IEC 62443-3-3:2013 Requisitos de seguridad de sistemas para la automatización industrial

Siete requisitos fundamentales, 51 requisitos de sistema

100 requisitos. Esta norma es certificable por un organismo acreditado. Versión de 07/2026.

La norma IEC 62443-3-3 admite certificación, y lo que se certifica es un sistema, no una organización ni una persona. Las vías son ISASecure SSA y el IECEE CB Scheme. Quien quiera certificar la organización necesita la 62443-2-1 o la 2-4, quien se refiera al componente necesita la 62443-4-2. Esta lista contiene los 51 requisitos de sistema y las 49 mejoras de requisito. Cuáles de ellos aplican depende del nivel de seguridad al que se aspire: 38 desde SL 1, 60 desde SL 2, 90 desde SL 3, los 100 en SL 4. Ninguna mejora aplica ya en SL 1. Esta lista es una ayuda de trabajo para la autoevaluación, no una prueba.

Empresa	Fecha	Elaborado por

5 FR 1: Quién o qué solicita el acceso, y si realmente es quien dice ser 24

SR 1.1 **Los usuarios humanos son identificados y su identidad se verifica antes de que obtengan acceso, en todos los puntos donde puedan operar o configurar el sistema de automatización. Esto incluye paneles de operador en la máquina, accesos de ingeniería y servicios de red.**

Cómo se demuestra: Inventario de todos los puntos de acceso del sistema, es decir HMI, sala de control, acceso de programación del PLC, switch, VPN y cliente de mantenimiento remoto, cada uno con el mecanismo de autenticación utilizado allí. Añadir un extracto de configuración o una captura de pantalla de la pantalla de inicio de sesión para cada clase de dispositivo. Una operación pequeña empieza con una tabla por dispositivo, columnas: dispositivo, interfaz, autenticación presente sí o no, justificación en caso de no. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.1 RE 1 **Cada usuario humano trabaja bajo un identificador individual asignado exclusivamente a esa persona. Las cuentas compartidas y de turno están deshabilitadas, las excepciones restantes se justifican caso por caso y se respaldan con medidas adicionales.**

Cómo se demuestra: Exportación de cuentas por sistema que relacione identificador con persona, lista de excepciones con justificación y medida compensatoria, por ejemplo una cámara o un registro de asistencia en el puesto de operador. Esta línea es una mejora de requisito y por tanto nunca es obligatoria en SL 1, se exige desde SL 2.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.1 RE 2 **Quien se conecte desde una red no confiable, por ejemplo desde internet o mediante una conexión de mantenimiento remoto, demuestra su identidad usando al menos dos factores independientes.**

Cómo se demuestra: Configuración del acceso remoto con el segundo factor activado, un registro de ejemplo de inicio de sesión que muestre ambos factores, y la lista de emisión de tokens o registros de aplicaciones. Una operación pequeña usa el segundo factor de la puerta de enlace VPN existente o una aplicación autenticadora, lo cual no cuesta nada más allá del tiempo de configuración. Mejora de requisito, exigida desde SL 3, no en SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.1 RE 3 **La verificación mediante dos factores independientes se aplica no solo al acceso desde el exterior, sino a cada inicio de sesión de un usuario humano, incluidos los inicios de sesión dentro de la red clasificada como confiable.**

Cómo se demuestra: Extracto de la política del servicio central de autenticación que muestre que el segundo factor se aplica sin ninguna excepción de red, más registros de muestra de inicio de sesión de la sala de control y del panel de operador. Mejora de requisito, exigida solo desde SL 4.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.2 **No solo las personas, sino también los procesos de software y los dispositivos se autentican ante el sistema antes de que se les permita intercambiar datos o usar servicios. Esto incluye los acoplamientos entre controladores, los enlaces de datos con sistemas de nivel superior y las herramientas de diagnóstico.**

Cómo se demuestra: Lista de las conexiones máquina a máquina con origen, destino, protocolo y la credencial utilizada en cada caso, por ejemplo certificado, cuenta de servicio o clave precompartida. Añadir un extracto de configuración de un acoplamiento que haga visible la autenticación. Exigido desde SL 2, no exigido en SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.2 RE 1 **Cada proceso de software y cada dispositivo presenta su propio identificador único. No se permiten cuentas de servicio compartidas ni una única clave usada en todo el sistema por muchos dispositivos.** Documento

Cómo se demuestra: Correspondencia de dispositivo a identificador o número de serie de certificado que demuestre que ningún identificador aparece dos veces. Mejora de requisito, exigida desde SL 3 y por tanto no forma parte de SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.3 **Las cuentas se gestionan a lo largo de todo su ciclo de vida: creación, cambio de privilegios, deshabilitación al causar baja y eliminación se rigen por reglas y están respaldadas por los sistemas implicados. Esto cubre cuentas de usuario, cuentas de servicio y cuentas de emergencia.** Documento

Cómo se demuestra: Registro de cuentas con tipo, propietario, propósito y estado, más evidencia de altas y bajas, por ejemplo un traspaso firmado o un ticket que muestre la deshabilitación con su fecha. Es recomendable una revisión periódica de cuentas, y en una operación pequeña basta con una conciliación anual de la lista de cuentas frente a la lista de personal. Exigido desde SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.3 RE 1 **La gestión de cuentas está unificada en todos los componentes del sistema, de modo que deshabilitar una cuenta en un lugar no permanezca sin efecto en dispositivos individuales.**

Cómo se demuestra: Evidencia de la integración con el directorio central, por ejemplo servicio de directorio o RADIUS, con una lista de los componentes conectados y una lista explícita de los dispositivos que no pueden conectarse junto con su procedimiento alternativo. Registro de prueba de una deshabilitación que surte efecto en todos los sistemas conectados. Mejora de requisito, exigida desde SL 3.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.4 **Los identificadores se emiten según reglas fijas, se asignan sin ambigüedad a una persona, un dispositivo o un rol, se retiran cuando ya no se usan y nunca se vuelven a asignar más tarde a otro titular.**

Cómo se demuestra: Regla de nomenclatura de los identificadores, por ejemplo apellido más inicial o código de planta más número, más el historial de identificadores retirados que demuestre que no se reutilizan. Una operación pequeña mantiene una única lista corrida con fecha de emisión y fecha de retiro. Exigido desde SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.5 **Los autenticadores tales como contraseñas, claves, certificados y tokens se emiten de forma ordenada, se cambian cuando se sospecha una divulgación y se revocan cuando es necesario. Las cuentas por defecto y las contraseñas de fábrica entregadas se cambian antes de la puesta en marcha.**

Cómo se demuestra: Lista de emisión de tokens y certificados con destinatario y fecha, evidencia de cambios y revocaciones, más una lista de verificación de puesta en marcha por dispositivo con el punto contraseña de fábrica cambiada, firmado. Exigido desde SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 1.5 RE 1 **Las credenciales de los procesos de software no se almacenan como archivo legible en el soporte de almacenamiento, sino en un almacenamiento respaldado por hardware que impide que la parte secreta pueda leerse.**

Cómo se demuestra: Evidencia de tipo del componente de seguridad utilizado, por ejemplo TPM, elemento seguro o HSM, con un extracto de configuración que demuestre que la clave se almacena dentro del componente. Un registro de compra o una hoja de datos es suficiente como evidencia de tipo. Mejora de requisito, exigida desde SL 3, no exigida en SL 1 ni SL 2.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.6 **El acceso inalámbrico al sistema, por ejemplo WLAN, mandos remotos por radio o diagnóstico por Bluetooth, solo puede usarse tras la identificación y autenticación tanto del usuario como del dispositivo, y se gestiona de forma deliberada.**

