Cumplimiento de la norma ISA/IEC 62443 y su impacto en la ciberseguridad OT:

Requisitos y mejores prácticas

La ciberseguridad OT se ha vuelto un desafío crucial debido al crecimiento acelerado de la automatización industrial y la proliferación de activos IoT, que han incrementado la vulnerabilidad de la infraestructura crítica ante ciberamenazas.

En este contexto, las organizaciones buscan garantizar la integridad y seguridad de sus sistemas de automatización y control industrial (IACS), y los estándares **ISA/IEC 62443** han emergido como la referencia clave para la protección de los sistemas OT en distintos sectores.

En esta guía de mapeo, exploraremos los estándares de ciberseguridad OT de la ISA/IEC 62443, explicando su propósito, importancia y cómo contribuyen a la seguridad de los IACS. Además, exploraremos cómo nuestra solución de ciberseguridad, a través de plataformas como la de nuestro partner Nozomi Networks, contribuye a proteger estos sistemas y garantizar el cumplimiento de las partes 2-1 y 3-3 de la norma.

¿Qué es la norma ISA/IEC 62443 y por quées importante en la ciberseguridad OT?

La serie de normas **ISA/IEC 62443** fue desarrollada por el Comité ISA99 y el Comité Técnico 65/Grupo de Trabajo 10 de la IEC con el objetivo de establecer **mejores prácticas y procesos** para la implementación de sistemas de fabricación y control electrónico seguros en entornos de sistemas de control industrial (ICS).

Su enfoque principal es mejorar la seguridad electrónica de los sistemas de control y fabricación, identificar vulnerabilidades y proporcionar directrices para su mitigación. Mantener el cumplimiento con la ISA/IEC 62443 reduce la probabilidad de ciberataques, ayudando a las organizaciones a evitar consecuencias regulatorias, financieras y de seguridad, al tiempo que garantiza niveles óptimos de protección para los ICS y la seguridad ciberfísica.

Estos estándares son aplicables a los responsables del diseño, implementación y gestión de sistemas de control, pero también pueden ser utilizados por operadores de sistemas, integradores, especialistas en seguridad y fabricantes de ICS. La ISA/IEC 62443 se organiza en cuatro grupos, cada uno enfocado en un área específica y su audiencia correspondiente. Nuestras soluciones de ciberseguridad facilitan la **implementación de las partes 2-1 y 3-3, proporcionando herramientas avanzadas para mejorar la ciberseguridad OT.**

Serie de estándares ISA/IEC 62443

GENERAL

- **62443-1-1:** Terminología, conceptos y modelos.
- **62443-1-2:** Glosario maestro de términos y abreviaturas.
- **62443-1-3:** Métricas de conformidad de seguridad del sistema.
- **TR62443-1-4:** Ciclo de vida de la seguridad en IACS y casos de uso.

POLÍTICAS Y PROCEDIMIENTOS

- **62443-2-1:** Establecimiento de un programa de seguridad para IACS.
- **62443-2-2:** Clasificación de programas de seguridad para IACS.
- **TR62443-2-3:** Gestión de parches en el entorno IACS.
- **62443-2-4:** Requisitos de programas de seguridad para proveedores de servicios IACS.
- **TR62443-2-5:** Guía de implementación para propietarios de activos IACS.

SISTEMA

- **TR62443-3-1:** Tecnologías de seguridad para IACS.
- **62443-3-2:** Evaluación de riesgos de seguridad para el diseño del sistema.
- **TR62443-3-3:** Requisitos de seguridad del sistema y niveles de seguridad.

COMPONENTE

- **62443-4-1:** Requisitos del ciclo de vida del desarrollo de seguridad de productos.
- **62443-4-2:** Requisitos de seguridad técnica para componentes de IACS.

