice que se emite al usuario previsto.
SR 1.9	BR	En el caso de los sistemas de control que utilicen autenticación de clave pública (PKI), el sistema de control debe proporcionar la capacidad de: l)validar los certificados comprobando la validez de la firma de un certificado determinado; m)validar los certificados a través de una ruta de certificación a una CA aceptada o, en el caso de los certificados autofirmados, desplegando certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; n)validar los certificados comprobando el estado de revocación de un certificado determinado; o)establecer el control del usuario sobre la clave privada correspondiente; y p)asignar la identidad autenticada a un usuario.
	RE1	El sistema de control debe proporcionar la capacidad de proteger las claves privadas pertinentes a través de mecanismos de hardware con arreglo a las prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad.
SR 1.10	BR	El sistema de control debe proporcionar la capacidad de ocultar la retroalimentación de la información de autenticación durante el proceso. No debe dar pistas sobre los fallos de autenticación como, por ejemplo, “nombre de usuario desconocido”
SR 1.11	BR	El sistema de control debe proporcionar la capacidad de aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por cualquier usuario dentro de un periodo configurable de tiempo.
SR 1.12	BR	El sistema de control debe proporcionar la capacidad de mostrar un mensaje de aviso del sistema antes de la autenticación. El personal autorizado debe poder configurar el mensaje de aviso de uso del sistema.

SR 1.13	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza. Debe permitir el acceso sólo cuando se esté autorizado y restringir el acceso desde conexiones telefónicas o no autorizadas. Es posible que los procedimientos requieran la autenticación multifactor para permitir el acceso remoto.
	RE1	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza.
FR2. Control de uso		
SR 2.1	BR	El sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control a fin de admitir el reparto de tareas y el privilegio mínimo. Verificar que las acciones del usuario están permitidas según el rol asignado y permitir que solo las personas cualificadas y autorizadas realicen cambios en los componentes del sistema.
	RE1	En todas las interfaces, el sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios (personas, procesos de software y dispositivos) para controlar el uso del sistema de control con el fin de admitir el reparto de tareas y el privilegio mínimo.
	RE2	El sistema de control debe proporcionar la capacidad de que un usuario o rol autorizado defina y modifique la asignación de permisos a roles para todos los usuarios humanos.
	RE3	El sistema de control debe admitir el permiso manual del supervisor de las autorizaciones actuales de los usuarios humanos para un tiempo o secuencia de eventos configurables.
SR 2.2	BR	El sistema de control debe proporcionar la capacidad de autorizar, supervisar y aplicar las restricciones de uso para las conexiones inalámbricas al sistema de control con arreglo a las prácticas comúnmente aceptadas en el sector de la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de identificar e informar de la presencia de dispositivos inalámbricos no autorizados que transmitan dentro del entorno físico del sistema de control.
SR 2.3	BR	El sistema de control debe proporcionar la capacidad de aplicar automáticamente las restricciones de uso configurables, que incluyen: a) prevenir el uso de dispositivos portátiles y móviles; b) requerir autorización basada en un contexto específico; y c) restringir la transferencia de códigos y datos a/de dispositivos portátiles y móviles.
	RE1	El sistema de control debe proporcionar la capacidad de verificar que los dispositivos portátiles y móviles que están intentando conectarse a la zona cumplan con los requisitos de seguridad de la misma.
SR 2.4	BR	El sistema de control debe proporcionar la capacidad de aplicar restricciones de uso para las tecnologías de código móvil basadas en la posibilidad de que causen daños al sistema de control, incluyendo: a) prevenir la ejecución del código móvil; b) requerir procesos de autenticación y autorización adecuados para el origen del código; c) restringir la transferencia del código móvil a/del sistema de control; y d) supervisar el uso del código móvil.

	RE1	El sistema de control debe proporcionar la capacidad de verificar la integridad del código móvil antes de autorizar que se ejecute el código.
SR 2.5	BR	El sistema de control debe proporcionar la capacidad de evitar un acceso posterior iniciando un bloqueo de la sesión tras un período de tiempo configurable de inactividad o mediante iniciación manual. La sesión debe continuar bloqueada hasta que el usuario autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados. En los casos en los que el sistema de control no pueda admitir el bloqueo de la sesión, la entidad responsable debería emplear las contramedidas compensatorias que se consideren adecuadas como mayores medidas de seguridad física y auditorias.
SR 2.6	BR	El sistema de control debe proporcionar la capacidad de terminar una sesión remota, ya sea automáticamente después de un período de inactividad configurable o manualmente por parte del usuario que inició la sesión.
SR 2.7	BR	El sistema de control debe proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado a un número configurable de sesiones.
SR 2.8	BR	El sistema de control debe proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de copias de seguridad y restauración, cambios en la configuración, actividad potencial de reconocimiento y eventos del registro de auditoría. Los registros individuales de auditoría deben incluir la marca de tiempo, fuente (dispositivo, proceso de software o cuenta de usuario humano de origen), categoría, tipo, identificador del evento y resultado del evento.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar de manera centralizada los eventos de auditoría y de elaborar registros de auditoría de múltiples componentes a través del sistema de control en una pista de auditoría para todo el sistema (lógica o física) con correlación de tiempo. El sistema de control debe proporcionar la capacidad de exportar dichos registros de auditorías en formatos habituales para la industria para que se analicen con las herramientas comerciales habituales de análisis de registros, como por ejemplo la administración de eventos e información de seguridad (SIEM).
SR 2.9	BR	El sistema de control debe asignar una capacidad suficiente de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros y la configuración del sistema. el sistema de control debe proporcionar mecanismos de auditoría para reducir la posibilidad de que se exceda dicha capacidad.
	RE1	El sistema de control debe proporcionar la capacidad de emitir un aviso cuando el volumen de almacenamiento de registros de auditoría asignado alcance un porcentaje configurable de capacidad máxima de almacenamiento de registros de auditoría.
SR 2.10	BR	El sistema de control debe proporcionar la capacidad de alertar al personal y evitar la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de auditorías. El sistema de control debe proporcionar la capacidad de admitir las acciones apropiadas en respuesta a un fallo en el procesamiento de auditorías de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.

SR 2.11	BR	El sistema de control debe proporcionar marcas de tiempo (fecha y hora) para la generación de registros de auditoría. Evitar que las fuentes horarias sufran alteraciones no autorizadas.
	RE1	El sistema de control debe proporcionar la capacidad de sincronizar los relojes internos del sistema a una frecuencia configurable.
SR 2.12	BR	El sistema de control debe proporcionar la capacidad de determinar si un usuario humano ha realizado una acción concreta.
FR3. Integridad del sistema		
SR 3.1	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el sistema para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos criptográficos para reconocer cambios de información durante la comunicación.
SR 3.2	BR	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección para prevenir, detectar, mitigar e informar de los efectos de un código malicioso o de software no autorizado. El sistema de control debe proporcionar la capacidad de actualizar los mecanismos de protección.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección contra códigos maliciosos en todos los puntos de entrada y salida.
	RE2	El sistema de control debe proporcionar la capacidad de gestionar los mecanismos de protección contra códigos maliciosos.
SR 3.3	BR	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad (medidas de antivirus, identificación, detección de intrusos y auditorias) e informar de las anomalías que se produzcan durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado. Las funciones de seguridad deben incluir todas las funciones que sean necesarias para cumplir con los requisitos de seguridad especificados n esta norma.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos automáticos para facilitar la gestión de la verificación de la seguridad durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado.
SR 3.4	BR	El sistema de control debe proporcionar la capacidad de detectar, registrar, informar y proteger contra cambios no autorizados en el software y en la información en reposo.
	RE1	El sistema de control debe proporcionar la capacidad de emplear herramientas automatizadas que notifiquen a un conjunto configurable de receptores cuando se produzcan discrepancias durante la verificación de la integridad.