Cómo se demuestra: Inventario de todos los enlaces inalámbricos con propósito, alcance y método de cifrado, extracto de configuración del punto de acceso y la lista de dispositivos finales aprobados. Una operación pequeña documenta además qué interfaces inalámbricas de los dispositivos se han desactivado deliberadamente. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.6 RE 1 **Todo acceso inalámbrico debe poder atribuirse a un usuario específico o a un dispositivo específico, una clave de red compartida por todos los participantes no es suficiente.**

Cómo se demuestra: Evidencia de un método con credenciales individuales, por ejemplo autenticación WLAN empresarial contra un directorio o certificados por dispositivo, más un registro de conexión que muestre el identificador individual. Mejora de requisito, exigida desde SL 2 y por tanto no en SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.7 **Allí donde se usan contraseñas, su fortaleza mínima puede configurarse, por ejemplo longitud mínima y tipos de caracteres requeridos, y los valores configurados surten efecto para todas las cuentas afectadas.**

Cómo se demuestra: Extracto de configuración de la política de contraseñas por sistema con los valores realmente establecidos, por ejemplo longitud >= 10 caracteres y al menos tres tipos de caracteres, más una lista de los sistemas que técnicamente no puedan soportar este ajuste junto con su medida compensatoria. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.7 RE 1 **Para los usuarios humanos rigen reglas adicionales sobre la generación y vigencia de contraseñas: se impide la reutilización de contraseñas anteriores y la validez está limitada en el tiempo.**

Cómo se demuestra: Extracto de configuración que muestre el historial de contraseñas, por ejemplo bloqueo de reutilización de las últimas cinco contraseñas, y la validez máxima configurada. Mejora de requisito, exigida desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.7 RE 2 **El límite de vigencia de la contraseña se aplica no solo a las personas, sino a todas las cuentas, incluidas las de servicio, mantenimiento y dispositivo.**

Cómo se demuestra: Plan de rotación de cuentas técnicas con la fecha del último y del próximo cambio por cuenta, más evidencia de los cambios, por ejemplo un registro de cambio o un ticket. Mejora de requisito, exigida solo desde SL 4.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.8 **Allí donde se usan certificados, estos proceden de una gestión ordenada de certificados con reglas definidas para solicitud, emisión, periodo de validez, renovación y revocación.** Documento

Cómo se demuestra: Política de certificados o una breve regla escrita que indique responsabilidad, periodos de validez y la vía de revocación, más un inventario de los certificados emitidos con sus fechas de caducidad. Una operación pequeña mantiene una tabla con certificado, dispositivo, fecha de caducidad y fecha de recordatorio, lo que evita paradas de planta silenciosas causadas por certificados caducados. Exigido desde SL 2.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.9 **Cuando se usan pares de claves para la autenticación, el sistema valida el certificado por completo: cadena de confianza, periodo de validez, estado de revocación y prueba de que la contraparte realmente posee la clave privada. La relación entre certificado y cuenta es inequívoca.**

Cómo se demuestra: Extracto de configuración con la comprobación de revocación activada, por ejemplo CRL u OCSP, registro de prueba de un inicio de sesión rechazado con un certificado caducado o revocado, más la tabla de correspondencia de certificado a cuenta. Exigido desde SL 3, no exigido en SL 1 ni SL 2.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.9 RE 1 **Las claves privadas residen exclusivamente en un almacenamiento respaldado por hardware del que no pueden leerse, y también se usan dentro de ese almacenamiento.**

Cómo se demuestra: Hoja de datos o evidencia de certificación del componente de seguridad utilizado y un extracto de configuración que muestre que la clave se genera dentro del componente, de forma que la clave privada nunca lo abandona. Mejora de requisito, exigida solo desde SL 4.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.10 **Durante el inicio de sesión el sistema no revela ninguna información que pueda explotarse. Las contraseñas introducidas se ocultan y los mensajes de error no revelan si el identificador o la contraseña eran incorrectos.**

Cómo se demuestra: Captura de pantalla de la pantalla de inicio de sesión con la entrada enmascarada y una captura de pantalla del mensaje de error tras un intento fallido. Para dispositivos que técnicamente no puedan hacerlo, por ejemplo paneles de operador antiguos, añadir una breve nota sobre la medida compensatoria, por ejemplo acceso físico restringido al lugar de la instalación. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.11 **El número de intentos de inicio de sesión fallidos consecutivos está limitado y la respuesta a ello es configurable, por ejemplo un bloqueo temporal. La respuesta elegida no impide la operación de la planta relacionada con la seguridad.**

Cómo se demuestra: Extracto de configuración con el umbral, por ejemplo bloqueo tras <= 5 intentos fallidos, y la duración del bloqueo, más una breve valoración de por qué el bloqueo no impide la operación de emergencia ni una parada segura de la planta. En puestos de operador con función de seguridad, un bloqueo temporizado es preferible a un bloqueo de cuenta permanente. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.12 **Puede mostrarse un aviso de uso antes del inicio de sesión, que remita a las reglas de uso y monitorización del sistema. El texto y su presentación son configurables por el propietario del activo.**

Cómo se demuestra: Captura de pantalla del texto de aviso mostrado y la redacción aprobada con la fecha de aprobación. Las operaciones pequeñas acuerdan la redacción brevemente con la representación de los empleados o con la dirección, un párrafo es suficiente. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.13 **El acceso desde redes no confiables, por ejemplo el mantenimiento remoto por proveedores, está restringido a rutas definidas, se monitoriza y puede interrumpirse en cualquier momento.**

Cómo se demuestra: Inventario de las rutas de acceso remoto con propósito, parte remota, persona de contacto y la ruta utilizada, más registros de conexión y evidencia de la capacidad de desconexión, por ejemplo un interruptor de llave, una regla de cortafuegos o un enrutador de mantenimiento remoto que pueda apagarse. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 1.13 RE 1 **Cada sesión individual desde una red no confiable es aprobada explícitamente por una persona responsable antes de establecer la conexión, una conexión permanentemente abierta no es suficiente.**

Cómo se demuestra: Registros de aprobación por sesión de mantenimiento remoto con hora, motivo, persona que aprueba y duración, técnicamente por ejemplo mediante un interruptor de llave en el enrutador de acceso o mediante un portal de aprobación. En una operación pequeña basta con un cuaderno de bitácora de mantenimiento remoto en el armario de control, firmado por el técnico de mantenimiento en cada sesión. Mejora de requisito, exigida desde SL 2 y por tanto nunca en SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6 FR 2: Control de uso (privilegios, sesiones, registros de auditoría) 24

SR 2.1 **El sistema aplica técnicamente los privilegios que se han concedido: cada persona conectada, cada dispositivo y cada proceso de software recibe exactamente el acceso que se le ha asignado, y cualquier intento que vaya más allá es rechazado.**

