Requisitos de seguridad para sistemas de control de edificios

Condiciones para proveedores y conexiones locales y remotas

Versión 10 | 11 de noviembre de 2026

1 Objeto y alcance

Este documento establece los requisitos de seguridad para los sistemas de control de cada edificio de Nasuvinsa, funcionen de forma autónoma o conectada. Se aplica al suministro, instalación, puesta en servicio, mantenimiento y retirada, con independencia de que exista conexión a Internet o a una plataforma IoT. Su finalidad principal es proteger el control local y el funcionamiento seguro de las instalaciones.

Comprende PLC, sondas y otros sensores, actuadores, sistemas de detección y alarma de inundación, controladores y sistemas de gestión del edificio, además de sus redes, pasarelas, aplicaciones e interfaces de administración. Incluye las herramientas de mantenimiento y, cuando se autoricen, los portales, nubes y servicios externos de fabricantes o terceros.

Toda conexión remota estará prohibida y deshabilitada por defecto, tanto entrante como saliente, incluida la consulta o telemetría. Solo podrá habilitarse mediante autorización expresa, previa y documentada de Nasuvinsa, con alcance, vigencia y condiciones de seguridad definidos. La disponibilidad de un portal del fabricante o de una función de soporte no autoriza su uso.

Se considera remota cualquier conexión desde o hacia equipos, redes o servicios fuera del entorno de control autorizado del edificio, aunque se origine en el propio inmueble. Los flujos locales necesarios deberán documentarse y autorizarse. La integración con la plataforma IoT es opcional y está sujeta a las mismas condiciones de autorización.

2 Responsabilidades

Función	Responsabilidad mínima
Nasuvinsa	Define alcance y criticidad, aprueba la arquitectura y las conexiones remotas y autoriza la puesta en servicio de cada sistema local.
Operador de plataforma	Cuando haya integración autorizada, aplica aislamiento, identidades, permisos y validación de datos y órdenes en su plataforma.
Fabricante	Declara capacidades y limitaciones del producto, versiones, vulnerabilidades conocidas y condiciones y duración del soporte.
Integrador	Configura el sistema local con conexiones remotas deshabilitadas por defecto y entrega documentación, pruebas y evidencias.
Mantenedor	Ejecuta las tareas de vigilancia, actualización, copia, recuperación y respuesta que le asigne el contrato.

Cada obligación tendrá un responsable identificado. Los anexos A, B y C se completarán y aprobarán antes de la puesta en servicio, también en edificios sin plataforma. La autorización de una conexión remota no sustituye la aceptación de seguridad del sistema.

3 Arquitectura y control de acceso

R01 Inventario y criticidad. El integrador entregará un inventario con identificador, ubicación, función, fabricante, modelo, versión, interfaces, responsable y fin de soporte de cada activo. Incluirá PLC, sondas, detección de inundación, portales de administración, radios, módems y tarjetas SIM cuando existan. Lo vinculará al diagrama de red y a los servicios del edificio, identificando las consecuencias sobre personas, equipos y servicios.

R02 Segmentación y filtrado. Se separarán las redes de control de las redes de usuarios, invitados, administración y terceros, según el análisis de riesgos. Se denegarán por defecto las comunicaciones entrantes y salientes y solo se permitirán los flujos documentados y autorizados. El filtrado deberá existir en la infraestructura de red aunque el controlador no disponga de firewall. La ausencia de conexión a una plataforma no exime de estas medidas.

R03 Prohibición por defecto de conexiones remotas. Quedarán deshabilitados los portales remotos, servicios cloud, telemetría del fabricante, túneles y herramientas de acceso a PLC, sondas, sistemas de inundación y demás equipos. La prohibición incluye conexiones iniciadas desde el edificio, VPN, retransmisores, módems móviles y vías alternativas a la red principal. Se impedirán aperturas automáticas de puertos y la reactivación de accesos no autorizados tras reinicios o actualizaciones. Ninguna conexión se habilitará sin la autorización de R32; el cifrado o una IP permitida no sustituyen esa autorización.

R04 Administración y mantenimiento. Las interfaces locales se limitarán a personal, puestos y funciones autorizados. El mantenimiento remoto será excepcional y requerirá autorización previa, cuentas nominales, MFA y un punto de acceso controlado. Se habilitará solo durante la ventana aprobada y se cerrará al finalizar. Se registrarán las sesiones y se permitirá su revocación sin afectar al control local. No se admitirán cuentas compartidas de uso ordinario ni accesos permanentes reservados al proveedor.