SR 3.5	BR	El sistema de control debe validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que tengan un impacto directo en la acción del sistema de control. Las directrices a tener en cuenta deberían incluir la Code Review Guide del Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control debe proporcionar la capacidad de establecer el valor de salida a un estado predeterminado si no se puede mantener el funcionamiento normal como resultado de un ataque.
SR 3.7	BR	El sistema de control debe identificar y tratar las condiciones de error de manera tal que se pueda aplicar un remedio efectivo. Esto se debe hacer sin proporcionar información que pueda ser aprovechada por adversarios para atacar el sistema de control, a no ser que sea necesario para resolver los problemas de manera oportuna.
SR 3.8	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de las sesiones. El sistema de control debe rechazar cualquier uso por parte de identificadores de sesión no válidos.
	RE1	El sistema de control debe proporcionar la capacidad de anular los identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación).
	RE2	El sistema de control debe proporcionar la capacidad de generar un identificador de sesión único para cada sesión y considerar no válidos todos los identificadores de sesión imprevistos.
SR 3.9	BR	El sistema de control debe proteger la información y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
SR 4.1	BR	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información (especialmente en dispositivos portátiles) para la que se admite la autorización explícita de lectura, ya esté en reposo o en tránsito. La técnica elegida tenga en cuenta las posibles ramificaciones en el rendimiento del sistema de control y la capacidad de recuperarse tras un fallo del sistema o un ataque.
	RE1	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información en reposo y en sesiones con acceso remoto a través de una red que no es de confianza.
SR 4.2	BR	El sistema de control debe proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura de los componentes que vayan a ser liberados del servicio activo y/o puestos fuera de servicio.
	RE1	El sistema de control debe proporcionar la capacidad de evitar la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles (no retienen la información después de ser liberados para la gestión de la memoria).
SR 4.3	BR	Si se requiere el uso de criptografía, el sistema de control debe usar algoritmos criptográficos, tamaños de clave y mecanismos para el establecimiento y gestión de claves con arreglo a las prácticas y recomendaciones de seguridad comúnmente aceptadas en el sector que se encuentran en documentos como la Publicación Especial NIST SP800-57

FR5. Flujo de datos restringidos		
SR 5.1	BR	El sistema de control debe proporcionar la capacidad de segmentar de manera lógica las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de otras redes del sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de segmentar físicamente las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de las redes no críticas del sistema de control.
	RE2	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
SR 5.2	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas y conductos de riesgo. Como parte de una estrategia de protección de defensa total, se deberían dividir los sistemas de control de mayor impacto en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red con arreglo a las políticas y procedimientos de seguridad y a una evaluación de riesgos.
	RE1	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
	RE2	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
	RE3	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo). Esta función de "cierre en caso de fallo" debe designarse de tal forma que no interfiera en el funcionamiento de un sistema instrumentado de seguridad (SIS) o en otras funciones relacionadas con la seguridad.
SR 5.3	BR	Un sistema de control debe proporcionar la capacidad de evitar la recepción de mensajes de propósito general (correo electrónico, redes sociales o cualquier otro sistema de mensajería) entre personas recibidos de usuarios o sistemas externos al sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de evitar tanto la transmisión como la recepción de mensajes entre personas de propósito general.
SR 5.4	BR	El sistema de control debe proporcionar la capacidad de admitir la partición de datos (por medios físicos o lógicos), aplicaciones y servicios en base a su criticidad para facilitar la implementación de un modelo de zonificación.
FR6. Respuesta oportuna a los incidentes		
SR 6.1	BR	El sistema de control debe proporcionar la capacidad de que las personas y/o las herramientas autorizadas accedan a los registros de auditoría en modo de lectura.

	RE1	El sistema de control debe permitir el acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API).
SR 6.2	BR	El sistema de control debe proporcionar la capacidad de supervisar continuamente el rendimiento del mecanismo de seguridad utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
SR 7.1	BR	El sistema de control debe proporcionar la capacidad de funcionar en modo degradado durante un evento de denegación de servicio. Un evento de denegación de servicio en el sistema de control no debería afectar negativamente a ningún sistema relacionado con la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar las cargas de comunicación (por ejemplo, limitando la tasa) para mitigar los efectos de los tipos de desbordamiento de información de los eventos de denegación de servicio.
	RE2	El sistema de control debe proporcionar la capacidad de restringir la posibilidad de que cualquier usuario provoque eventos de denegación de servicio que puedan afectar a otros sistemas de control o redes.
SR 7.2	BR	El sistema de control debe proporcionar la capacidad de limitar el uso de recursos por parte de las funciones de seguridad para evitar el agotamiento de los recursos.
SR 7.3	BR	El sistema de control debe facilitar la identidad y ubicación de los archivos críticos y la capacidad de llevar a cabo copias de seguridad de la información a nivel del usuario y del sistema (incluyendo información sobre el estado del sistema) sin que esto afecte a las operaciones habituales.
	RE1	El sistema de control debe proporcionar la capacidad de verificar la fiabilidad de los mecanismos de copias de seguridad.
	RE2	El sistema de control debe proporcionar la capacidad de automatizar la función de copia de seguridad en base a una frecuencia configurable.
SR 7.4	BR	El sistema de control debe proporcionar la capacidad de recuperarse y reconstituirse hasta un estado seguro conocido después de una interrupción o fallo. Un estado seguro conocido significa que se atribuyen a todos los parámetros del sistema (ya sean predeterminados o configurables) valores seguros, se reinstalan los parches críticos para la seguridad, se restablecen los ajustes de configuración relacionados con la seguridad, se dispone de la documentación y los procedimientos operativos del sistema, se reinstala y configura la aplicación y el software del sistema con ajustes seguros, se carga la información de las copias de seguridad más recientes y conocidas y se somete a ensayo y se comprueba el funcionamiento del sistema en su totalidad.
SR 7.5	BR	El sistema de control debe proporcionar la capacidad de cambiar de y a una fuente de alimentación de emergencia sin que esto afecte el estado de seguridad existente o un modo degradado documentado.

SR 7.6	BR	El sistema de control debe proporcionar la capacidad de ser configurado de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El sistema de control debe proporcionar una interfaz a los ajustes de configuración de red y seguridad desplegados actualmente.
	RE1	El sistema de control debe proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad desplegados actualmente en un formato legible por una máquina.
SR 7.7	BR	El sistema de control debe proporcionar la capacidad de prohibir y/o restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
SR 7.8	BR	El sistema de control debe proporcionar la capacidad de informar de la lista actual de componentes instalados y de sus propiedades asociadas.

Requisitos de seguridad del componente generales

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
CR 1.1	BR	Los componentes deben proporcionar la capacidad de identificar y autenticar a todos los usuarios en todas las interfaces que permita el reparto de tareas y los privilegios mínimos. Se puede proporcionar a nivel componente o a nivel sistema.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios humanos.
	RE2	Los componentes deben proporcionar la capacidad de emplear la autenticación multifactor para todo el acceso de usuarios humanos al componente.
CR 1.2	BR	Los componentes deben proporcionar la capacidad de identificarse a sí mismos y autenticar a cualquier otro componente de acuerdo con el requisito del sistema SR 1.2 de la NormaIEC62443-3-3.Si el componente, como en el caso de una aplicación, se ejecuta en el contexto de un usuario humano, además, la identificación y autenticación del usuario humano de acuerdo con el requisito del sistema SR1.1 de la Norma IEC62443-3-3 puede formar parte del proceso de identificación y autenticación del componente hacia los demás componentes.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a cualquier otro componente.
CR 1.3	BR	Los componentes deben proporcionar la capacidad de permitir la gestión de todas las cuentas de forma directa o integrándose en un sistema que gestione las cuentas.
CR 1.4	BR	Los componentes deben proporcionar la capacidad de integrarse en un sistema que soporte la gestión de identificadores y/o la capacidad de permitir la gestión de identificadores.

CR 1.5	BR	Los componentes deben proporcionar la capacidad de: a) permitir el uso del contenido inicial del autenticador; b) permitir el reconocimiento de los cambios en los autenticadores predeterminados realizados en el momento de la instalación; c) funcionar correctamente con operaciones periódicas de modificación/actualización de los autenticadores; y d) proteger a los autenticadores de la divulgación y modificación no autorizada cuando se almacenan, utilizan y transmiten.
	RE1	Los autenticadores en los que se apoya el componente deben estar protegidos mediante mecanismos de hardware (Memoria protegida por contraseña, memoria OTP, comprobaciones de integridad hardware de datos y mecanismo de arranque de seguridad de dispositivos.).
CR 1.7	BR	Los componentes que utilicen autenticación basada en contraseña, deben proporcionar o integrarse en un sistema que proporcione la capacidad de aplicar la fortaleza de las contraseñas configurables de acuerdo con directrices de contraseñas reconocidas y probadas internacionalmente.
	RE1	Los componentes deben proporcionar, o integrarse en un sistema que proporcione la capacidad de proteger una cuenta de usuario humano determinada contra la reutilización de una contraseña para un número configurable de generaciones. Además, el componente debe proporcionar la capacidad de aplicar las restricciones de vigencia mínimas y máximas de la contraseña para los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad. El componente debería proporcionar la capacidad de solicitar al usuario que cambie su contraseña en un tiempo configurable antes de su caducidad.
CR 1.8	BR	Cuando se utilice una infraestructura de clave pública (PKI), el componente debe proporcionar o integrarse en un sistema que ofrezca la capacidad de interactuar y funcionar de conformidad con el requisito del sistema SR 1.8 de la Norma IEC62443-3-3.
CR 1.9	BR	Los componentes que utilicen autenticación basada en clave pública deben suministrarse directamente o integrarse en un sistema que ofrezca la capacidad en el mismo entorno del sistema de control para: a)validar los certificados comprobando la validez de la firma de un certificado determinado; b)validar la cadena de certificados o, en el caso de los certificados autofirmados, desplegar certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; c)validar los certificados comprobando el estado de revocación de un certificado determinado; d)establecer el control del usuario sobre la clave privada correspondiente; e)asignar la identidad autenticada a un usuario y f)garantizar que los algoritmos y claves utilizados para la autenticación de clave pública cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger las claves privadas críticas de larga duración mediante mecanismos de hardware.
CR 1.10	BR	Cuando un componente ofrezca la capacidad de autenticación, el componente debe ofrecer la capacidad de ocultar la retroalimentación de la información del autenticador durante el proceso de autenticación.
CR 1.11	BR	Cuando un componente ofrezca una capacidad de autenticación, el componente debe proporcionar la capacidad de: a) aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por parte de cualquier usuario durante un período de tiempo configurable; b) denegar el acceso durante un período de tiempo específico o hasta que un administrador lo desbloquee