Cómo se demuestra: Un concepto de privilegios que relacione cuentas con permisos, más una captura de pantalla o un extracto de configuración por sistema de control, HMI y estación de ingeniería que muestre los privilegios activos. Además, un registro de prueba en el que una cuenta con pocos privilegios intenta una acción bloqueada y es rechazada. Exigido desde SL 1. Una operación pequeña se gestiona con dos o tres roles, por ejemplo operar, mantener, diseñar, y los documenta en una sola página.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.1 RE 1 **La aplicación de privilegios se refiere no solo a los operadores humanos, sino igualmente a los procesos de software y dispositivos que acceden al sistema por sí mismos.**

Cómo se demuestra: Una lista de cuentas técnicas y de servicio, por ejemplo clientes OPC UA, conexiones de historian, servicios de copia de seguridad, cada una con su conjunto de privilegios asignado. Un extracto de la gestión de privilegios que muestre que estas cuentas no funcionan con derechos de administrador. Mejora de requisito, exigida desde SL 2, no en SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.1 RE 2 **Los privilegios no se conceden a las personas de forma individual sino a través de roles, y la correspondencia entre rol y acciones permitidas queda registrada de forma trazable.** Documento

Cómo se demuestra: Una matriz de roles y privilegios en forma de tabla: las filas son los roles, las columnas las acciones tales como cambiar un valor de consigna, descargar un programa, reconocer una alarma, crear una cuenta. Más la lista de correspondencia entre persona y rol. Mejora de requisito, exigida desde SL 2. Una hoja de cálculo mantenida con fecha de cambio es evidencia totalmente suficiente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.1 RE 3 **Para casos excepcionales estrictamente definidos, un supervisor autorizado puede levantar una restricción de privilegios por un periodo limitado, y cada una de estas excepciones queda registrada en el rastro de auditoría.**

Cómo se demuestra: Una descripción del procedimiento de aprobación de excepciones que indique quién puede concederla y cuánto tiempo permanece vigente, más registros de auditoría de excepciones ya concedidas, tomados del registro del sistema. Mejora de requisito, exigida desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.1 RE 4 **Las intervenciones especialmente críticas requieren la aprobación de dos personas autorizadas independientes antes de ejecutar la acción.**

Cómo se demuestra: Una lista de las acciones sujetas a doble aprobación, por ejemplo cambiar parámetros de seguridad o descargar un nuevo programa de control, junto con evidencia de configuración y registros de auditoría que identifiquen a ambos aprobadores. Mejora de requisito, exigida solo desde SL 4.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.2 **El uso de conexiones inalámbricas en la red de automatización está vinculado a una autorización explícita, y solo los participantes aprobados pueden intercambiar datos o intervenir de forma inalámbrica.**

Cómo se demuestra: Un inventario de todos los enlaces inalámbricos, por ejemplo puntos de acceso WLAN, emparejamientos Bluetooth, enrutadores de telefonía móvil, cada uno con su propósito y sus participantes aprobados. Más la configuración de control de acceso en el punto de acceso. Exigido desde SL 1. Quien no opere ningún enlace inalámbrico en la red de proceso lo declara exactamente así por escrito y lo respalda con una vista de configuración que muestre lo inalámbrico deshabilitado.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.2 RE 1 **Los dispositivos inalámbricos no autorizados en las inmediaciones de la red de automatización se detectan y se notifican.**

Cómo se demuestra: Un registro de la monitorización inalámbrica o de un escaneo inalámbrico periódico con fecha, lista de resultados y una nota sobre cada dispositivo desconocido. Se nombra la vía de notificación a la función responsable. Mejora de requisito, exigida desde SL 2, no en SL 1. Una operación pequeña puede realizar un escaneo trimestral con un portátil y archivar el resultado como registro.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.3 **El uso de dispositivos portátiles y móviles en el sistema, por ejemplo portátiles de servicio, almacenamiento USB o tabletas, se rige por reglas y está técnicamente limitado a dispositivos aprobados de forma explícita.**

Cómo se demuestra: El conjunto de reglas para el uso de dispositivos, una lista de dispositivos de servicio aprobados con sus identificadores, y evidencia de la restricción técnica, por ejemplo puertos USB en HMI y estación de ingeniería deshabilitados o limitados a dispositivos concretos. Exigido desde SL 1. Una operación pequeña trabaja con dos memorias de servicio etiquetadas que solo se escriben en una única estación de transferencia.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.3 RE 1 **Antes de la conexión se comprueba el estado de seguridad de un dispositivo portátil o móvil, y se impide el acceso a los dispositivos que no cumplan los requisitos.**

Cómo se demuestra: Los criterios de comprobación del estado del dispositivo, por ejemplo protección antimalware actualizada y nivel de parches, más registros de comprobación por dispositivo de servicio y evidencia de la aplicación técnica, por ejemplo mediante una estación de transferencia o un control de acceso a la red. Mejora de requisito, exigida desde SL 3.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.4 **Para el código móvil ejecutado en el sistema, por ejemplo scripts en interfaces de operador o contenido activo en informes, se define qué tipos están permitidos, y se impide la ejecución de los tipos no permitidos.** Documento

Cómo se demuestra: Una definición de qué código móvil está permitido en qué sistemas, más evidencia de configuración de la restricción, por ejemplo ejecución de scripts en el navegador HMI deshabilitada, macros en archivos de evaluación bloqueadas. Exigido desde SL 1. Una definición de una página que cubra los tres o cuatro casos que realmente existen es suficiente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.4 RE 1 **Antes de ejecutar código móvil se verifica que proviene de la fuente esperada y que no ha sido alterado.**

Cómo se demuestra: Evidencia de configuración de la verificación de firma o del control de suma de comprobación, más un registro de prueba en el que se rechaza código manipulado o sin firmar. Mejora de requisito, exigida desde SL 3.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.5 **Una sesión se bloquea tras un periodo definido sin acción del operador y solo se libera de nuevo tras una nueva autenticación, sin perder la visualización de la información de proceso relevante para la seguridad.**

Cómo se demuestra: Un extracto de configuración con el tiempo de bloqueo configurado por puesto de trabajo, más una justificación para los puestos de trabajo en salas de control permanentemente atendidas donde el bloqueo se configura deliberadamente de otra manera. Exigido desde SL 1. Evidencia visual: una captura de pantalla de la pantalla de bloqueo con la línea de alarma aún visible.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.6 **Las sesiones remotas se terminan tras un periodo definido sin actividad o a petición del operador, de manera que no quede ninguna conexión remota abierta sin supervisión.**

Cómo se demuestra: La configuración de acceso remoto con su límite de tiempo de inactividad, registros de auditoría de sesiones remotas terminadas, y una descripción de cómo el operador puede desconectar de inmediato una sesión de mantenimiento remoto en curso, por ejemplo mediante un interruptor de llave o una liberación por sesión. Exigido desde SL 2, no en SL 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.7 **El número de sesiones simultáneas por cuenta o rol está limitado, y los intentos de inicio de sesión que superen ese límite se rechazan.**

Cómo se demuestra: Un extracto de configuración con el límite superior definido por rol, por ejemplo <= 1 sesión simultánea para cuentas de ingeniería, más un registro de prueba del segundo intento de inicio de sesión rechazado. Exigido desde SL 3.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.8 **Los eventos relevantes para la seguridad se registran, y cada entrada indica al menos la hora, el origen, la cuenta que lo desencadenó, el tipo de evento y el resultado.** Documento