R05 Identidad de equipos y servicios. Los activos locales estarán identificados individualmente. Cada equipo, pasarela o servicio que admita autenticación utilizará una identidad propia y revocable. Para los equipos que carezcan de ella se aprobarán controles compensatorios de red, acceso físico y pasarela cuando corresponda. No se compartirán credenciales entre edificios. Se definirán altas, sustituciones y bajas, exista o no plataforma.

R06 Autorización y mínimo privilegio. Los sistemas locales, interfaces de administración, pasarelas y plataformas que existan verificarán los permisos por edificio, activo y operación. Se separarán consulta, configuración y actuación. Una cuenta de lectura no podrá enviar órdenes ni modificar consignas. La aceptación de una dirección IP o de un certificado no otorgará acceso general. Las autorizaciones remotas se limitarán a los recursos expresamente aprobados.

R07 Gestión de credenciales. Se eliminarán las contraseñas de fábrica y se custodiarán los secretos fuera del código, los registros y la documentación compartida. Se definirán renovación, revocación y alertas de caducidad de certificados y claves. Para cuentas humanas se priorizarán contraseñas largas y bloqueo de valores comprometidos; el cambio será obligatorio ante compromiso. Se limitarán los intentos de autenticación según las condiciones operativas aprobadas. Los accesos de emergencia tendrán custodia, uso registrado y revisión posterior.

R08 Configuración y protección de equipos. Se deshabilitarán servicios, cuentas, interfaces y funciones innecesarias, incluidas las funciones remotas instaladas por defecto. Se protegerán armarios, puertos de programación y soportes. No se conectarán routers, puntos de acceso, módems ni equipos que creen puentes con redes externas sin autorización. Se conservará la configuración aprobada y se comprobará tras cambios o reinicios. Un sistema operativo cerrado no acredita por sí mismo el cumplimiento.

4 Comunicaciones locales e integraciones autorizadas

R09 Protección de las comunicaciones. Las comunicaciones IP de administración e integración, locales o remotas autorizadas, utilizarán TLS 1.2 o superior o un mecanismo equivalente aprobado para el protocolo. Se preferirá TLS 1.3 en nuevas integraciones compatibles. Se verificarán identidades y certificados sin desactivar validaciones. La autenticación de equipos empleará TLS mutuo o una alternativa aprobada. Los protocolos de campo sin estas capacidades se tratarán conforme a R10.

R10 Protocolos y equipos heredados. Cuando un tramo de campo no permita cifrado o autenticación adecuados, se identificarán los activos y flujos y se aprobarán medidas compensatorias, como aislamiento, filtrado y protección física. Se documentará el riesgo residual, también en instalaciones autónomas. Un canal cifrado hasta una pasarela no protege automáticamente el tramo de campo. Las limitaciones del equipo no justifican habilitar acceso remoto.

R11 Especificación de las interfaces. El anexo A recogerá las interfaces locales y las remotas autorizadas, su protocolo, versión, dirección, esquema y autenticación. Se entregarán mapas de señales y contratos de API o mensajería cuando existan. Se definirán compatibilidad, aviso de cambios y errores. En MQTT se documentarán los temas, permisos y reglas de retención y entrega. En sistemas autónomos se declarará expresamente la ausencia de conexiones remotas autorizadas.

R12 Calidad y validación de los datos. Cada señal tendrá identificador, origen, unidad, tipo y significado. Se definirán calidad, frecuencia, marcas de tiempo y antigüedad admisible según su función. El sistema receptor, sea controlador local o plataforma, validará formatos, rangos y procedencia. Los datos ausentes, inválidos o antiguos se distinguirán de un valor válido y no activarán automatismos fuera de las reglas aprobadas.

R13 Envío y ejecución de órdenes. Las órdenes intercambiadas entre sistemas tendrán un destino inequívoco, permisos específicos, correlación y vigencia. Se validarán rango, frecuencia, duplicados y caducidad. Se diferenciarán recepción, ejecución y confirmación del estado. La aplicación evitará actuaciones adicionales por reintentos y rechazará órdenes caducadas, también tras una reconexión. Las consignas y cambios locales estarán sujetos a los permisos y límites aprobados.