		cuando se haya alcanzado este límite. Un administrador puede desbloquear una cuenta antes de la caducidad del período de tiempo de espera.
CR 1.12	BR	Cuando un componente proporcione un acceso de usuario humano local/IHM, debe proporcionar la capacidad de mostrar un mensaje de notificación de uso del sistema antes de la autenticación. Personal autorizado debe poder configurar el mensaje de notificación de uso del sistema.
CR 1.14	BR	Para los componentes que utilicen claves simétricas, el componente debe proporcionar la capacidad de: a) establecer la confianza mutua utilizando la clave simétrica; b) almacenar de forma segura el secreto compartido; c) restringir el acceso al secreto compartido; y d) garantizar que los algoritmos y claves utilizados para la autenticación de clave simétrica cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger claves simétricas críticas y de larga duración mediante mecanismos de hardware.
FR2. Control de uso		
CR 2.1	BR	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios identificados y autenticados en función de las responsabilidades que se les hayan asignado.
	RE1	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios en función de las responsabilidades que se les asignen y del privilegio mínimo.
	RE2	Los componentes, directamente o a través de un mecanismo de compensación de seguridad, deben proporcionar un rol autorizado para definir y modificar la asignación de permisos a roles para todos los usuarios humanos. Los roles no deberían limitarse a jerarquías fijas anidadas en las que un rol de nivel superior sea un superconjunto de un rol menos privilegiado. Por ejemplo, un administrador de sistema no debería incluir necesariamente privilegios de operador.
	RE3	Los componentes deben proporcionar el permiso manual del supervisor durante un tiempo o secuencia de eventos configurables. La implementación de un permiso manual, controlado y auditado de mecanismos automatizados en caso de emergencia u otros eventos graves permite a un supervisor autorizar a un operador para que reaccione rápidamente ante condiciones inusuales sin cerrar la sesión actual y establecer una nueva sesión como un usuario humano con mayores privilegios.
CR 2.2	BR	Si un componente soporta el uso a través de interfaces inalámbricas, debe proporcionar la capacidad de integrarse en el sistema que soporta la autorización de uso, la supervisión y las restricciones de acuerdo con las prácticas industriales comúnmente aceptadas.
CR 2.5	BR	Si un componente proporciona una interfaz para un usuario humano, tanto si se accede localmente como a través de una red, el componente debe proporcionar la capacidad de: a)protegerse contra el acceso posterior iniciando un bloqueo de sesión después de un período de tiempo configurable de inactividad o mediante la iniciación manual por parte del usuario y b)mantener el bloqueo de la sesión hasta que el usuario propietario de la sesión, u otro usuario humano autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados.

CR 2.6	BR	Si un componente soporta sesiones remotas, el componente debe proporcionar la capacidad de terminar una sesión remota automáticamente después de un período de inactividad configurable, manualmente por parte de una autoridad local, o manualmente por parte del usuario que inició la sesión.
CR 2.7	BR	Los componentes deben proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado (persona, proceso de software o dispositivo).
CR 2.8	BR	Los componentes deben proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: a) control de acceso; b) errores de solicitud; c) eventos del sistema de control; d) evento de copia de seguridad y restauración; e) cambios de configuración; y f) eventos de registro de auditoría. Los registros de auditoría individuales deben incluir: a) marca de tiempo; b) fuente (dispositivo de origen, proceso de software o cuenta de usuario humano); c) categoría; d) tipo; e) ID del evento; y f) resultado del evento.
CR 2.9	BR	Los componentes deben: a) proporcionar la capacidad de asignar una capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros; y b) proporcionar mecanismos para proteger contra un fallo del componente cuando alcance o supere la capacidad de almacenamiento de datos de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de emitir un aviso cuando el almacenamiento de registros de auditoría asignado alcance un umbral de capacidad configurable.
CR 2.10	BR	Los componentes deben: a) proporcionar la capacidad de proteger contra la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de una auditoría; y b) proporcionar la capacidad para permitir las acciones apropiadas en respuesta a un fallo en el procesamiento de una auditoría de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
CR 2.11	BR	Los componentes deben proporcionar la capacidad de crear marcas de tiempo (incluyendo fecha y hora) para su uso en los registros de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de crear marcas de tiempo que estén sincronizadas con una fuente de tiempo de todo el sistema.
CR 2.12	BR	Si un componente proporciona una interfaz para un usuario humano, el componente debe proporcionar la capacidad de determinar si un determinado usuario humano ha realizado una determinada acción. Los elementos de control que no puedan permitir tal capacidad se deben enumerar en los documentos de los componentes.
FR3. Integridad del sistema		
CR 3.1	BR	Los componentes deben proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el componente para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	Los componentes deben proporcionar la capacidad de verificar la autenticidad de la información recibida durante la comunicación.

CR 3.3	BR	Los componentes deben proporcionar la capacidad de permitir la verificación de la operación prevista de las funciones de seguridad de acuerdo con el requisito del sistema.
CR 3.4	BR	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de integridad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de integridad.
	RE1	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de autenticidad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de autenticidad.
	RE2	Si el componente está realizando la verificación de la integridad, debe poder notificar automáticamente a una entidad configurable cuando descubra que se ha intentado realizar un cambio no autorizado.
CR 3.5	BR	Los componentes deben validar la sintaxis, la longitud y el contenido de cualquier dato de entrada que se utilice como entrada de control de procesos industriales o entrada a través de interfaces externas que tengan un impacto directo en la acción del componente.
CR 3.6	BR	Los componentes que se conectan física o lógicamente a un proceso de automatización deben proporcionar la capacidad de establecer salidas a un estado predeterminado si no se puede mantener el funcionamiento normal definido por el proveedor de componentes.
CR 3.7	BR	Los componentes deben identificar y tratar las condiciones de error de manera que no proporcionen información que pueda ser aprovechada por adversarios para atacar el sistema de control.
CR 3.8	BR	Los componentes deben proporcionar mecanismos para proteger la integridad de las sesiones de comunicación, incluyendo: a) la capacidad de invalidar identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación); b) la capacidad de generar un identificador de sesión único para cada sesión y reconocer solo los identificadores de sesión generados por el sistema; y c) la capacidad de generar identificadores de sesión únicos con fuentes de aleatoriedad comúnmente aceptadas.
CR 3.9	BR	Los componentes deben proteger la información de auditoría, los registros de auditoría y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
CR 4.1	BR	Los componentes deben: a) proporcionar la capacidad de proteger la confidencialidad de la información en reposo para la que se admite la autorización explícita de lectura; y b) permitir la protección de la confidencialidad de la información en tránsito, como se define en el requisito del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Los componentes deben proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura, de los componentes que vayan a ser liberados del servicio activo y/o poner fuera de servicio.

	RE1	Los componentes deben proporcionar la capacidad de proteger contra la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles.
	RE2	Los componentes deben proporcionar la capacidad de verificar que se ha producido el borrado de la información.
CR 4.3	BR	Si se requiere el uso de criptografía, el componente debe utilizar mecanismos de seguridad criptográfica de acuerdo con prácticas y recomendaciones de seguridad internacionalmente reconocidas y probadas.
FR5. Flujo de datos restringidos		
CR 5.1	BR	Los componentes deben permitir una red segmentada que admitan zonas y conductos, según sea necesario, para permitir una arquitectura de red más amplia basada en la segmentación lógica y la criticidad.
FR6. Respuesta oportuna a los incidentes		
CR 6.1	BR	Los componentes deben proporcionar la capacidad para que las personas y/o las herramientas autorizadas puedan acceder a los registros de auditoría de solo lectura.
	RE1	Los componentes deben proporcionar acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API) o enviando los registros de auditoría a un sistema centralizado.
CR 6.2	BR	Los componentes deben proporcionar la capacidad de ser continuamente supervisados utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
CR 7.1	BR	Los componentes deben proporcionar la capacidad de mantener las funciones esenciales cuando operen en modo degradado como resultado de un evento de denegación de servicio.
	RE1	Los componentes deben proporcionar la capacidad de mitigar los efectos de los tipos de eventos de denegación de servicio de desbordamiento de información y/o mensajes.
CR 7.2	BR	Los componentes deben proporcionar la capacidad de limitar el uso de recursos en las funciones de seguridad para proteger contra el agotamiento de los recursos.
CR 7.3	BR	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
	RE1	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.