Cómo se demuestra: Una definición de los tipos de evento que deben registrarse, por ejemplo inicio de sesión, inicio de sesión fallido, cambio de privilegios, cambio de programa, cambio de configuración, más un extracto real del registro de auditoría que muestre los campos indicados. Exigido desde SL 1. Una operación pequeña reúne los registros del sistema de control, HMI y cortafuegos en una carpeta con un periodo de retención fijo.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.8 RE 1 **Los registros de auditoría de los distintos componentes se reúnen en un punto central y forman un único registro a nivel de todo el sistema que puede evaluarse en conjunto.**

Cómo se demuestra: Un esquema de arquitectura de la recopilación de registros que muestre todas las fuentes conectadas, más una evaluación que sitúe eventos de al menos dos componentes en una misma línea temporal. Mejora de requisito, exigida desde SL 3.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.9 **Se dispone de almacenamiento suficiente para los registros de auditoría, de forma que los eventos se conserven durante el periodo de retención definido y no se sobrescriban de forma involuntaria.**

Cómo se demuestra: Un cálculo o estimación de la necesidad de almacenamiento a partir del volumen diario de registros por el periodo de retención, más el tamaño de almacenamiento configurado y la regla de archivado. Exigido desde SL 1. En la práctica basta con una copia diaria a una ubicación de almacenamiento separada con un periodo de retención documentado.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 2.9 RE 1 **Cuando se alcanza un umbral definido de nivel de llenado del almacenamiento de auditoría, se emite una advertencia a la función responsable antes de que la capacidad de almacenamiento se agote por completo.**

Cómo se demuestra: Un extracto de configuración del umbral, por ejemplo una advertencia a partir de >= 80 por ciento de utilización, más un ejemplo de la notificación disparada y la lista de destinatarios. Mejora de requisito, exigida desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.10 **Si el registro de auditoría falla o el almacenamiento de auditoría se llena, el sistema reacciona de una manera previamente definida y se informa a la función responsable, sin poner en peligro la operación segura de la planta.**

Cómo se demuestra: La reacción definida para cada caso de fallo, por ejemplo sobrescribir las entradas más antiguas y generar una notificación en lugar de detener la planta, con una justificación desde el punto de vista del proceso. Evidencia mediante una notificación de prueba disparada y la entrada de auditoría correspondiente. Exigido desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.11 **Cada registro de auditoría lleva una marca de tiempo procedente de una fuente horaria identificada, de modo que los eventos de distintos componentes puedan ordenarse entre sí.**

Cómo se demuestra: Una indicación de la fuente horaria usada por componente y un extracto de registro con una marca de tiempo visible que incluya la zona horaria. Exigido desde SL 2, no en SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.11 RE 1 **Los relojes de todos los componentes participantes están sincronizados con una fuente horaria común de forma que la desviación se mantenga dentro de un límite definido.**

Cómo se demuestra: La configuración de sincronización horaria, por ejemplo servidor NTP e intervalo de sincronización, más un registro de comprobación con la desviación medida por componente frente al límite definido, por ejemplo <= 1 segundo. Mejora de requisito, exigida desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.11 RE 2 **La propia fuente horaria está protegida contra manipulaciones, y una referencia horaria inverosímil o alterada se detecta y se notifica.**

Cómo se demuestra: Una descripción de cómo está protegida la fuente horaria, por ejemplo sincronización horaria autenticada, restricción a una fuente interna, monitorización de saltos de tiempo, más notificaciones o registros de auditoría de una desviación detectada. Mejora de requisito, exigida solo desde SL 4.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.12 **Para acciones críticas definidas, puede establecerse sin lugar a dudas a posteriori quién las desencadenó, de modo que la persona que actuó no pueda negar de forma creíble haberlo hecho.** Documento

Cómo se demuestra: Una lista de las acciones a las que se aplica esta evidencia, por ejemplo cambio de receta, liberación de lote, cambio de valores límite, más los registros correspondientes con un identificador de persona único y evidencia de que las cuentas de grupo están excluidas para estas acciones. Exigido desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 2.12 RE 1 **La atribución irrefutable de la persona que actúa se aplica no solo a acciones críticas seleccionadas, sino a todos los usuarios y a todas las acciones que desencadenan.**

Cómo se demuestra: Evidencia de que cada cuenta está vinculada a una única persona y de que no quedan inicios de sesión compartidos, más un extracto de registro de acciones cualesquiera en el que aparece de forma consistente un identificador de persona único. Mejora de requisito, exigida solo desde SL 4.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7 FR 3: Integridad del sistema, protección de datos, software y sesiones frente a modificaciones no autorizadas 19

SR 3.1 **El sistema de control detecta cuando la información ha sido alterada en tránsito por un canal de comunicación, y lo hace tanto para datos de control como para datos de configuración y tráfico de gestión. La protección cubre también las conexiones que salen del sistema o que cruzan segmentos de red no confiables.**

Cómo se demuestra: Una visión general de red y protocolos que indique qué canal usa qué mecanismo de integridad (suma de comprobación, código de autenticación de mensaje, telegramas firmados), un extracto de configuración de los ajustes de seguridad del bus de campo u OPC UA, y un registro de prueba que muestre que un telegrama manipulado fue rechazado de forma demostrable. Una operación pequeña recoge esto en una tabla por conexión con las columnas origen, destino, protocolo y mecanismo de integridad, y demuestra la eficacia una vez con una captura de tráfico. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.1 RE 1 **La protección de integridad en tránsito se apoya en mecanismos criptográficos, de forma que una manipulación deliberada por parte de un atacante con medios propios no pueda pasar inadvertida. Una simple suma de comprobación frente a errores de transmisión no es suficiente aquí.**

Cómo se demuestra: Una lista de los mecanismos criptográficos y longitudes de clave en uso por canal, una referencia a la gestión de claves subyacente, y extractos de configuración (por ejemplo conjuntos de cifrado TLS, SecurityPolicy de OPC UA, perfiles IPsec). Las operaciones pequeñas se apoyan en los perfiles seguros por defecto de sus controladores y archivan una captura de pantalla del ajuste activo. Mejora de requisito, exigida desde SL 3 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.2 **Existen mecanismos de protección contra código malicioso que impiden la ejecución de código de programa no deseado en los componentes del sistema y que notifican cualquier detección. Los mecanismos se eligen de forma que no perturben la operación prevista de la planta, y se mantienen actualizados.**

Cómo se demuestra: Una visión general por componente de qué mecanismo aplica (antivirus, listas blancas de aplicaciones, sistema operativo reforzado sin derechos de ejecución), evidencia de que las firmas o listas blancas se actualizan, y alertas del sistema de protección. Cuando el antivirus no es viable, por ejemplo en un controlador, la medida compensatoria se registra con su justificación. A las operaciones pequeñas les va bien con listas blancas en el PC de operador y una regla escrita para medios USB. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.2 RE 1 **La protección contra código malicioso surte efecto adicionalmente en los puntos de entrada y salida de la planta, donde los datos entran o salen, y no solo en los propios equipos finales.**

Cómo se demuestra: Una lista de todos los puntos de entrada y salida (acceso de mantenimiento remoto, pasarela de transferencia de datos, medios extraíbles, traspaso a la red de oficina, vía de correo electrónico para versiones de programa) con el mecanismo de escaneo efectivo en cada uno, más registros de los traspasos que se comprobaron. Las operaciones pequeñas configuran un único PC de traspaso con escaneo de virus como pasarela y lo fijan en una instrucción de trabajo. Mejora de requisito, exigida desde SL 2 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.2 RE 2 **Los mecanismos de protección contra código malicioso se gestionan desde un punto central, las actualizaciones se distribuyen de forma centralizada, y las detecciones se recopilan en un único lugar para su evaluación.**