R14 Prioridad y límites de actuación. Se documentará la prioridad entre automatismos locales, intervención manual y órdenes externas autorizadas. Las protecciones locales permanecerán activas. Las actuaciones sobre sistemas de protección de personas o funciones críticas requerirán análisis y autorización específicos. Se podrá bloquear el control remoto conservando el funcionamiento local previsto. La autorización de consulta no habilitará actuaciones.

R15 Capacidad y recuperación de comunicaciones. Se acordarán frecuencias, límites de mensajes, tiempos de espera, reintentos y almacenamiento según las interfaces existentes. La recuperación evitará saturar redes, controladores o plataformas y conservará la calidad y antigüedad de los datos. Los fallos de sincronización horaria se tratarán cuando afecten a registros, certificados u órdenes. Estas condiciones se aplican también a comunicaciones entre equipos del propio edificio.

Integración opcional con la plataforma IoT “Plataforma Nasuvinsa”

Cuando se autorice esta integración, se utilizará preferentemente una pasarela con comunicaciones salientes autenticadas, aislamiento por edificio y permisos separados de lectura y actuación. No se expondrán directamente controladores o interfaces de campo a Internet. La conexión no habilitará portales del fabricante ni otros accesos remotos.

Los detalles de direcciones, puertos, certificados, señales y límites se mantendrán en anexos controlados por versión. La documentación de integración no contendrá contraseñas, claves privadas ni otros secretos.

5 Soporte y operación de seguridad

R16 Vigencia del soporte. El proveedor declarará el periodo de soporte de hardware, firmware, software y conectores, sus condiciones y el preaviso de fin de soporte. Se acordará un plan de sustitución o una excepción antes de mantener activos sin soporte. El contrato identificará quién recibe los avisos del fabricante y quién evalúa su efecto en cada instalación.

R17 Componentes y vulnerabilidades. Se entregará un inventario de componentes y dependencias con sus versiones. Para nuevos suministros y desarrollos propios incluirá una lista de materiales de software o SBOM; su ausencia requerirá una excepción aprobada con evidencia alternativa. El desarrollo propio incorporará revisión de código, análisis de dependencias y pruebas de seguridad. El proveedor mantendrá un canal de comunicación de vulnerabilidades y declarará las conocidas que afecten a la solución.

R18 Actualizaciones seguras. Se establecerán plazos de evaluación, mitigación y corrección por severidad, exposición y efecto operativo en el anexo C. Se verificará la autenticidad e integridad de las actualizaciones y se emplearán firmas cuando el producto las soporte. Los cambios se probarán antes de su despliegue, con copia y recuperación previstas. Si no existe parche o no puede aplicarse, se aprobará una mitigación y una fecha de revisión.

R19 Control de cambios. Los cambios de firmware, lógica, red, permisos o consignas protegidas requerirán registro, evaluación de impacto y autorización según su criticidad. Se conservarán versiones y pruebas. Los cambios urgentes tendrán validación posterior. Tras un cambio se comprobará que no se reactivan conexiones remotas no autorizadas. Toda nueva conexión externa requerirá autorización previa y actualización de los anexos A y C; documentarla después no regulariza su habilitación.

R20 Registros y trazabilidad. Se registrarán accesos y fallos de autenticación, altas y bajas, cambios de permisos, configuración y software, órdenes relevantes y alertas. Cada registro identificará fecha, origen, actor o servicio, activo, acción y resultado; en cambios de consignas, también los valores anterior y nuevo cuando proceda. Los registros se protegerán frente a alteración y acceso indebido y estarán disponibles para investigación durante el plazo acordado.

R21 Supervisión y alertas. Se definirán responsables, cobertura y reglas de detección de accesos anómalos, intentos de conexión remota, cambios no autorizados, pérdida de comunicación y fallos de copia o credenciales. La supervisión podrá ser local; no exige conectar con una plataforma. Se distinguirán alertas de seguridad y alarmas operativas. Se probarán generación, entrega y escalado, incluidos los fallos del canal habitual. Todo canal externo de notificación deberá autorizarse.