CR 7.4	BR	Los componentes deben proporcionar la capacidad de poder ser recuperados y reconstituidos hasta un estado de seguridad conocido después de una interrupción o fallo.
CR 7.6	BR	Los componentes deben proporcionar la capacidad de poder ser configurados de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El componente debe proporcionar una interfaz con los ajustes de configuración de red y seguridad actualmente desplegados.
	RE1	Los componentes deben proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad actualmente desplegados en un formato legible por una máquina.
CR 7.7	BR	Los componentes deben proporcionar la capacidad de restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
CR 7.8	BR	Los componentes deben proporcionar la capacidad de permitir un inventario de componentes del sistema de control de acuerdo con el requisito del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisitos de seguridad del componente a nivel de software

ID req	BR/RE	Explicación
SAR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	La aplicación debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
SAR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.

Requisitos de seguridad para los dispositivos integrados (PLCs, IED)

ID req	BR/RE	Explicación
EDR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del

		código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	El dispositivo integrado debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
EDR 2.13	BR	Los dispositivos integrados deben proteger contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, depuración JTAG).
	RE1	Los dispositivos integrados deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
EDR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.
EDR 3.10	BR	El dispositivo integrado debe admitir la capacidad de ser actualizado y someterse a una subida de nivel.
	RE1	El dispositivo integrado debe validar la autenticidad e integridad de cualquier actualización o subida de nivel del software antes de la instalación.
EDR 3.11	BR	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
EDR 3.12	BR	Los dispositivos integrados deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
EDR 3.13	BR	Los dispositivos integrados deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
EDR 3.14	BR	Los dispositivos integrados deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el arranque del componente y los procesos en tiempo de ejecución antes de su uso.
	RE1	Los dispositivos integrados deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos Host

ID req	BR/RE	Explicación
HDR 2.4	BR	En caso de que un dispositivo host utilice tecnologías de código móvil, dicho dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo host: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a cargar código móvil en el dispositivo host; y c) controlar la ejecución del código basándose en comprobaciones de integridad en el código móvil y antes de que el código se ejecute.
	RE1	El dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
HDR 2.13	BR	Los dispositivos host deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos host deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
HDR 3.2	BR	Los dispositivos host deben contar con mecanismos homologados por el proveedor de productos del sistema de control que garanticen la protección contra códigos maliciosos. El proveedor del producto del sistema de control debe documentar cualquier requisito especial de configuración relacionado con la protección contra el código malicioso.
	RE1	El dispositivo host debe informar automáticamente de las versiones del software y de los archivos de protección contra el código malicioso en uso (como parte de la función de registro general).
HDR 3.10	BR	Los dispositivos host deben contar con la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos host deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
HDR 3.11	BR	Los dispositivos host deben ofrecer la capacidad de admitir mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos host deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
HDR 3.12	BR	Los dispositivos host deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.

HDR 3.13	BR	Los dispositivos host deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
HDR 3.14	BR	Los dispositivos host deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos host deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos de red

ID req	BR/RE	Explicación
NDR 1.6	BR	Un dispositivo de red que permita la gestión de acceso inalámbrico debe proporcionar la capacidad de identificar y autenticar a todos los usuarios (personas, procesos de software o dispositivos) que participan en la comunicación inalámbrica.
	RE1	El dispositivo de red debe proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios (personas, procesos o dispositivos de software) que participen en la comunicación inalámbrica.
NDR 1.13	BR	El dispositivo de red que permita el acceso de dispositivos a una red debe poder supervisar y controlar todos los métodos de acceso al dispositivo de red a través de redes que no son de confianza.
	RE1	El dispositivo de red debe proporcionar la capacidad de denegar las solicitudes de acceso a través de redes que no sean de confianza a menos que se apruebe explícitamente mediante un rol asignado.
NDR 2.4	BR	En caso de que un dispositivo de red utilice tecnologías de código móvil, el dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo de red: a) controlar la ejecución del código móvil; b) controlar qué usuarios (persona, proceso de software o dispositivo) están autorizados a transferir código móvil hacia/desde el dispositivo de red; y c) controlar la ejecución del código basándose en verificaciones de integridad antes de que el código se ejecute
	RE1	El dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
NDR 2.13	BR	Los dispositivos de red deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos de red deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.

NDR 3.2	BR	El dispositivo de red debe proporcionar protección contra códigos maliciosos.
NDR 3.10	BR	Los dispositivos de red deben admitir la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos de red deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
NDR 3.11	BR	Los dispositivos de red deben ofrecer mecanismos de detección y resistencia a la manipulación para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos de red deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
NDR 3.12	BR	Los dispositivos de red deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
NDR 3.13	BR	Los dispositivos de red deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
NDR 3.14	BR	Los dispositivos de red deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos de red deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.
NDR 5.2	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas de riesgo y conductos.
	RE1	El componente de red debe proporcionar la capacidad de denegar tráfico de red por defecto y permitir tráfico de red por excepción (también denominado "denegar todo, permiso por excepción").
	RE2	El componente de red debe ofrecer la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
NDR 5.3	RE3	El componente de red debe proporcionar la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo).

	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de proteger contra la recepción de mensajes de propósito general entre personas recibidos de usuarios o sistemas externos al sistema de control.

ANEXO IV: REQUISITOS PARA NIVEL SL4

Requisitos de seguridad del sistema

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
SR 1.1	BR	Todos los usuarios que accedan al sistema han de ser identificados y autenticados tanto a nivel de sistemas como de aplicación puede ser a través de contraseñas, dispositivos de acceso o multifactor (combinación de las anteriores).
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios humanos.
	RE2	El sistema de control debe proporcionar la capacidad de emplear la autenticación multifactor para permitir el acceso de usuarios humanos al sistema de control a través de una red que no es de confianza.
	RE3	El sistema de control debe proporcionar la capacidad de emplear la autenticación multifactor para permitir el acceso de todos los usuarios humanos al sistema de control.
SR 1.2	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar todos los procesos de software y dispositivos. Esta capacidad debe hacer cumplir dicha identificación y autenticación en todas las interfaces que proporcionen acceso al sistema de control para permitir los privilegios mínimos, de conformidad con las políticas y procedimientos de seguridad aplicables.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única todos los procesos de software y dispositivos.
SR 1.3	BR	El sistema de control debe tener la capacidad de gestionar cuentas de usuarios (agregar, eliminar, modificar o desactivar) estableciendo condiciones para pertenecer a un grupo y la asignación de autorizaciones. Sólo se admitirán cuentas compartidas, cuando por condiciones del sistema se establezca en el análisis de riesgo, aunque deberán de establecerse contramedidas y documentarlas.
	RE1	El sistema de control debe proporcionar la capacidad de admitir la gestión de cuentas unificada.
SR 1.4	BR	El sistema de control debe proporcionar la capacidad de admitir la gestión de los identificadores (permite operar dentro de un dominio o zona de control específico del sistema) por usuario, grupo, rol o interfaz del sistema de control.
SR 1.5	BR	El sistema de control debe proporcionar la capacidad de: 1) iniciar el contenido del autenticador; 2) cambiar todos los autenticadores predeterminados; 3) cambiar/actualizar los autenticadores; 4) protegerlos contra la divulgación y modificación no autorizada. Ejemplos de autenticadores son claves físicas, tarjetas de acceso, claves privadas, entre otras.