Cómo se demuestra: La configuración de la consola de gestión central, un informe sobre el estado de actualización de todos los componentes conectados, y una evaluación de las detecciones notificadas a lo largo de un periodo de tiempo. Mejora de requisito, exigida desde SL 3 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.3 **Las funciones de seguridad del sistema se verifican a intervalos planificados y después de cambios para confirmar que realmente funcionan. Las pruebas se programan de forma que no pongan en peligro la operación de la planta, y los resultados se registran.** Documento

Cómo se demuestra: Un plan de pruebas que indique el objeto de la prueba, el intervalo y la ventana de tiempo, junto con los registros de prueba que muestren fecha, examinador, comportamiento esperado y comportamiento observado. Pruebas individuales útiles son: un inicio de sesión con una cuenta deshabilitada falla, el antivirus reacciona a un archivo de prueba, el acceso de mantenimiento remoto es inalcanzable sin liberación. Las operaciones pequeñas asocian las pruebas a la parada de mantenimiento ya planificada y trabajan con una lista de verificación fija. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.3 RE 1 **La verificación de las funciones de seguridad se ejecuta con medios automatizados, de forma que sea repetible sin esfuerzo manual y entregue un resultado consistente.**

Cómo se demuestra: Los scripts o herramientas de prueba junto con su calendario, sus archivos de salida, y una comparación de varias ejecuciones que demuestre que se detectan desviaciones. Mejora de requisito, exigida desde SL 3 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.3 RE 2 **La verificación de las funciones de seguridad también es posible durante la operación normal, sin tener que detener la planta ni ponerla en un estado especial.**

Cómo se demuestra: Una descripción del procedimiento de prueba con evidencia de que no tiene efecto adverso sobre el proceso, por ejemplo un análisis del impacto en los tiempos de ciclo y en la carga de red, más registros de prueba tomados de la operación productiva. Mejora de requisito, exigida desde SL 4 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.4 **Se detectan los cambios no autorizados en el software, el firmware y la información en reposo. Esto se aplica por igual a los programas de control, los conjuntos de parámetros, las recetas y los archivos de configuración.**

Cómo se demuestra: Un inventario de las versiones dignas de protección con los valores de comprobación o firmas almacenados, los resultados de las comparaciones de integridad, y la conciliación documentada con la versión guardada en el control de versiones. Las operaciones pequeñas guardan la versión de programa liberada junto con su suma de comprobación en una ubicación protegida contra escritura y comparan ante sospecha o tras el mantenimiento. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.4 RE 1 **Si se detecta una violación de la integridad del software o de la información, el sistema lo notifica automáticamente a un punto responsable, sin que nadie tenga que buscarlo activamente.**

Cómo se demuestra: La configuración de las vías de notificación (alarma en la sala de control, correo electrónico, mensaje al sistema de monitorización), una lista de destinatarios con arreglos de suplencia, y al menos una alarma de prueba con un tiempo de respuesta documentado. Mejora de requisito, exigida desde SL 3 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.5 **Las entradas que el sistema acepta procedentes de datos de proceso, interfaces o interfaces de usuario se comprueban en cuanto a sintaxis permitida, rango de valores permitido y longitud permitida antes de procesarlas. Las entradas no válidas no provocan un comportamiento incontrolado.**

Cómo se demuestra: Una especificación de los límites y formatos por entrada, extractos de la lógica de validación en el controlador o la aplicación, y casos de prueba con entradas deliberadamente inválidas (un valor demasiado grande, un tipo de dato erróneo, una cadena de caracteres demasiado larga) junto con el comportamiento documentado del sistema. Las operaciones pequeñas registran los límites de plausibilidad por punto de medición en una tabla y los verifican durante la puesta en marcha. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 3.6 **Para el caso de un fallo se define qué estado adoptan las salidas hacia la planta, y el sistema adopta exactamente ese estado. El estado definido está alineado con la seguridad funcional de la planta.**

Cómo se demuestra: Una definición por salida o grupo de salidas (mantener valor, valor sustituto definido, estado de parada segura) con una justificación procedente de la evaluación de riesgos, un extracto de configuración del controlador, y evidencia de una prueba de fallo, por ejemplo una rotura de cable o una pérdida de comunicación, que muestre el comportamiento esperado. Exigido desde SL 1 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.7 **El sistema gestiona las condiciones de error de forma que la operación permanezca bajo control y no se revele ninguna información que ayude a un atacante. Los mensajes de error mostrados a los operadores se mantienen breves, mientras que los detalles técnicos solo pasan a los registros internos.**

Cómo se demuestra: Una visión general de las clases de error con el comportamiento del sistema previsto para cada una, ejemplos de los mensajes mostrados comparados con las entradas de registro internas correspondientes, y evidencia de prueba de que ninguna ruta de archivo, nombre de cuenta, salida de base de datos o detalle de versión aparece en la interfaz de operador. Exigido desde SL 1 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.8 **Las sesiones activas están protegidas contra el secuestro y contra la inyección de mensajes ajenos. Una sesión termina tras el cierre de sesión o tras un periodo definido sin actividad, y después no puede reutilizarse.**

Cómo se demuestra: La configuración de la gestión de sesiones con los límites configurados para el tiempo de inactividad y la duración máxima, evidencia del mecanismo que protege contra la repetición de mensajes, y un registro de prueba en el que una sesión capturada ya no funciona tras el cierre de sesión. Exigido desde SL 2 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.8 RE 1 **Los identificadores de sesión pierden su validez cuando la sesión termina y el sistema no vuelve a aceptarlos, ni siquiera cuando se presentan de nuevo desde el exterior.**

Cómo se demuestra: Un extracto de configuración de la gestión de sesiones que cubra la invalidación, más un registro de prueba en el que un identificador previamente válido se envía de nuevo tras el cierre de sesión y el sistema lo rechaza. Mejora de requisito, exigida desde SL 3 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.8 RE 2 **Para cada sesión nueva se genera un identificador dedicado de un solo uso. Los identificadores no se reutilizan entre sesiones, usuarios o dispositivos.**

Cómo se demuestra: Una descripción del procedimiento de generación y evidencia del registro o de una captura de tráfico de que varios inicios de sesión consecutivos reciben identificadores distintos. Mejora de requisito, exigida desde SL 3 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.8 RE 3 **Los identificadores de sesión se generan con mecanismos aleatorios reconocidos, de forma que no puedan adivinarse ni derivarse de identificadores anteriores.**

Cómo se demuestra: Una indicación del generador de números aleatorios utilizado y su fuente de entropía, una declaración del proveedor o un informe de prueba al respecto, y una evaluación estadística de una muestra de identificadores generados. Mejora de requisito, exigida desde SL 4 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.9 **Los registros relacionados con la seguridad y las herramientas usadas para evaluarlos están protegidos contra el acceso, la modificación y la eliminación no autorizados. El círculo de personas autorizadas a cambiar o eliminar registros se mantiene reducido y está identificado.** Documento