R22 Respuesta a incidentes. El anexo C fijará canales, contactos, severidades y plazos desde la detección de indicios razonables, sin esperar a completar la investigación. El aviso describirá lo conocido, los activos afectados y las primeras medidas. Se conservarán evidencias y se coordinarán contención, recuperación y comunicación con Nasuvinsa. Las actuaciones sobre la instalación respetarán las condiciones de seguridad y continuidad acordadas.

R23 Evaluación y pruebas seguras. Se revisarán riesgos y vulnerabilidades con la periodicidad acordada y ante cambios relevantes. Los escaneos, pruebas de intrusión y ensayos potencialmente disruptivos tendrán alcance y autorización previos. Se realizarán en un entorno de prueba o bajo condiciones operativas aprobadas, con supervisión y recuperación previstas. Se evitarán pruebas no coordinadas sobre controladores en servicio.

6 Continuidad y ciclo de vida

R24 Autonomía y continuidad local. Las funciones de control, detección y alarma previstas en el proyecto, incluidas las de inundación, deberán funcionar localmente sin depender de portales remotos o de la plataforma IoT. Se probarán pérdida de comunicaciones, bloqueo de conexiones externas, fallo de controlador, corte eléctrico y datos inválidos según el alcance. Se definirán estado seguro, autonomía e intervención manual. La reconexión no reactivará órdenes antiguas ni anulará protecciones.

R25 Copias de seguridad. Durante toda la explotación se mantendrán copias de programas y proyectos de PLC, configuraciones, mapas de señales, conectores y datos necesarios para restablecer el servicio. Se realizarán también antes y después de cambios relevantes. Se protegerán frente a acceso, modificación y pérdida simultánea con el sistema original. Los secretos incluidos tendrán custodia y recuperación específicas. Se vigilará el resultado de las copias.

R26 Recuperación verificable. Se fijarán por servicio el tiempo objetivo de recuperación o RTO y la pérdida máxima de datos admisible o RPO, junto con repuestos, herramientas, licencias y dependencias. Se ejecutará una prueba de restauración antes de la aceptación y con la periodicidad acordada. La prueba incluirá comprobaciones funcionales de la instalación y confirmará que puede recuperarse sin depender de una única persona.

R27 Terceros y cadena de suministro. Se identificarán fabricantes, subcontratistas y servicios que accedan a equipos o datos o condicionen el servicio. Se trasladarán las obligaciones de acceso, confidencialidad, soporte e incidentes a sus acuerdos. La garantía o el mantenimiento no habilitan conexiones remotas por sí mismos. El proveedor declarará dependencias de portales o nubes antes del suministro. Cualquier cambio de acceso o dependencia requerirá aprobación previa. Las certificaciones identificarán entidad, producto, versión y alcance cubierto.

R28 Entrega y reversibilidad. La entrega incluirá documentación de la instalación, proyectos y configuraciones editables, mapas de señales, interfaces y procedimientos de mantenimiento y recuperación. Se acordarán los derechos de uso y los medios necesarios para que un mantenedor autorizado pueda continuar el servicio. Los datos se podrán exportar en un formato documentado. Las restricciones de licencias y dependencias propietarias se declararán antes de la contratación.

R29 Protección y uso de los datos. Se identificarán los datos recogidos, su finalidad, destinatarios, ubicación, conservación y medidas de protección. Se limitarán los accesos y el uso a lo autorizado. La información sensible almacenada y sus copias se protegerán mediante cifrado y control de acceso según su clasificación. Cuando haya datos personales, se determinarán los roles y las obligaciones contractuales aplicables, incluidos los subencargados cuando proceda. Se considerarán los datos de accesos, ocupación o consumos cuando permitan identificar o vincular información a personas.

R30 Retirada y cambio de proveedor. La baja incluirá revocación de cuentas, certificados y accesos remotos, retirada de rutas y reglas innecesarias, entrega de documentación actualizada y devolución o eliminación de datos según las obligaciones de conservación. Se sanearán los equipos y soportes retirados. Se verificará la continuidad del servicio durante la transición y se conservará evidencia de las acciones realizadas.

La exigencia de soporte y recuperación se aplicará a la solución completa. Las limitaciones de un fabricante, una licencia o un componente se identificarán antes de la aceptación y tendrán un tratamiento aprobado.