	RE1	Para los usuarios de procesos de software y dispositivos, el sistema de control debe proporcionar la capacidad de proteger los autenticadores pertinentes a través de mecanismos de hardware.
SR 1.6	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar a todos los usuarios que participen en una comunicación inalámbrica. Ejemplos de tecnologías inalámbricas son Bluetooth, infrarrojos, enrutadores móviles, etc.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios (personas, procesos de software o dispositivos) que participen en la comunicación inalámbrica.
SR 1.7	BR	En los sistemas de control que utilicen la contraseña como medio de autenticación debe aplicar una fortaleza configurable en base a la longitud mínima y la variedad de caracteres. Se aplicará vigencia máxima para las contraseñas y se notificará cuando esta expire. Esta protección se puede mejorar limitando la reutilización de las contraseñas.
	RE1	El sistema de control debe proporcionar la capacidad de evitar que una cuenta de un usuario humano determinada reutilice una contraseña para un número configurable de generaciones. Además, el sistema de control debe proporcionar la capacidad de aplicar restricciones de vigencia mínimas y máximas de las contraseñas a los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad.
	RE2	El sistema de control debe proporcionar la capacidad de aplicar restricciones de vigencia mínimas y máximas de las contraseñas a todos los usuarios.
SR 1.8	BR	En los casos en los que se utilice una PKI, el sistema de control debe proporcionar la capacidad de que una PKI funcione con arreglo a las mejores prácticas comúnmente aceptadas u obtener certificados de clave pública de una PKI existente. El registro de esta debe incluir la autorización de un supervisor que verifique la identidad del titular del certificado y que garantice que se emite al usuario previsto.
SR 1.9	BR	En el caso de los sistemas de control que utilicen autenticación de clave pública (PKI), el sistema de control debe proporcionar la capacidad de: l)validar los certificados comprobando la validez de la firma de un certificado determinado; m)validar los certificados a través de una ruta de certificación a una CA aceptada o, en el caso de los certificados autofirmados, desplegando certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; n)validar los certificados comprobando el estado de revocación de un certificado determinado; o)establecer el control del usuario sobre la clave privada correspondiente; y p)asignar la identidad autenticada a un usuario.
	RE1	El sistema de control debe proporcionar la capacidad de proteger las claves privadas pertinentes a través de mecanismos de hardware con arreglo a las prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad.
SR 1.10	BR	El sistema de control debe proporcionar la capacidad de ocultar la retroalimentación de la información de autenticación durante el proceso. No debe dar pistas sobre los fallos de autenticación como, por ejemplo, "nombre de usuario desconocido"
SR 1.11	BR	El sistema de control debe proporcionar la capacidad de aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por cualquier usuario dentro de un periodo configurable de tiempo.

SR 1.12	BR	El sistema de control debe proporcionar la capacidad de mostrar un mensaje de aviso del sistema antes de la autenticación. El personal autorizado debe poder configurar el mensaje de aviso de uso del sistema.
SR 1.13	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza. Debe permitir el acceso sólo cuando se esté autorizado y restringir el acceso desde conexiones telefónicas o no autorizadas. Es posible que los procedimientos requieran la autenticación multifactor para permitir el acceso remoto.
	RE1	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza.
FR2. Control de uso		
SR 2.1	BR	El sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control a fin de admitir el reparto de tareas y el privilegio mínimo. Verificar que las acciones del usuario están permitidas según el rol asignado y permitir que solo las personas cualificadas y autorizadas realicen cambios en los componentes del sistema.
	RE1	En todas las interfaces, el sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios (personas, procesos de software y dispositivos) para controlar el uso del sistema de control con el fin de admitir el reparto de tareas y el privilegio mínimo.
	RE2	El sistema de control debe proporcionar la capacidad de que un usuario o rol autorizado defina y modifique la asignación de permisos a roles para todos los usuarios humanos.
	RE3	El sistema de control debe admitir el permiso manual del supervisor de las autorizaciones actuales de los usuarios humanos para un tiempo o secuencia de eventos configurables.
	RE4	El sistema de control debe admitir la doble aprobación cuando la acción pueda resultar en un impacto grave en el proceso industrial.
SR 2.2	BR	El sistema de control debe proporcionar la capacidad de autorizar, supervisar y aplicar las restricciones de uso para las conexiones inalámbricas al sistema de control con arreglo a las prácticas comúnmente aceptadas en el sector de la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de identificar e informar de la presencia de dispositivos inalámbricos no autorizados que transmitan dentro del entorno físico del sistema de control.
SR 2.3	BR	El sistema de control debe proporcionar la capacidad de aplicar automáticamente las restricciones de uso configurables, que incluyen: a) prevenir el uso de dispositivos portátiles y móviles; b) requerir autorización basada en un contexto específico; y c) restringir la transferencia de códigos y datos a/de dispositivos portátiles y móviles.
	RE1	El sistema de control debe proporcionar la capacidad de verificar que los dispositivos portátiles y móviles que están intentando conectarse a la zona cumplan con los requisitos de seguridad de la misma.

SR 2.4	BR	El sistema de control debe proporcionar la capacidad de aplicar restricciones de uso para las tecnologías de código móvil basadas en la posibilidad de que causen daños al sistema de control, incluyendo: a) prevenir la ejecución del código móvil; b) requerir procesos de autenticación y autorización adecuados para el origen del código; c) restringir la transferencia del código móvil a/del sistema de control; y d) supervisar el uso del código móvil.
	RE1	El sistema de control debe proporcionar la capacidad de verificar la integridad del código móvil antes de autorizar que se ejecute el código.
SR 2.5	BR	El sistema de control debe proporcionar la capacidad de evitar un acceso posterior iniciando un bloqueo de la sesión tras un período de tiempo configurable de inactividad o mediante iniciación manual. La sesión debe continuar bloqueada hasta que el usuario autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados. En los casos en los que el sistema de control no pueda admitir el bloqueo de la sesión, la entidad responsable debería emplear las contramedidas compensatorias que se consideren adecuadas como mayores medidas de seguridad física y auditorias.
SR 2.6	BR	El sistema de control debe proporcionar la capacidad de terminar una sesión remota, ya sea automáticamente después de un período de inactividad configurable o manualmente por parte del usuario que inició la sesión.
SR 2.7	BR	El sistema de control debe proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado a un número configurable de sesiones.
SR 2.8	BR	El sistema de control debe proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de copias de seguridad y restauración, cambios en la configuración, actividad potencial de reconocimiento y eventos del registro de auditoría. Los registros individuales de auditoría deben incluir la marca de tiempo, fuente (dispositivo, proceso de software o cuenta de usuario humano de origen), categoría, tipo, identificador del evento y resultado del evento.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar de manera centralizada los eventos de auditoría y de elaborar registros de auditoría de múltiples componentes a través del sistema de control en una pista de auditoría para todo el sistema (lógica o física) con correlación de tiempo. El sistema de control debe proporcionar la capacidad de exportar dichos registros de auditorías en formatos habituales para la industria para que se analicen con las herramientas comerciales habituales de análisis de registros, como por ejemplo la administración de eventos e información de seguridad (SIEM).
SR 2.9	BR	El sistema de control debe asignar una capacidad suficiente de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros y la configuración del sistema. El sistema de control debe proporcionar mecanismos de auditoría para reducir la posibilidad de que se exceda dicha capacidad.
	RE1	El sistema de control debe proporcionar la capacidad de emitir un aviso cuando el volumen de almacenamiento de registros de auditoría asignado alcance un porcentaje configurable de capacidad máxima de almacenamiento de registros de auditoría.

SR 2.10	BR	El sistema de control debe proporcionar la capacidad de alertar al personal y evitar la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de auditorías. El sistema de control debe proporcionar la capacidad de admitir las acciones apropiadas en respuesta a un fallo en el procesamiento de auditorías de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
SR 2.11	BR	El sistema de control debe proporcionar marcas de tiempo (fecha y hora) para la generación de registros de auditoría. Evitar que las fuentes horarias sufran alteraciones no autorizadas.
	RE1	El sistema de control debe proporcionar la capacidad de sincronizar los relojes internos del sistema a una frecuencia configurable.
	RE2	Se debe evitar que la fuente horaria sufra alteraciones no autorizadas y, en caso de producirse una, se debe iniciar un evento de auditoría.
SR 2.12	BR	El sistema de control debe proporcionar la capacidad de determinar si un usuario humano ha realizado una acción concreta.
	RE1	El sistema de control debe proporcionar la capacidad de determinar si un usuario específico (persona, proceso de software o dispositivo) ha realizado una acción concreta.
FR3. Integridad del sistema		
SR 3.1	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el sistema para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos criptográficos para reconocer cambios de información durante la comunicación.
SR 3.2	BR	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección para prevenir, detectar, mitigar e informar de los efectos de un código malicioso o de software no autorizado. El sistema de control debe proporcionar la capacidad de actualizar los mecanismos de protección.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección contra códigos maliciosos en todos los puntos de entrada y salida.
	RE2	El sistema de control debe proporcionar la capacidad de gestionar los mecanismos de protección contra códigos maliciosos.
SR 3.3	BR	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad (medidas de antivirus, identificación, detección de intrusos y auditorias) e informar de las anomalías que se produzcan durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado. Las funciones de