Cómo se demuestra: Un concepto de autorización para los datos de registro con asignación nominal, la configuración del reenvío a un sistema de registro separado, periodos de retención, y evidencia de prueba de que un operador ordinario no puede eliminar entradas. Las operaciones pequeñas reenvían los registros a un dispositivo separado al que los operadores de planta no tienen acceso de escritura. Exigido desde SL 2 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 3.9 RE 1 **Los registros relacionados con la seguridad se almacenan adicionalmente en un soporte que excluye la sobrescritura posterior, de forma que una entrada ya escrita no pueda alterarse más, ni siquiera con derechos administrativos.** Documento

Cómo se demuestra: Una descripción del almacenamiento utilizado (soporte de escritura única, archivo resistente a manipulaciones, cadena de firmas continuamente extendida), evidencia de un intento fallido de cambiar una entrada, y la regla de conservación y recuperación de los soportes. Mejora de requisito, exigida desde SL 3 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8 FR 4: Confidencialidad de los datos 6

SR 4.1 **El sistema de automatización protege la información confidencial frente a la divulgación no autorizada, tanto en tránsito como en reposo. Se define qué datos cuentan como confidenciales, por ejemplo recetas, conjuntos de parámetros, credenciales, archivos de configuración o datos de diagnóstico con referencia personal.** Documento

Cómo se demuestra: Una lista de los tipos de datos dignos de protección, indicando dónde se guardan y cómo se transmiten, más la medida de protección específica para cada entrada, por ejemplo una conexión cifrada, un soporte de almacenamiento cifrado o un recurso compartido restringido. Una operación pequeña se gestiona con una tabla de una sola página: tipo de dato, dónde se encuentra, quién puede verlo, qué lo protege. Exigido desde SL 1 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 4.1 RE 1 **Para la información que viaja por redes no confiables o se almacena fuera del entorno protegido, la confidencialidad se hace cumplir por medios técnicos y no meramente se promete en una regla organizativa.**

Cómo se demuestra: Un extracto de configuración del cifrado de transporte o de almacenamiento en uso, por ejemplo el perfil VPN para mantenimiento remoto, los ajustes TLS de la interfaz del sistema de control, o el cifrado de los soportes de copia de seguridad. Una captura de pantalla fechada del ajuste activo es suficiente como evidencia. Exigido desde SL 2 en adelante, no desde SL 1, porque esta es una mejora de requisito.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 4.1 RE 2 **La confidencialidad también se hace cumplir en los límites entre zonas, de forma que la información no quede visible en claro cuando cruza de una zona a otra.**

Cómo se demuestra: Un plan de zonas y conductos que marque qué cruces están cifrados, junto con la configuración del componente de frontera tal como una pasarela, un cortafuegos o un diodo de datos. Una captura de tráfico o un registro de prueba que muestre que no aparecen datos en texto claro en la frontera. Exigido desde SL 4 en adelante.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR 4.2 **Se define cómo se elimina de forma fiable la información confidencial cuando los dispositivos se dan de baja, cambian de propietario, salen a reparación o se reutilizan, de modo que no queden datos residuales legibles.** Documento

Cómo se demuestra: Un procedimiento de baja escrito con el método de saneamiento por tipo de dispositivo, más registros de borrado que indiquen la identificación del dispositivo, la fecha y la persona que lo llevó a cabo. Una operación pequeña registra esto como una línea por dispositivo en una lista compartida y archiva junto a ella los certificados de los contratistas externos de eliminación. Exigido desde SL 2 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 4.2 RE 1 **Las áreas de almacenamiento compartidas se purgan antes de reasignarse a otro usuario o proceso, de modo que el contenido perteneciente al usuario anterior no pueda leerse.**

Cómo se demuestra: Una declaración del proveedor o un registro de configuración que cubra la purga de las áreas de memoria y búfer reutilizadas, complementado con un registro de prueba de la recepción o del mantenimiento. Cuando un componente no pueda hacerlo, la medida compensatoria documentada sirve como evidencia, por ejemplo no compartir el dispositivo entre distintos roles. Exigido desde SL 3 en adelante, no desde SL 1, porque esta es una mejora de requisito.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 4.3 **Allí donde se usa criptografía, los algoritmos, longitudes de clave y manejo de claves siguen las buenas prácticas reconocidas, y se define cómo se generan, distribuyen, almacenan, rotan y revocan las claves.** Documento

Cómo se demuestra: Una visión general de los mecanismos usados por sistema, indicando algoritmo, longitud de clave y periodo de validez, más las reglas de gestión de claves y registros de rotaciones de claves y renovaciones de certificados. Las recomendaciones públicas sirven como referencia, por ejemplo las guías técnicas de la BSI alemana. Una operación pequeña mantiene una lista de certificados con fechas de caducidad y un recordatorio >= 30 días antes del vencimiento. Exigido desde SL 1 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9 FR 5: Flujo de datos restringido, zonas y conductos 11

SR 5.1 **El sistema de control puede dividirse en zonas separadas, y el tráfico entre esas zonas pasa únicamente por conductos definidos. La división sigue una lógica explicable, por ejemplo según la necesidad de protección, la propiedad o la función de las secciones de planta implicadas.** Documento

Cómo se demuestra: Diagrama de red que muestre las zonas y los conductos entre ellas, una lista de zonas con la lógica de cada frontera, y la configuración de los componentes de separación tales como definiciones de VLAN o interfaces de cortafuegos. Una operación pequeña se conforma con un esquema de una sola página que muestre oficina, red de máquina y acceso remoto como tres cuadros con los enlaces entre ellos, más una captura de pantalla de la configuración de VLAN del switch.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.1 RE 1 **La separación de zonas se implementa físicamente, es decir mediante componentes de red dedicados y cableado dedicado, y no descansa únicamente en la configuración lógica dentro de dispositivos compartidos. Apartado 9.1 de esta lista, exigido desde SL 2 en adelante. Las mejoras de requisito de esta norma nunca son obligatorias ya en SL 1.**

Cómo se demuestra: Inventario de componentes de red que indique qué switch o enrutador sirve a qué zona, fotos o plano de armario de las distribuciones separadas, etiquetado de cables. Las operaciones pequeñas demuestran esto con dos switches separados, claramente etiquetados, en lugar de un único dispositivo compartido y una foto del armario de control en la documentación de la planta.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.1 RE 2 **La red de automatización puede operar de forma independiente de las redes ajenas a la automatización. Si la informática de oficina o un enlace externo falla, el control y la monitorización de la planta siguen funcionando. Exigido desde SL 3 en adelante.**

Cómo se demuestra: Lista de dependencias de los servicios usados dentro de la red de automatización tales como servidor horario, resolución de nombres, servicio de directorio o servidor de licencias, indicando dónde se aloja cada uno, junto con un registro de prueba de un ensayo de desconexión en el que se retiró el enlace con la informática de oficina. Una operación pequeña anota el resultado de dicho ensayo en el registro de mantenimiento: enlace ascendente retirado, la planta siguió funcionando, solo faltaron los informes de oficina.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.1 RE 3 **Las zonas que albergan funciones especialmente críticas, por ejemplo funciones de seguridad o de protección, están separadas del resto de las zonas tanto lógica como físicamente. Exigido desde SL 4 en adelante.**

Cómo se demuestra: Marcado de las zonas críticas en el diagrama de zonas con la justificación de la clasificación, evidencia de componentes de red dedicados y cableado dedicado para esas zonas, configuración de los conductos con evidencia de que no existe ninguna ruta compartida.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.2 **En las fronteras de zona, el tráfico se controla, se monitoriza y se permite o deniega según reglas definidas. No existe ninguna ruta entre dos zonas que eluda este punto de control.**