7 Cumplimiento y aceptación

R31 Aceptación y puesta en servicio. El integrador entregará los anexos, evidencias de configuración y pruebas del anexo B, también para sistemas autónomos. Cada requisito se marcará conforme, no conforme o no aplicable justificado. Las no conformidades requerirán corrección o excepción vigente aprobada. Nasuvinsa y el responsable de operación aceptarán el sistema antes de su uso; el operador de plataforma participará cuando exista integración. Se comprobará el bloqueo efectivo de conexiones remotas no autorizadas.

R32 Autorizaciones remotas y excepciones. Toda conexión remota requiere autorización previa y expresa de Nasuvinsa. El anexo C justificará necesidad, alternativas locales, activos, flujos, usuarios, permisos, vigencia, revisión y revocación. El mantenimiento se limitará a ventanas; los servicios persistentes requerirán aprobación específica. Una excepción de seguridad identificará requisito incumplido, medidas compensatorias y riesgo residual. Autorizar una conexión no exime de otros requisitos. Ninguna excepción podrá dispensar obligaciones legales ni condiciones de seguridad de las personas.

R33 Aplicabilidad normativa. Se determinará y documentará la normativa aplicable al sistema y al servicio contratado, incluido el ENS y su categoría cuando corresponda y las obligaciones de protección de datos personales. Las declaraciones o certificaciones exigidas deberán cubrir el alcance pertinente. Las referencias técnicas de este documento son apoyo para la especificación; no acreditan por sí solas la conformidad del producto o del servicio.

R34 Revisión y aplicabilidad. Nasuvinsa designará al responsable de mantener el documento y aprobar sus revisiones. Los anexos identificarán edificio, versión y fecha y se revisarán ante cambios de arquitectura, proveedor, acceso o criticidad. La ausencia de plataforma no permite declarar no aplicables los controles del edificio ni la prohibición remota. Solo se excluirán funciones inexistentes con justificación; las limitaciones técnicas requerirán una excepción.

7 1 Hitos y evidencias

Hito	Entrega necesaria	Validación
Diseño	Inventario local, criticidad, arquitectura y anexo A. Accesos remotos previstos o ausencia de ellos.	Nasuvinsa y operación local; plataforma solo si hay integración.
Puesta en servicio	Configuración, pruebas del anexo B y anexo C. Bloqueo remoto verificado y autorizaciones vigentes.	Aceptación antes de poner en servicio, también sin plataforma.
Explotación	Registros de cambios, revisiones, actualizaciones, copias, restauraciones e incidentes.	Responsables y periodicidad definidos en el contrato.
Cambio o retirada	Entrega actualizada, transferencia de la administración, revocación y tratamiento de datos.	Comprobación del cierre y de la continuidad del servicio.

7 2 Uso de los anexos

El anexo A describe el sistema local y sus conexiones autorizadas; el B registra las pruebas; el C concreta la operación, las autorizaciones remotas y las excepciones. Deben completarse antes de la puesta en servicio. Si no existe conexión remota se indicará expresamente, manteniendo la comprobación del bloqueo. Los parámetros se acordarán según criticidad y las obligaciones legales aplicables.

En nuevas instalaciones se exigirá esta configuración desde el diseño. En instalaciones existentes se inventariarán los accesos activos y se acordará su cierre seguro o autorización antes de aceptarlas. Se evitará interrumpir funciones críticas durante la regularización. La mera existencia previa de un portal o conexión no constituye autorización.

Anexo A Ficha del sistema de control del edificio

Se cumplimentará una ficha por edificio, también si funciona de forma autónoma. Los diagramas, inventarios y mapas extensos podrán adjuntarse con versión y ubicación. Se indicará expresamente si no existen conexiones remotas autorizadas.

A1 Identificación y alcance

Edificio y sistemas de control incluidos. [Completar]

Proveedor e integrador y contactos técnicos. [Completar]

Mantenedor y responsable de operación local. [Completar]

Versión de la ficha y fecha de aprobación. [Completar]

Funciones y criticidad de los servicios incluidos. [Completar]

Modo autónomo o conexiones remotas autorizadas y su código. [Completar]

Inventario y diagrama de red de referencia. [Completar]

A2 Flujos y dependencias

Registrar los flujos locales necesarios y los remotos expresamente autorizados, incluidos portales, telemetría, módems y servicios auxiliares. Indicar la autorización en cada flujo remoto. Duplicar filas cuando sea necesario. No incluir secretos.