ISA/IEC 62443 – Parte 2-1

La norma **ISA/IEC 62443 – Parte 2-1** establece los requisitos para la creación e implementación de un programa de seguridad industrial en sistemas de automatización y control (IACS). Su objetivo es proporcionar a los propietarios de activos un marco estructurado para la gestión del riesgo cibernético a lo largo del ciclo de vida de sus sistemas. Esta parte abarca desde la identificación de activos críticos y la evaluación de vulnerabilidades hasta la documentación de riesgos y la implementación de controles de seguridad, asegurando la protección continua de la infraestructura OT. El cumplimiento de estos lineamientos permite minimizar amenazas cibernéticas y fortalecer la resiliencia operativa en entornos

Control de Seguridad	*Descripción*	*Soporte de la solución de ciberseguridad*
SR 4.2.3.4 - Identificación de IACS	Identificación y agrupación de sistemas de automatización y control industrial (IACS).	Creación de inventarios precisos mediante monitoreo continuo de redes OT e IoT.
SR 4.2.3.5 - Desarrollo de diagramas de red	Creación de diagramas para visualizar activos y riesgos.	Identificación de activos, segmentación de red y priorización de riesgos.
SR 4.2.3.6 - Priorización de sistemas	Asignación de criterios y niveles de prioridad de mitigación de riesgos.	Definición de criterios de criticidad y uso de *Vulnerability Workbooks* para priorización.

Control de Seguridad	Descripción	Soporte de la solución de ciberseguridad
SR 4.2.3.7 - Evaluación de vulnerabilidades	Análisis detallado de vulnerabilidades de cada IACS.	Identificación y priorización de vulnerabilidades con datos de inteligencia de amenazas.
SR 4.2.3.9 - Evaluación detallada de riesgos	Análisis de riesgos basado en la evaluación de vulnerabilidades y criticidad de los IACS.	Uso de métricas KEVs, VWE, CPE, CVE para informes detallados de riesgos.
SR 4.2.3.12 - Evaluación de riesgos durante todo el ciclo de vida	Evaluaciones de riesgo en todas las fases del ciclo de vida de los activos.	Soporte con inventario de activos, análisis de red y detección de amenazas.
SR 4.2.3.13 - Documentación de la evaluación de riesgos	Registro de metodología y resultados de evaluación de riesgos.	Generación de reportes detallados sobre vulnerabilidades y factores de riesgo.
SR 4.2.3.14 - Mantenimiento de registros de evaluación de vulnerabilidades	Registro y actualización continua de evaluaciones de vulnerabilidad.	Seguimiento y mantenimiento de registros de vulnerabilidades detectadas.
SR 4.3.3.3.6 - Protección de conexiones	Protección de la comunicación entre dispositivos y redes.	Detección de conexiones no autorizadas y uso de protocolos inseguros.

Control de Seguridad	Descripción	Soporte de la solución de ciberseguridad
SR 4.3.3.6.2 - Autenticación de usuarios	Control de acceso a sistemas críticos.	Alertas de intentos de acceso sospechosos y auditoría de eventos.
SR 4.3.4.3.7 - Procedimiento de gestión de parches	Establecimiento de procesos documentados para aplicar parches de seguridad.	Monitoreo de software y firmware para aplicar actualizaciones de seguridad.
SR 4.3.4.5.1 - Plan de respuesta a incidentes	Implementación de procedimientos para gestionar incidentes de ciberseguridad.	Generación de reportes de eventos anómalos y alertas en tiempo real.

ISA/IEC 62443 – Parte 3-3

La norma **ISA/IEC 62443 – Parte 3-3** define los requisitos de seguridad específicos para los sistemas industriales y establece niveles de seguridad (S1-S4) en función de la criticidad y el riesgo de cada entorno. Su enfoque se centra en la autenticación de usuarios, integridad de comunicaciones, segmentación de red, protección contra código malicioso y monitoreo continuo de amenazas, entre otros aspectos clave. Al aplicar estos controles, las organizaciones pueden establecer mecanismos de defensa en profundidad, garantizando la confiabilidad y disponibilidad de sus sistemas IACS frente a ataques cibernéticos sofisticados.

Control de Seguridad	*Nivel de Seguridad*	*Soporte de la solución de ciberseguridad*
SR 3.3.1.1 - Identificación y autenticación de usuarios	S1 - S4	Monitoreo de actividad de usuarios y alertas de intentos sospechosos.
SR 3.3.1.5 - Gestión de autenticadores	S1 - S4	Detección de contraseñas débiles o en texto claro.
SR 3.3.1.6 - Gestión de acceso inalámbrico	S1 - S4	Inventario de puntos de acceso y monitoreo de ataques inalámbricos.