Cómo se demuestra: Conjunto de reglas exportado del cortafuegos o del dispositivo de frontera, registros de conexiones denegadas y permitidas, evidencia de que no existen rutas laterales, por ejemplo mediante una comprobación de tarjetas de red adicionales, módems o enrutadores de telefonía móvil en los ordenadores de planta. Una operación pequeña demuestra esto con la exportación de reglas de su único cortafuegos y una breve nota de recorrido que confirme que no hay ningún enrutador no planificado en ningún armario de control.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.2 RE 1 **El conjunto de reglas en la frontera de zona funciona según el principio de que todo está denegado a menos que se haya permitido de forma explícita. Cada regla de permiso está justificada individualmente y vinculada a un propósito. Exigido desde SL 2 en adelante.**

Cómo se demuestra: Conjunto de reglas con una regla final visible que descarta el resto, y una lista de permisos que indique origen, destino, servicio, propósito y persona responsable para cada regla. Las operaciones pequeñas mantienen esta lista como una tabla de cinco columnas junto a la exportación del cortafuegos y la revisan una vez al año en busca de reglas que ya nadie necesita.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.2 RE 2 **La red de automatización puede aislarse deliberadamente de todas las conexiones externas y mantenerse funcionando en modo isla. La acción puede activarse sin tener que detener la planta. Exigido desde SL 3 en adelante.**

Cómo se demuestra: Descripción del procedimiento de aislamiento que indique quién puede activarlo y cómo, evidencia de la implementación técnica tal como un conjunto de reglas de emergencia o un interruptor de aislamiento etiquetado, más el registro de un simulacro en el que el aislamiento se ejercitó realmente. Una operación pequeña realiza el simulacro una vez al año durante el mantenimiento y anota fecha, duración y cualquier incidencia.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.2 RE 3 **Si el dispositivo en la frontera de zona falla o pierde sus reglas, deniega el tráfico en lugar de dejarlo pasar. Un fallo no debe dejar tras de sí una conexión abierta. Exigido desde SL 4 en adelante.**

Cómo se demuestra: Declaración del proveedor o evidencia de configuración sobre cómo se comporta el componente en caso de fallo y al reiniciar, registro de prueba de un fallo provocado deliberadamente con el resultado observado, alineación con la evaluación de riesgos de la planta, porque una frontera que deniega el tráfico puede tener consecuencias propias según el proceso.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.3 **Los servicios generales de comunicación de persona a persona tales como correo electrónico, mensajería o videollamadas pueden impedirse en los dispositivos de automatización y dentro de las redes de automatización. El alcance del bloqueo está definido y justificado.**

Cómo se demuestra: Definición de qué servicios no están permitidos en la red de automatización, más la implementación técnica: puertos y destinos bloqueados en el conjunto de reglas, aplicaciones eliminadas o bloqueadas en los puestos de operador, evidencia del inventario de software de los dispositivos. Una operación pequeña resuelve esto con un bloqueo de aplicaciones en la estación HMI y una regla que deniega el tráfico de correo y web saliente desde la red de máquina.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.3 RE 1 **Dichos servicios de comunicación de persona a persona se impiden en toda la red de automatización, y no simplemente se restringen en parte ni se limitan a dispositivos individuales. Exigido desde SL 2 en adelante.**

Cómo se demuestra: Evidencia de que el bloqueo se aplica a todos los dispositivos de la zona, por ejemplo mediante una revisión del software instalado en cada ordenador de la zona y una prueba de conexión desde un ordenador de planta cualquiera. Las operaciones pequeñas demuestran esto con una lista de dispositivos en la que cada fila está marcada con la fecha de comprobación, y una captura de pantalla del intento de conexión fallido.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 5.4 **Los datos y funciones de aplicación están compartimentados de forma que los procesos con distintas necesidades de protección o distintos privilegios no puedan acceder a las mismas áreas. La separación está integrada en la arquitectura del sistema y no queda al azar de la instalación.**

Cómo se demuestra: Visión general de las aplicaciones que indique qué datos y servicios usan y qué cuentas hay detrás de ellas, configuración de instancias, bases de datos, directorios o máquinas virtuales separadas, y una lista de privilegios por área. Una operación pequeña resuelve esto con cuentas de usuario separadas y carpetas de datos separadas para ingeniería y operación, más una nota sobre qué aplicación accede a qué carpeta.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

10 FR 6: Respuesta oportuna a los eventos 3

SR 6.1 **Los registros de auditoría recopilados en el sistema pueden ser leídos y evaluados por las personas y roles autorizados para ello sin perturbar la operación en curso de la planta, y el acceso a esos registros está a su vez restringido a usuarios autorizados.**

Cómo se demuestra: Una matriz de roles y permisos que muestre quién puede ver los datos de registro, más una captura de pantalla o exportación de una vista de registro que se haya obtenido realmente, con una marca de tiempo. Añadir una breve nota sobre la vía usada para la obtención, por ejemplo la interfaz de operador del controlador, un servidor de registro o una exportación de archivo. Las operaciones pequeñas se conforman con una visión general de una página por planta: dónde está el registro, quién tiene acceso de lectura, cómo se obtiene. Una extracción de prueba una vez al año, registrada en el diario de mantenimiento, demuestra que la vía funciona. Aplica desde SL 1 en adelante para todos los niveles de seguridad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 6.1 RE 1 **Los registros de auditoría pueden obtenerse a través de una interfaz automática de modo que las herramientas de análisis puedan procesarlos sin necesidad de una nueva transcripción manual, y los datos se proporcionan en un formato documentado y de uso común.**

Cómo se demuestra: Una descripción de la interfaz en uso junto con el formato, por ejemplo syslog, OPC UA Alarms and Conditions, una consulta REST o una exportación CSV, más un registro de muestra y la configuración del sistema receptor. La evidencia puede ser un extracto de la configuración del SIEM o del recolector de registros junto con la prueba de los registros entrantes. Sin un SIEM, basta con un recolector de registros en un servidor sencillo que obtiene los registros por la noche mediante un script y los almacena; el propio script más un listado de directorio de los archivos recopilados es la evidencia. Como mejora, esto solo se exige desde SL 3 en adelante, no desde SL 1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 6.2 **La actividad relevante para la seguridad en el sistema se monitoriza de forma continua, la monitorización detecta intentos de ataque y usos indebidos y los notifica con prontitud a un punto de contacto identificado, y se definen las herramientas, vías de notificación y responsabilidades usadas para ello.**

Cómo se demuestra: Una visión general de las herramientas de monitorización por zona, por ejemplo un sensor de red, alertas de antivirus, alarmas de cortafuegos o comprobación de integridad, indicando quién recibe la alerta y en qué plazo se espera una respuesta. Configuraciones de alarma, una lista de alertas generadas en los últimos meses y las notas de tratamiento correspondientes sirven como evidencia. Las operaciones pequeñas no necesitan una sala de control las 24 horas: un buzón compartido o una bandeja de tickets que agrupe las alertas de los sistemas existentes, más una regla fija de que una persona identificada la revisa cada día laborable, es suficiente y se demuestra mediante el historial del buzón. Exigido desde SL 2 en adelante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