		seguridad deben incluir todas las funciones que sean necesarias para cumplir con los requisitos de seguridad especificados en esta norma.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos automáticos para facilitar la gestión de la verificación de la seguridad durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado.
	RE2	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad durante las operaciones normales.
SR 3.4	BR	El sistema de control debe proporcionar la capacidad de detectar, registrar, informar y proteger contra cambios no autorizados en el software y en la información en reposo.
	RE1	El sistema de control debe proporcionar la capacidad de emplear herramientas automatizadas que notifiquen a un conjunto configurable de receptores cuando se produzcan discrepancias durante la verificación de la integridad.
SR 3.5	BR	El sistema de control debe validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que tengan un impacto directo en la acción del sistema de control. Las directrices a tener en cuenta deberían incluir la Code Review Guide del Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control debe proporcionar la capacidad de establecer el valor de salida a un estado predeterminado si no se puede mantener el funcionamiento normal como resultado de un ataque.
SR 3.7	BR	El sistema de control debe identificar y tratar las condiciones de error de manera tal que se pueda aplicar un remedio efectivo. Esto se debe hacer sin proporcionar información que pueda ser aprovechada por adversarios para atacar el sistema de control, a no ser que sea necesario para resolver los problemas de manera oportuna.
SR 3.8	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de las sesiones. El sistema de control debe rechazar cualquier uso por parte de identificadores de sesión no válidos.
	RE1	El sistema de control debe proporcionar la capacidad de anular los identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación).
	RE2	El sistema de control debe proporcionar la capacidad de generar un identificador de sesión único para cada sesión y considerar no válidos todos los identificadores de sesión imprevistos.
	RE3	El sistema de control debe proporcionar la capacidad de generar identificadores de sesión únicos con fuentes de aleatoriedad comúnmente aceptadas.
SR 3.9	BR	El sistema de control debe proteger la información y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
	RE1	El sistema de control debe proporcionar la capacidad de generar registros de auditoría en medios de solo una escritura mediante hardware.

FR4. Confidencialidad de los datos		
SR 4.1	BR	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información (especialmente en dispositivos portátiles) para la que se admite la autorización explícita de lectura, ya esté en reposo o en tránsito. La técnica elegida tenga en cuenta las posibles ramificaciones en el rendimiento del sistema de control y la capacidad de recuperarse tras un fallo del sistema o un ataque.
	RE1	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información en reposo y en sesiones con acceso remoto a través de una red que no es de confianza.
	RE2	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información que atraviese cualquier límite de la zona.
SR 4.2	BR	El sistema de control debe proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura de los componentes que vayan a ser liberados del servicio activo y/o puestos fuera de servicio.
	RE1	El sistema de control debe proporcionar la capacidad de evitar la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles (no retienen la información después de ser liberados para la gestión de la memoria).
SR 4.3	BR	Si se requiere el uso de criptografía, el sistema de control debe usar algoritmos criptográficos, tamaños de clave y mecanismos para el establecimiento y gestión de claves con arreglo a las prácticas y recomendaciones de seguridad comúnmente aceptadas en el sector que se encuentran en documentos como la Publicación Especial NIST SP800-57
FR5. Flujo de datos restringidos		
SR 5.1	BR	El sistema de control debe proporcionar la capacidad de segmentar de manera lógica las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de otras redes del sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de segmentar físicamente las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de las redes no críticas del sistema de control.
	RE2	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
	RE3	El sistema de control debe proporcionar la capacidad de aislar lógica y físicamente las redes críticas del sistema de control de redes no críticas del sistema de control.
SR 5.2	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas y conductos de riesgo. Como parte de una estrategia de protección de defensa total, se deberían dividir los sistemas de control de mayor impacto en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red con arreglo a las políticas y procedimientos de seguridad y a una evaluación de riesgos.

	RE1	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
	RE2	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
	RE3	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo). Esta función de "cierre en caso de fallo" debe designarse de tal forma que no interfiera en el funcionamiento de un sistema instrumentado de seguridad (SIS) o en otras funciones relacionadas con la seguridad.
SR 5.3	BR	Un sistema de control debe proporcionar la capacidad de evitar la recepción de mensajes de propósito general (correo electrónico, redes sociales o cualquier otro sistema de mensajería) entre personas recibidos de usuarios o sistemas externos al sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de evitar tanto la transmisión como la recepción de mensajes entre personas de propósito general.
SR 5.4	BR	El sistema de control debe proporcionar la capacidad de admitir la partición de datos (por medios físicos o lógicos), aplicaciones y servicios en base a su criticidad para facilitar la implementación de un modelo de zonificación.
FR6. Respuesta oportuna a los incidentes		
SR 6.1	BR	El sistema de control debe proporcionar la capacidad de que las personas y/o las herramientas autorizadas accedan a los registros de auditoría en modo de lectura.
	RE1	El sistema de control debe permitir el acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API).
SR 6.2	BR	El sistema de control debe proporcionar la capacidad de supervisar continuamente el rendimiento del mecanismo de seguridad utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
SR 7.1	BR	El sistema de control debe proporcionar la capacidad de funcionar en modo degradado durante un evento de denegación de servicio. Un evento de denegación de servicio en el sistema de control no debería afectar negativamente a ningún sistema relacionado con la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar las cargas de comunicación (por ejemplo, limitando la tasa) para mitigar los efectos de los tipos de desbordamiento de información de los eventos de denegación de servicio.

	RE2	El sistema de control debe proporcionar la capacidad de restringir la posibilidad de que cualquier usuario provoque eventos de denegación de servicio que puedan afectar a otros sistemas de control o redes.
SR 7.2	BR	El sistema de control debe proporcionar la capacidad de limitar el uso de recursos por parte de las funciones de seguridad para evitar el agotamiento de los recursos.
SR 7.3	BR	El sistema de control debe facilitar la identidad y ubicación de los archivos críticos y la capacidad de llevar a cabo copias de seguridad de la información a nivel del usuario y del sistema (incluyendo información sobre el estado del sistema) sin que esto afecte a las operaciones habituales.
	RE1	El sistema de control debe proporcionar la capacidad de verificar la fiabilidad de los mecanismos de copias de seguridad.
	RE2	El sistema de control debe proporcionar la capacidad de automatizar la función de copia de seguridad en base a una frecuencia configurable.
SR 7.4	BR	El sistema de control debe proporcionar la capacidad de recuperarse y reconstituirse hasta un estado seguro conocido después de una interrupción o fallo. Un estado seguro conocido significa que se atribuyen a todos los parámetros del sistema (ya sean predeterminados o configurables) valores seguros, se reinstalan los parches críticos para la seguridad, se restablecen los ajustes de configuración relacionados con la seguridad, se dispone de la documentación y los procedimientos operativos del sistema, se reinstala y configura la aplicación y el software del sistema con ajustes seguros, se carga la información de las copias de seguridad más recientes y conocidas y se somete a ensayo y se comprueba el funcionamiento del sistema en su totalidad.
SR 7.5	BR	El sistema de control debe proporcionar la capacidad de cambiar de y a una fuente de alimentación de emergencia sin que esto afecte el estado de seguridad existente o un modo degradado documentado.
SR 7.6	BR	El sistema de control debe proporcionar la capacidad de ser configurado de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El sistema de control debe proporcionar una interfaz a los ajustes de configuración de red y seguridad desplegados actualmente.
	RE1	El sistema de control debe proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad desplegados actualmente en un formato legible por una máquina.
SR 7.7	BR	El sistema de control debe proporcionar la capacidad de prohibir y/o restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
SR 7.8	BR	El sistema de control debe proporcionar la capacidad de informar de la lista actual de componentes instalados y de sus propiedades asociadas.

Requisitos de seguridad del componente generales

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
CR 1.1	BR	Los componentes deben proporcionar la capacidad de identificar y autenticar a todos los usuarios en todas las interfaces que permita el reparto de tareas y los privilegios mínimos. Se puede proporcionar a nivel componente o a nivel sistema.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios humanos.
	RE2	Los componentes deben proporcionar la capacidad de emplear la autenticación multifactor para todo el acceso de usuarios humanos al componente.
CR 1.2	BR	Los componentes deben proporcionar la capacidad de identificarse a sí mismos y autenticar a cualquier otro componente de acuerdo con el requisito del sistema SR 1.2 de la NormaIEC62443-3-3.Si el componente, como en el caso de una aplicación, se ejecuta en el contexto de un usuario humano, además, la identificación y autenticación del usuario humano de acuerdo con el requisito del sistema SR1.1 de la Norma IEC62443-3-3 puede formar parte del proceso de identificación y autenticación del componente hacia los demás componentes.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a cualquier otro componente.
CR 1.3	BR	Los componentes deben proporcionar la capacidad de permitir la gestión de todas las cuentas de forma directa o integrándose en un sistema que gestione las cuentas.
CR 1.4	BR	Los componentes deben proporcionar la capacidad de integrarse en un sistema que soporte la gestión de identificadores y/o la capacidad de permitir la gestión de identificadores.
CR 1.5	BR	Los componentes deben proporcionar la capacidad de: a) permitir el uso del contenido inicial del autenticador; b) permitir el reconocimiento de los cambios en los autenticadores predeterminados realizados en el momento de la instalación; c) funcionar correctamente con operaciones periódicas de modificación/actualización de los autenticadores; y d) proteger a los autenticadores de la divulgación y modificación no autorizada cuando se almacenan, utilizan y transmiten.
	RE1	Los autenticadores en los que se apoya el componente deben estar protegidos mediante mecanismos de hardware (Memoria protegida por contraseña, memoria OTP, comprobaciones de integridad hardware de datos y mecanismo de arranque de seguridad de dispositivos.).