Origen y zona	Destino y zona	Protocolo y puerto	Sentido	Protección	Uso y autorización
[Completar]	[Completar]	[Completar]	[Completar]	[Completar]	[Completar]
[Completar]	[Completar]	[Completar]	[Completar]	[Completar]	[Completar]

A3 Datos y órdenes

Mapa de señales locales e interfaces de integración si existen. [Completar]

Identificadores, unidades, tiempos, calidad y antigüedad máxima de datos. [Completar]

Órdenes autorizadas, rangos, vigencia, duplicados y confirmación. [Completar]

Control y alarmas locales y respuesta ante fallos o bloqueo remoto. [Completar]

A4 Identidad y restricciones

Emisión, renovación, revocación y custodia de credenciales. [Completar]

Portales y accesos deshabilitados y autorizaciones o excepciones. [Completar]

Dependencias externas y plataforma IoT solo si se autoriza su uso. [Completar]

Anexo B Pruebas de aceptación

Registrar resultado, fecha, responsable y evidencia. Aplicar también a sistemas autónomos: el bloqueo remoto y las funciones locales siempre se verificarán. Usar apto, no apto o no aplicable justificado para funciones inexistentes. Las pruebas tendrán alcance y condiciones de seguridad autorizados.

ID	Requisitos	Criterio de aceptación	Resultado y evidencia
T01	R01 a R03 R08	Inventario y red coinciden. Se bloquean accesos entrantes y salientes no autorizados, incluidos nube del fabricante y vías móviles, también tras reinicios.	[Completar]
T02	R04 R06	La administración local está restringida. El mantenimiento remoto permanece deshabilitado; si se autoriza, exige cuenta nominal y MFA y se cierra al finalizar la ventana.	[Completar]
T03	R05 R06	Los permisos limitan consulta y actuación en equipos locales y, si existe, en la plataforma. No hay accesos indebidos entre edificios.	[Completar]
T04	R07 R09	Las credenciales inválidas se rechazan. Se verifica su revocación y, cuando existan, la validación y renovación de certificados.	[Completar]
T05	R10	Los tramos sin protección nativa están identificados y aislados. Las medidas compensatorias coinciden con las excepciones aprobadas.	[Completar]
T06	R11 R12	Datos malformados, ajenos, ausentes o antiguos reciben el tratamiento previsto. Se verifican unidades e identificadores de señales.	[Completar]
T07	R13 R14	Se rechazan órdenes no autorizadas, caducadas o fuera de rango. Los duplicados no repiten actuaciones y prevalecen las protecciones locales.	[Completar]
T08	R15 R24	El control y las alarmas locales, incluida inundación cuando forme parte del sistema, funcionan con conexiones remotas bloqueadas. La reconexión no ejecuta órdenes antiguas.	[Completar]
T09	R16 a R19	Se acredita soporte e inventario. Una actualización autorizada y su recuperación mantienen la configuración y no reactivan accesos remotos no autorizados.	[Completar]
T10	R20 a R23	Un evento de prueba genera registro y alerta local y activa el escalado. Un canal de aviso externo solo se usa si está autorizado.	[Completar]
T11	R25 R26	Se restaura una copia en un entorno acordado y se comprueba el servicio, con tiempos y pérdida de datos dentro de los objetivos.	[Completar]
T12	R27 a R30	La documentación y exportación permiten la transición. Se comprueban terceros, tratamiento de datos y el procedimiento de revocación y retirada.	[Completar]

Decisión de aceptación. [Completar: aceptado, pendiente de correcciones o sujeto a las excepciones vigentes identificadas].

Responsables y fecha. [Completar: integrador, operación local y Nasuvinsa; operador de plataforma solo si hay integración].

Anexo C Operación y autorizaciones

Acordar los parámetros por servicio y severidad, con inicio del plazo, cobertura, responsable y evidencia. El soporte contratado no autoriza acceso remoto. Las autorizaciones y excepciones deberán estar resueltas antes de poner en servicio el sistema.