11 FR 7: Disponibilidad de recursos 13

SR 7.1 **Ante sobrecarga o ataques de inundación deliberados, el sistema permanece en un estado de operación definido, las funciones de control esenciales siguen funcionando, y el fallo de un servicio individual no arrastra consigo a toda la planta.**

Cómo se demuestra: Configuración de los mecanismos de protección (limitación de tasa, límites de conexión, control de tormentas de difusión en los switches), declaraciones del proveedor sobre el comportamiento bajo carga, más un registro de una prueba de carga o de un evento de sobrecarga real con observación de la función de control. Exigido desde SL 1. Una operación pequeña cubre esto con capturas de pantalla de los ajustes del switch y del cortafuegos y una breve nota sobre qué función siguió funcionando durante una prueba de la célula más importante.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.1 RE 1 **La carga de comunicación que los componentes individuales pueden inyectar en la red está limitada, de modo que un componente defectuoso o comprometido no pueda inundar el segmento de red.**

Cómo se demuestra: Límites de ancho de banda y multicast por puerto en los componentes de red, evidencia del límite para cada conexión, más una medición de la carga base real por dispositivo. Exigido desde SL 2, no desde SL 1. Sin switches gestionados esta línea no puede demostrarse, y ese es entonces el punto abierto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.1 RE 2 **Una situación de sobrecarga dentro del sistema considerado no se propaga a sistemas o redes adyacentes; el impacto hacia el exterior está técnicamente contenido.**

Cómo se demuestra: Reglas de segmentación y filtrado en las fronteras, evidencia de que el tráfico saliente está limitado, más un registro de prueba que muestre que una carga generada en la red de célula no degradó la red de oficina ni una red vecina. Exigido desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.2 **El uso de tiempo de procesamiento, memoria, espacio de almacenamiento y ancho de banda de red está acotado de forma que un único proceso o servicio no pueda consumir los recursos necesarios para el control.**

Cómo se demuestra: Configuración de los límites de recursos (cuotas, prioridades de proceso, límites de memoria), evaluación de la monitorización de utilización durante un periodo representativo, más los umbrales a partir de los cuales se emite una advertencia. Exigido desde SL 1. Las operaciones pequeñas usan los medios integrados del sistema operativo y una monitorización sencilla con una alerta de espacio en disco y CPU por correo electrónico.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.3 **Existen copias de seguridad de las configuraciones del sistema, los datos de aplicación y las versiones de programa; pueden generarse sin interrumpir la operación en curso y están protegidas contra el acceso y la modificación no autorizados.** Documento

Cómo se demuestra: Concepto de copia de seguridad que cubra alcance, frecuencia y periodo de retención, registros de copia de seguridad de las ejecuciones más recientes, más evidencia de la protección de acceso de los soportes de copia de seguridad (almacenamiento separado, cifrado, permisos dedicados). Exigido desde SL 1. Una operación pequeña respalda los proyectos del PLC y las versiones del HMI en un soporte cifrado que se desconecta físicamente tras la copia, y registra fecha y versión en una lista sencilla.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.3 RE 1 **Se ha verificado la utilidad de las copias de seguridad; se demuestra que a partir de ellas realmente puede restaurarse un estado funcional.**

Cómo se demuestra: Registro de un ensayo de restauración con fecha, versión de copia de seguridad probada, sistema de destino y resultado, al menos para los componentes críticos. Exigido desde SL 2, no desde SL 1. Las operaciones pequeñas comprueban una vez al año, como muestra, un programa de PLC y una imagen de HMI en un dispositivo de repuesto y registran el resultado en dos frases.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.3 RE 2 **La copia de seguridad se ejecuta automáticamente según un calendario definido; una ejecución fallida se detecta y se notifica.**

Cómo se demuestra: Calendario del trabajo de copia de seguridad, registros de ejecución sin lagunas, más evidencia de la notificación de fallo para una ejecución que no tuvo éxito (alarma, ticket, correo). Exigido desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.4 **Tras una perturbación, fallo o ataque, el sistema puede devolverse a un estado conocido y seguro; la recuperación se ha ensayado y las responsabilidades están identificadas.** Documento

Cómo se demuestra: Plan de reinicio para cada componente crítico con secuencia, soportes necesarios, contactos y tiempo objetivo, junto con el registro del último ejercicio de recuperación. Exigido desde SL 1. Una operación pequeña se conforma con una ficha de reinicio de una página por línea, guardada en el armario de control y comprobada cada vez que se sustituye una pieza de repuesto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.5 **Si falla el suministro eléctrico regular, el sistema pasa a un estado definido: o bien el suministro se mantiene mediante una fuente de respaldo o tiene lugar un apagado ordenado sin pérdida del estado seguro.**

Cómo se demuestra: Evidencia de dimensionamiento y mantenimiento del sistema de alimentación ininterrumpida o del generador de emergencia, registro de prueba de la última prueba de batería o de carga, más una descripción del comportamiento en la conmutación y en el restablecimiento de la red eléctrica. Exigido desde SL 1. Las operaciones pequeñas prueban el SAI bajo carga una vez al año y registran fecha de prueba, tiempo de autonomía y antigüedad de la batería.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.6 **Los ajustes de red y de seguridad del sistema están fijados a un estado objetivo aprobado, las desviaciones de ese estado objetivo son detectables, y el estado actual puede consultarse en cualquier momento.** Documento

Cómo se demuestra: Configuración objetivo aprobada por clase de dispositivo (especificación de bastionado), estados de configuración actuales de los dispositivos, más el resultado de una comparación entre estado objetivo y estado real con una lista de desviaciones y el motivo de cada una. Exigido desde SL 1. Una operación pequeña guarda las exportaciones de configuración bajo control de versiones y compara antes y después de cada cambio.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.6 RE 1 **El estado actual de los ajustes de seguridad puede exportarse en forma legible por máquina de modo que pueda comprobarse automáticamente frente al estado objetivo.**

Cómo se demuestra: Salida de muestra en un formato legible por máquina (exportación de configuración, archivo estructurado, consulta por interfaz) y el script o herramienta que realiza la comparación frente al estado objetivo, junto con el informe de resultado de una ejecución. Exigido desde SL 3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.7 **El sistema está restringido a las funciones necesarias para la operación; los servicios, puertos, protocolos e interfaces que no se necesitan están deshabilitados o eliminados.**

Cómo se demuestra: Lista de servicios activos y puertos abiertos por componente con una justificación de la necesidad, evidencia de que el resto están deshabilitados (configuración, resultado de escaneo de puertos), más una regla para las interfaces USB y de mantenimiento. Exigido desde SL 1. Las operaciones pequeñas realizan un escaneo de puertos sencillo por segmento y justifican cada elemento abierto en una línea.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR 7.8 **Se dispone de un inventario actualizado de todos los componentes del sistema con fabricante, tipo, versión de firmware o software y dirección de red, y se mantiene actualizado cuando se producen cambios.** Documento

Cómo se demuestra: Inventario de componentes con su fecha de revisión y propietario, evidencia de mantenimiento a través del historial de cambios, más una comparación frente a un descubrimiento de red para encontrar dispositivos no registrados. Exigido desde SL 2, no desde SL 1. Una operación pequeña mantiene el inventario como una tabla y lo actualiza como regla fija cada vez que se sustituye un dispositivo y cada vez que se actualiza el firmware.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación