Instrucciones de Seguridad para Proveedores de Dispositivos de Control accesibles por Internet en Edificios de NASUVINSA

Este documento establece las directrices de seguridad que deben seguir todos los proveedores de dispositivos de control instalados en edificios y accesibles por Internet. El objetivo es garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos.

En aquellos casos en que el sistema operativo del elemento de control sea muy restrictivo (por ejemplo, PLCs con sistema operativo cerrado y no generalista como el que desarrollan algunos fabricantes de hardware) la lista se cumplirá casi automáticamente. En aquellos casos en que el sistema operativo es abierto, el integrador deberá realizar un esfuerzo adicional con el objetivo de cumplir con los requisitos de seguridad expuestos a continuación.

Medidas de Seguridad Básicas

Autenticación y Control de Acceso

1. **Mecanismos de Autenticación Fuerte**: Implementar autenticación de dos factores (2FA), multifactor (MFA)[1] o identificación mediante certificado en aquellos dispositivos que lo permitan o justificar la imposibilidad de hacerlo.
2. **Gestión de Contraseñas**: Establecer políticas de complejidad, rotación y almacenamiento seguro de contraseñas mediante automatización del dispositivo si es posible, o bien mediante definición de políticas en caso contrario.[2]

Red y Comunicaciones

3. **Cifrado de Tráfico**: Utilizar obligatoriamente TLS 1.2 o superior para cifrar la transmisión de datos. En caso de la existencia de equipos intermedios (sin conexión directa a internet) en los que no sea posible, justificar la imposibilidad de hacerlo.[3]
4. **Firewalls y Listas de Control de Acceso**: Configurar firewalls para filtrar tráfico no deseado, concretamente se deberá permitir el acceso únicamente a las direcciones IP fijas pertenecientes al proveedor de servicio de control y a la dirección IP de la Plataforma Nasuvinsa[4]. La configuración de firewall sólo es necesaria cuando el equipo instalado admita dicha configuración, habitualmente sistemas con sistema operativo generales tipo Windows, Linux, etc. Se deberá justificar en su caso la imposibilidad de hacerlo.

[1] Referencia: NIST SP 800-63B

[2] Referencia: ISO/IEC 27001, Sección A.9

[3] Referencia: PCI DSS, Requisito 4

[4] Referencia: CIS Controls, Control 9

Gestión y Configuración de Dispositivos

5. **Actualizaciones de Seguridad**: Provisión para actualizaciones de seguridad[5] de todos los elementos de cada dispositivo y aplicación de las mismas lo antes posible. Se debe realizar todo aquello que esté al alcance del Integrador.
6. **Configuración Segura por Defecto**: Deshabilitar servicios y capacidades innecesarios[6] en todos los dispositivos instalados, estén conectados al exterior o no.

Seguimiento y Auditoría

7. **Registro y Monitorización**: Habilitar logs detallados y monitorización en tiempo real cuando sea posible o realizar análisis periódicos en su defecto.[7]
8. **Alertas de Seguridad**: Sistema de alertas en caso de actividad sospechosa o violaciones de la integridad de la información.[8] Esto requiere de un análisis proactivo por parte del proveedor de servicios con el objetivo de detectar incidencias de acceso a recursos no autorizados, por ejemplo, mediante la inspección periódica de registros de acceso y la definición del método de notificación a Nasuvinsa en caso de detectar cualquier tipo de sospecha de anomalía.

Integridad y Resiliencia

9. **Copias de Seguridad**: Realizar copias de seguridad regulares y garantizar su integridad.[9] Independientemente de los acuerdos de mantenimiento que se apliquen en la fase de operación, durante la fase de integración y puesta en marcha se deberá definir y ejecutar una política de copias de seguridad que permita restablecer el servicio en caso de pérdida de datos o código.
10. **Plan de Recuperación ante Desastres**: Mantener un plan actualizado para recuperación de servicios ante escenarios de pérdida de información, código o recursos físicos como averías de PLCs.[10]

[5] Referencia: NIST SP 800-40

[6] Referencia: CIS Controls, Control 5

[7] Referencia: ISO/IEC 27001, Sección A.12.4

[8] Referencia: NIST SP 800-92

[9] Referencia: ISO/IEC 27001, Sección A.12.3

[10] Referencia: ISO/IEC 22301

Cumplimiento y Evaluación

11. **Evaluación de Riesgos**: Realizar evaluaciones periódicas para identificar vulnerabilidades[11] y definir el procedimiento de análisis y actuación, por ejemplo, indicando qué partes del software deben ser actualizadas, de qué manera se supervisará la disponibilidad de actualizaciones y cómo se procederá a su aplicación.

Interacción con Terceros

12. **Seguridad en la Cadena de Suministro**: Asegurar que todos los componentes y bibliotecas de terceros integrados en los dispositivos instalados cumplen con estándares de seguridad o se encuentran libres de vulnerabilidades o defectos que puedan afectar a la seguridad de los sistemas de información de Nasuvinsa.[12] Justificar el uso de prácticas de desarrollo seguro en los casos de desarrollo interno de librerías o componentes.

[11] Referencia: NIST SP 800-30

[12] Referencia: NIST SP 800-161