CR 1.7	BR	Los componentes que utilicen autenticación basada en contraseña, deben proporcionar o integrarse en un sistema que proporcione la capacidad de aplicar la fortaleza de las contraseñas configurables de acuerdo con directrices de contraseñas reconocidas y probadas internacionalmente.
	RE1	Los componentes deben proporcionar, o integrarse en un sistema que proporcione la capacidad de proteger una cuenta de usuario humano determinada contra la reutilización de una contraseña para un número configurable de generaciones. Además, el componente debe proporcionar la capacidad de aplicar las restricciones de vigencia mínimas y máximas de las contraseñas para los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad. El componente debería proporcionar la capacidad de solicitar al usuario que cambie su contraseña en un tiempo configurable antes de su caducidad.
	RE2	Los componentes deben proporcionar, o integrarse en un sistema que proporcione, la capacidad de aplicar las restricciones mínimas y máximas de vigencia de las contraseñas para todos los usuarios.
CR 1.8	BR	Cuando se utilice una infraestructura de clave pública (PKI), el componente debe proporcionar o integrarse en un sistema que ofrezca la capacidad de interactuar y funcionar de conformidad con el requisito del sistema SR 1.8 de la Norma IEC62443-3-3.
CR 1.9	BR	Los componentes que utilicen autenticación basada en clave pública deben suministrarse directamente o integrarse en un sistema que ofrezca la capacidad en el mismo entorno del sistema de control para: a) validar los certificados comprobando la validez de la firma de un certificado determinado; b) validar la cadena de certificados o, en el caso de los certificados autofirmados, desplegar certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; c) validar los certificados comprobando el estado de revocación de un certificado determinado; d) establecer el control del usuario sobre la clave privada correspondiente; e) asignar la identidad autenticada a un usuario y f) garantizar que los algoritmos y claves utilizados para la autenticación de clave pública cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger las claves privadas críticas de larga duración mediante mecanismos de hardware.
CR 1.10	BR	Cuando un componente ofrezca la capacidad de autenticación, el componente debe ofrecer la capacidad de ocultar la retroalimentación de la información del autenticador durante el proceso de autenticación.
CR 1.11	BR	Cuando un componente ofrezca una capacidad de autenticación, el componente debe proporcionar la capacidad de: a) aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por parte de cualquier usuario durante un período de tiempo configurable; b) denegar el acceso durante un período de tiempo específico o hasta que un administrador lo desbloquee cuando se haya alcanzado este límite. Un administrador puede desbloquear una cuenta antes de la caducidad del período de tiempo de espera.
CR 1.12	BR	Cuando un componente proporcione un acceso de usuario humano local/IHM, debe proporcionar la capacidad de mostrar un mensaje de notificación de uso del sistema antes de la autenticación. Personal autorizado debe poder configurar el mensaje de notificación de uso del sistema.

CR 1.14	BR	Para los componentes que utilicen claves simétricas, el componente debe proporcionar la capacidad de: a) establecer la confianza mutua utilizando la clave simétrica; b) almacenar de forma segura el secreto compartido; c) restringir el acceso al secreto compartido; y d) garantizar que los algoritmos y claves utilizados para la autenticación de clave simétrica cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger claves simétricas críticas y de larga duración mediante mecanismos de hardware.
FR2. Control de uso		
CR 2.1	BR	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios identificados y autenticados en función de las responsabilidades que se les hayan asignado.
	RE1	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios en función de las responsabilidades que se les asignen y del privilegio mínimo.
	RE2	Los componentes, directamente o a través de un mecanismo de compensación de seguridad, deben proporcionar un rol autorizado para definir y modificar la asignación de permisos a roles para todos los usuarios humanos. Los roles no deberían limitarse a jerarquías fijas anidadas en las que un rol de nivel superior sea un superconjunto de un rol menos privilegiado. Por ejemplo, un administrador de sistema no debería incluir necesariamente privilegios de operador.
	RE3	Los componentes deben proporcionar el permiso manual del supervisor durante un tiempo o secuencia de eventos configurables. La implementación de un permiso manual, controlado y auditado de mecanismos automatizados en caso de emergencia u otros eventos graves permite a un supervisor autorizar a un operador para que reaccione rápidamente ante condiciones inusuales sin cerrar la sesión actual y establecer una nueva sesión como un usuario humano con mayores privilegios.
	RE4	Los componentes deben permitir la doble aprobación cuando la acción pueda tener un impacto grave en el proceso industrial. La doble aprobación debería limitarse a las acciones que requieran un nivel muy elevado de confianza de que se llevarán a cabo de forma fiable y correcta. No deberían emplearse mecanismos de doble aprobación cuando sea necesaria una respuesta inmediata para proteger la salud, la seguridad y el entorno, por ejemplo, la parada de emergencia de un proceso industrial.
CR 2.2	BR	Si un componente soporta el uso a través de interfaces inalámbricas, debe proporcionar la capacidad de integrarse en el sistema que soporta la autorización de uso, la supervisión y las restricciones de acuerdo con las prácticas industriales comúnmente aceptadas.
CR 2.5	BR	Si un componente proporciona una interfaz para un usuario humano, tanto si se accede localmente como a través de una red, el componente debe proporcionar la capacidad de: a) protegerse contra el acceso posterior iniciando un bloqueo de sesión después de un período de tiempo configurable de inactividad o mediante la iniciación manual por parte del usuario y b) mantener el bloqueo de la sesión hasta que el usuario propietario de la sesión, u otro usuario humano autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados.

CR 2.6	BR	Si un componente soporta sesiones remotas, el componente debe proporcionar la capacidad de terminar una sesión remota automáticamente después de un período de inactividad configurable, manualmente por parte de una autoridad local, o manualmente por parte del usuario que inició la sesión.
CR 2.7	BR	Los componentes deben proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado (persona, proceso de software o dispositivo).
CR 2.8	BR	Los componentes deben proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: a) control de acceso; b) errores de solicitud; c) eventos del sistema de control; d) evento de copia de seguridad y restauración; e) cambios de configuración; y f) eventos de registro de auditoría. Los registros de auditoría individuales deben incluir: a) marca de tiempo; b) fuente (dispositivo de origen, proceso de software o cuenta de usuario humano); c) categoría; d) tipo; e) ID del evento; y f) resultado del evento.
CR 2.9	BR	Los componentes deben: a) proporcionar la capacidad de asignar una capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros; y b) proporcionar mecanismos para proteger contra un fallo del componente cuando alcance o supere la capacidad de almacenamiento de datos de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de emitir un aviso cuando el almacenamiento de registros de auditoría asignado alcance un umbral de capacidad configurable.
CR 2.10	BR	Los componentes deben: a) proporcionar la capacidad de proteger contra la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de una auditoría; y b) proporcionar la capacidad para permitir las acciones apropiadas en respuesta a un fallo en el procesamiento de una auditoría de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
CR 2.11	BR	Los componentes deben proporcionar la capacidad de crear marcas de tiempo (incluyendo fecha y hora) para su uso en los registros de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de crear marcas de tiempo que estén sincronizadas con una fuente de tiempo de todo el sistema.
	RE2	El mecanismo de sincronización de tiempo debe proporcionar la capacidad de detectar alteraciones no autorizadas y causar un evento de auditoría tras la alteración.
CR 2.12	BR	Si un componente proporciona una interfaz para un usuario humano, el componente debe proporcionar la capacidad de determinar si un determinado usuario humano ha realizado una determinada acción. Los elementos de control que no puedan permitir tal capacidad se deben enumerar en los documentos de los componentes.
	RE1	Los componentes deben proporcionar la capacidad de verificar la autenticidad de la información recibida durante la comunicación.
FR3. Integridad del sistema		

CR 3.1	BR	Los componentes deben proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el componente para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	Los componentes deben proporcionar la capacidad de verificar la autenticidad de la información recibida durante la comunicación.
CR 3.3	BR	Los componentes deben proporcionar la capacidad de permitir la verificación de la operación prevista de las funciones de seguridad de acuerdo con el requisito del sistema.
	RE1	Los componentes deben proporcionar la capacidad para permitir la verificación del funcionamiento previsto de las funciones de seguridad durante las operaciones normales. Esta RE ha de ser implementada cuidadosamente para evitar efectos perjudiciales. Puede no ser adecuada para sistemas de seguridad.
CR 3.4	BR	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de integridad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de integridad.
	RE1	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de autenticidad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de autenticidad.
	RE2	Si el componente está realizando la verificación de la integridad, debe poder notificar automáticamente a una entidad configurable cuando descubra que se ha intentado realizar un cambio no autorizado.
CR 3.5	BR	Los componentes deben validar la sintaxis, la longitud y el contenido de cualquier dato de entrada que se utilice como entrada de control de procesos industriales o entrada a través de interfaces externas que tengan un impacto directo en la acción del componente.
CR 3.6	BR	Los componentes que se conectan física o lógicamente a un proceso de automatización deben proporcionar la capacidad de establecer salidas a un estado predeterminado si no se puede mantener el funcionamiento normal definido por el proveedor de componentes.
CR 3.7	BR	Los componentes deben identificar y tratar las condiciones de error de manera que no proporcionen información que pueda ser aprovechada por adversarios para atacar el sistema de control.
CR 3.8	BR	Los componentes deben proporcionar mecanismos para proteger la integridad de las sesiones de comunicación, incluyendo: a) la capacidad de invalidar identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación); b) la capacidad de generar un identificador de sesión único para cada sesión y reconocer solo los identificadores de sesión generados por el sistema; y c) la capacidad de generar identificadores de sesión únicos con fuentes de aleatoriedad comúnmente aceptadas.