Control de Seguridad	Nivel de Seguridad	Soporte de la solución de ciberseguridad
SR 3.3.1.7 - Requerimientos de fuerza de autenticación por contraseña	S1 - S4	Identificación de contraseñas débiles o en texto claro.
SR 3.3.1.8 - Uso de certificados PKI	S1 - S4	Monitoreo de intercambio de certificados en la red.
SR 3.3.1.9 - Autenticación basada en clave pública	S1 - S4	Detección de fallos en autenticación de certificados y PKI.
SR 3.3.1.11 - Control de acceso desde redes no confiables	S1 - S4	Identificación de conexiones desde redes no confiables y monitoreo de acceso remoto.
SR 3.3.2.2 - Control de uso inalámbrico	S1 - S4	Inventario de dispositivos inalámbricos y monitoreo de amenazas.
SR 3.3.2.3 - Control de uso para dispositivos portátiles y móviles	S1 - S4	Monitoreo de dispositivos conectados a la red y detección de amenazas.

Control de Seguridad	Nivel de Seguridad	Soporte de la solución de ciberseguridad
SR 3.3.2.6 - Terminación de sesiones remotas	S1 - S3	Inspección de dispositivos en red y monitoreo de sesiones remotas.
SR 3.3.2.8 - Registro de eventos auditables	S1 - S4	Generación de registros de seguridad detallados para auditoría.
SR 3.3.2.9 - Capacidad de almacenamiento de auditoría	S1 - S4	Monitoreo de espacio disponible en servidores y almacenamiento.
SR 3.3.3.1 - Integridad de comunicaciones	S1 - S4	Detección de intentos de manipulación de tráfico de red.
SR 3.3.3.2 - Protección contra código malicioso	S1 - S4	Identificación de malware y análisis de tráfico malicioso.
SR 3.3.3.4 - Integridad de software e información	S1 - S4	Monitoreo de cambios en software y archivos en sistemas OT.

Control de Seguridad	Nivel de Seguridad	Soporte de la solución de ciberseguridad
SR 3.3.3.5 - Validación de entradas	S1 - S4	Detección de intentos de manipulación de datos en protocolos de red.
SR 3.3.3.8 - Integridad de sesiones	S1 - S4	Monitoreo de sesiones activas y detección de violaciones de sesión.
SR 3.3.4.1 - Confidencialidad de la información	S1 - S4	Identificación de exposición de datos sensibles en tránsito.
SR 3.3.4.3 - Uso de criptografía	S1 - S4	Identificación de cifrados débiles o no seguros.
SR 3.3.5.1 - Segmentación de red	S1 - S4	Visibilidad y segmentación de activos críticos dentro de la red.
SR 3.3.5.2 - Protección de límites de zona	S1 - S4	Monitoreo de dispositivos de protección de zona como firewalls.

Control de Seguridad	Nivel de Seguridad	Soporte de la solución de ciberseguridad
SR 3.3.6.2 - Monitoreo continuo de seguridad	S1 - S4	Análisis de anomalías y detección de vulnerabilidades en tiempo real.
SR 3.3.7.1 - Protección contra ataques de denegación de servicio (DoS)	S1 - S4	Alertas tempranas y detección de ataques DoS.
SR 3.3.7.2 - Gestión de recursos	S1 - S4	Monitoreo de congestión de red y mitigación de ataques de agotamiento de recursos.

Seguridad y cumplimiento

Con soluciones de ciberseguridad, mediante el respaldo tecnológico de la plataforma Nozomi Networks, las organizaciones que operan sistemas ICS pueden abordar los aspectos clave, requisitos y recomendaciones de ciberseguridad OT definidos en la norma **ISA/IEC 62443.** Nozomi Networks está comprometida con la implementación de controles efectivos de ciberseguridad para entornos industriales, combinando innovación tecnológica con una profunda experiencia en seguridad para ICS.

Nuestras soluciones han sido diseñadas para garantizar la seguridad operativa y la integridad de los procesos en alineación con los objetivos y prácticas establecidas en la **ISA/IEC 62443.**

Al adoptar un enfoque proactivo en la **ciberseguridad OT,** las empresas pueden mitigar riesgos, fortalecer la resiliencia de sus sistemas críticos y garantizar la protección continua de su infraestructura industrial.

Soluciones tecnológicas únicas de clase mundial

CONTÁCTANOS

soluciones@procetradi.com

www.procetradi.com

T: +(51) 445-1862 | +(51) 445-2115 | +(51) 445-7660

Av. Benavides 1850 Of. 301 Miraflores
Lima – Perú