C1 Parámetros de servicio

Parámetro que debe acordarse	Valor aprobado	Responsable
Severidades y cobertura de soporte. Contacto principal y alternativo, incluidos periodos no laborables cuando proceda.	[Completar]	[Completar]
Aviso de incidente desde la detección de indicios razonables. Canal, contenido mínimo y escalado.	[Completar]	[Completar]
Evaluación y contención de incidentes. Actualizaciones de estado e informe de cierre.	[Completar]	[Completar]
Evaluación de vulnerabilidades, mitigación y corrección por riesgo. Ventanas de cambio y excepciones temporales.	[Completar]	[Completar]
Conservación de registros, frecuencia de revisión y entrega de evidencias.	[Completar]	[Completar]
Frecuencia y retención de copias. RTO y RPO por servicio y frecuencia de pruebas de restauración.	[Completar]	[Completar]
Renovación y revocación de credenciales y sesiones. Duración de ventanas remotas y revisión de conexiones persistentes autorizadas.	[Completar]	[Completar]
Fin de soporte, preaviso y sustitución. Periodicidad de revisión de accesos, riesgos y documentación.	[Completar]	[Completar]

C2 Autorizaciones remotas y excepciones

Duplicar por conexión o excepción. Nasuvinsa deberá aprobar expresamente su necesidad, alcance y vigencia antes de habilitarla. Si no hay conexiones autorizadas, indicar ninguna. Autorizar una conexión no exime de otros controles.

Código, tipo de solicitud, equipos y edificio afectados. [Completar]

Necesidad, alternativas locales, flujos, destinos, usuarios y permisos. [Completar]

Controles, evidencias y riesgo residual o requisito incumplido. [Completar]

Responsable, ventana o vigencia, revisión y método de cierre. [Completar]

Decisión expresa de Nasuvinsa, aprobador, fecha y revocación. [Completar]

C3 Aprobación de la operación

Responsable del servicio y responsable de seguridad de Nasuvinsa. [Completar]

Mantenimiento, operación local y plataforma solo si existe. [Completar]

Referencias de los anexos aprobados y fecha de entrada en servicio. [Completar]

Referencias técnicas y normativas

Las referencias siguientes apoyan la selección y adaptación de requisitos. La adopción de una norma o certificación, sus partes, edición y alcance deberá indicarse expresamente en el contrato o en la documentación de aplicabilidad. No se presume la obligatoriedad de una referencia técnica por su inclusión en esta relación.

NIST SP 800-82 Rev. 3. Guide to Operational Technology Security. Referencia para arquitectura, acceso remoto, continuidad y particularidades de los sistemas de control. Se utiliza la revisión final 3; la revisión 4 se encuentra en fase de borrador en la fecha de este documento. Referencia oficial

NISTIR 8259A y 8259B. Capacidades técnicas de seguridad de dispositivos IoT y capacidades de apoyo del fabricante. El catálogo facilita concretar identificación, configuración, protección, actualización y soporte. Referencia oficial

NIST SP 800-63B-4. Digital Identity Guidelines. Authentication and Authenticator Management. Referencia para autenticación de personas y gestión de autenticadores. Referencia oficial

Serie ISA/IEC 62443. Seleccionar las partes pertinentes para propietarios, servicios de integración y mantenimiento, sistemas y productos. La parte 2-4 trata proveedores de servicios; las partes 4-1 y 4-2, desarrollo seguro y capacidades de componentes. Referencia oficial

CIS Controls v8.1. Referencia complementaria para configuración, cuentas, accesos, registros, recuperación, red y proveedores. Debe identificarse el control y la edición; la numeración de versiones anteriores no es intercambiable. Referencia oficial

ISO/IEC 27001:2022. Marco de gestión de seguridad de la información. Su uso requiere establecer el alcance y revisar las correspondencias de controles de la edición aplicada. Referencia oficial

ISO 22301:2019. Marco de gestión de continuidad del negocio. Se utilizará para concretar preparación, recuperación y revisión cuando resulte pertinente. Referencia oficial

Esquema Nacional de Seguridad. Real Decreto 311/2022. Determinar su aplicación al sistema y al servicio contratado, la categoría y las evidencias de conformidad exigibles conforme al alcance correspondiente. Referencia oficial

Reglamento General de Protección de Datos. Reglamento UE 2016/679. Determinar su aplicación cuando se traten datos personales y las obligaciones de responsables, encargados y subencargados. Referencia oficial

Antecedentes documentales. Versiones 08 y 09 de los requisitos de seguridad para proveedores. La versión 10 sitúa el control local de cada edificio en el centro del alcance y establece conexiones remotas prohibidas por defecto, con autorización expresa cuando proceda. La integración con la plataforma IoT es opcional.