CR 3.9	BR	Los componentes deben proteger la información de auditoría, los registros de auditoría y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
	RE1	Los componentes deben proporcionar la capacidad de almacenar registros de auditoría en medios de solo una escritura.
FR4. Confidencialidad de los datos		
CR 4.1	BR	Los componentes deben: a) proporcionar la capacidad de proteger la confidencialidad de la información en reposo para la que se admite la autorización explícita de lectura; y b) permitir la protección de la confidencialidad de la información en tránsito, como se define en el requisito del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Los componentes deben proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura, de los componentes que vayan a ser liberados del servicio activo y/o poner fuera de servicio.
	RE1	Los componentes deben proporcionar la capacidad de proteger contra la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles.
	RE2	Los componentes deben proporcionar la capacidad de verificar que se ha producido el borrado de la información.
CR 4.3	BR	Si se requiere el uso de criptografía, el componente debe utilizar mecanismos de seguridad criptográfica de acuerdo con prácticas y recomendaciones de seguridad internacionalmente reconocidas y probadas.
FR5. Flujo de datos restringidos		
CR 5.1	BR	Los componentes deben permitir una red segmentada que admitan zonas y conductos, según sea necesario, para permitir una arquitectura de red más amplia basada en la segmentación lógica y la criticidad.
FR6. Respuesta oportuna a los incidentes		
CR 6.1	BR	Los componentes deben proporcionar la capacidad para que las personas y/o las herramientas autorizadas puedan acceder a los registros de auditoría de solo lectura.
	RE1	Los componentes deben proporcionar acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API) o enviando los registros de auditoría a un sistema centralizado.
CR 6.2	BR	Los componentes deben proporcionar la capacidad de ser continuamente supervisados utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		

CR 7.1	BR	Los componentes deben proporcionar la capacidad de mantener las funciones esenciales cuando operen en modo degradado como resultado de un evento de denegación de servicio.
	RE1	Los componentes deben proporcionar la capacidad de mitigar los efectos de los tipos de eventos de denegación de servicio de desbordamiento de información y/o mensajes.
CR 7.2	BR	Los componentes deben proporcionar la capacidad de limitar el uso de recursos en las funciones de seguridad para proteger contra el agotamiento de los recursos.
CR 7.3	BR	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
	RE1	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
CR 7.4	BR	Los componentes deben proporcionar la capacidad de poder ser recuperados y reconstituidos hasta un estado de seguridad conocido después de una interrupción o fallo.
CR 7.6	BR	Los componentes deben proporcionar la capacidad de poder ser configurados de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El componente debe proporcionar una interfaz con los ajustes de configuración de red y seguridad actualmente desplegados.
	RE1	Los componentes deben proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad actualmente desplegados en un formato legible por una máquina.
CR 7.7	BR	Los componentes deben proporcionar la capacidad de restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
CR 7.8	BR	Los componentes deben proporcionar la capacidad de permitir un inventario de componentes del sistema de control de acuerdo con el requisito del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisitos de seguridad del componente a nivel de software

ID req	BR/RE	Explicación
SAR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del

		código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	La aplicación debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
SAR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.

Requisitos de seguridad para los dispositivos integrados (PLCs, IED)

ID req	BR/RE	Explicación
EDR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	El dispositivo integrado debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
EDR 2.13	BR	Los dispositivos integrados deben proteger contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, depuración JTAG).
	RE1	Los dispositivos integrados deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
EDR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.
EDR 3.10	BR	El dispositivo integrado debe admitir la capacidad de ser actualizado y someterse a una subida de nivel.
	RE1	El dispositivo integrado debe validar la autenticidad e integridad de cualquier actualización o subida de nivel del software antes de la instalación.
EDR 3.11	BR	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.

	RE1	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
EDR 3.12	BR	Los dispositivos integrados deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
EDR 3.13	BR	Los dispositivos integrados deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
EDR 3.14	BR	Los dispositivos integrados deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el arranque del componente y los procesos en tiempo de ejecución antes de su uso.
	RE1	Los dispositivos integrados deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos Host

ID req	BR/RE	Explicación
HDR 2.4	BR	En caso de que un dispositivo host utilice tecnologías de código móvil, dicho dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo host: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a cargar código móvil en el dispositivo host; y c) controlar la ejecución del código basándose en comprobaciones de integridad en el código móvil y antes de que el código se ejecute.
	RE1	El dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
HDR 2.13	BR	Los dispositivos host deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos host deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
HDR 3.2	BR	Los dispositivos host deben contar con mecanismos homologados por el proveedor de productos del sistema de control que garanticen la protección contra códigos maliciosos. El proveedor del producto del sistema de control debe documentar cualquier requisito especial de configuración relacionado con la protección contra el código malicioso.

	RE1	El dispositivo host debe informar automáticamente de las versiones del software y de los archivos de protección contra el código malicioso en uso (como parte de la función de registro general).
HDR 3.10	BR	Los dispositivos host deben contar con la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos host deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
HDR 3.11	BR	Los dispositivos host deben ofrecer la capacidad de admitir mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos host deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
HDR 3.12	BR	Los dispositivos host deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
HDR 3.13	BR	Los dispositivos host deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
HDR 3.14	BR	Los dispositivos host deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos host deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos de red

ID req	BR/RE	Explicación
NDR 1.6	BR	Un dispositivo de red que permita la gestión de acceso inalámbrico debe proporcionar la capacidad de identificar y autenticar a todos los usuarios (personas, procesos de software o dispositivos) que participan en la comunicación inalámbrica.
	RE1	El dispositivo de red debe proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios (personas, procesos o dispositivos de software) que participen en la comunicación inalámbrica.
NDR 1.13	BR	El dispositivo de red que permita el acceso de dispositivos a una red debe poder supervisar y controlar todos los métodos de acceso al dispositivo de red a través de redes que no son de confianza.

	RE1	El dispositivo de red debe proporcionar la capacidad de denegar las solicitudes de acceso a través de redes que no sean de confianza a menos que se apruebe explícitamente mediante un rol asignado.
NDR 2.4	BR	En caso de que un dispositivo de red utilice tecnologías de código móvil, el dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo de red: a) controlar la ejecución del código móvil; b) controlar qué usuarios (persona, proceso de software o dispositivo) están autorizados a transferir código móvil hacia/desde el dispositivo de red; y c) controlar la ejecución del código basándose en verificaciones de integridad antes de que el código se ejecute
	RE1	El dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
NDR 2.13	BR	Los dispositivos de red deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos de red deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
NDR 3.2	BR	El dispositivo de red debe proporcionar protección contra códigos maliciosos.
NDR 3.10	BR	Los dispositivos de red deben admitir la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos de red deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
NDR 3.11	BR	Los dispositivos de red deben ofrecer mecanismos de detección y resistencia a la manipulación para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos de red deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
NDR 3.12	BR	Los dispositivos de red deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
NDR 3.13	BR	Los dispositivos de red deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.

NDR 3.14	BR	Los dispositivos de red deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque
	RE1	Los dispositivos de red deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.
NDR 5.2	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas de riesgo y conductos.
	RE1	El componente de red debe proporcionar la capacidad de denegar tráfico de red por defecto y permitir tráfico de red por excepción (también denominado "denegar todo, permiso por excepción").
	RE2	El componente de red debe ofrecer la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
	RE3	El componente de red debe proporcionar la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo).
NDR 5.3	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de proteger contra la recepción de mensajes de propósito general entre personas recibidos de usuarios o sistemas externos al sistema de control.