NTT DATA

Zero Trust y defensa en profundidad en infraestructuras críticas con ISA/IEC 62443



Sumario

La ciberseguridad de las infraestructuras críticas ya no puede apoyarse únicamente en el perímetro ni asumir que los dispositivos situados dentro de una red industrial son inherentemente confiables. La evolución de las amenazas OT demuestra una capacidad creciente para alcanzar directamente los sistemas que supervisan, controlan y protegen los procesos físicos. En 2017, TRITON/TRISIS demostró que un adversario podía interactuar específicamente con controladores Triconex de un sistema instrumentado de seguridad (SIS). En noviembre de 2023, actores vinculados al IRGC comprometieron PLC/HMI Unitronics Vision expuestos a Internet en distintas infraestructuras críticas. Y el 29 de diciembre de 2025, una campaña destructiva contra el sector energético polaco afectó directamente a RTU, HMI y relés de protección de instalaciones eléctricas, llegando a dañar firmware y provocar la pérdida de telecontrol de estaciones remotas. Más recientemente, en marzo de 2026 Rockwell Automation alertó sobre actividad de actores de amenaza dirigida contra sus controladores y, durante 2026, Siemens ha advertido sobre campañas que señalan específicamente a PLC de la familia S7.

Estos casos evidencian que el adversario OT ya no se limita a atravesar el perímetro o comprometer sistemas IT conectados al entorno industrial: dispone de capacidades demostradas para interactuar con PLC, RTU, HMI, dispositivos de protección e incluso SIS. Este escenario cuestiona el supuesto tradicional de confianza implícita dentro de las redes de control y refuerza la necesidad de verificar identidades, restringir comunicaciones y limitar las posibilidades de movimiento lateral.

Sin embargo, Zero Trust no puede trasladarse íntegramente desde IT hacia OT. La disponibilidad, el determinismo, la seguridad del proceso, la existencia de activos legacy y la necesidad de preservar funciones esenciales limitan la aplicación de determinados mecanismos de autenticación, inspección o control.

Este artículo plantea, por tanto, que Zero Trust debe entenderse en OT como un conjunto de principios que deben adaptarse a las necesidades reales de la operación y al riesgo, y no como una arquitectura que deba reproducirse literalmente. ISA/IEC 62443 proporciona el marco para realizar esta adaptación: partir de las consecuencias del proceso, estructurar el sistema en zonas y conduits, determinar niveles de seguridad objetivo y seleccionar controles técnicos, organizativos o compensatorios proporcionados. De este modo, Zero Trust aporta la reducción de la confianza implícita, la Defensa en Profundidad aporta las capas de protección e ISA/IEC 62443 permite determinar dónde, cómo y con qué nivel de robustez deben materializarse ambas en una infraestructura crítica.



Palabras clave

Zero Trust; Defensa en Profundidad; ISA/IEC 62443; Ciberseguridad industrial; OT; Infraestructuras críticas; Servicios esenciales; Análisis de riesgos; SL-T.

Introducción

Las infraestructuras críticas dependen cada vez más de sistemas de automatización, supervisión y telecontrol para prestar servicios esenciales. Redes eléctricas, instalaciones de gas, sistemas de agua, infraestructuras de transporte y otros entornos industriales críticos combinan centros de control, emplazamientos remotos, redes de comunicaciones y activos de campo cuyo diseño histórico ha priorizado la seguridad y la disponibilidad del proceso. Durante años, esta realidad favoreció arquitecturas relativamente cerradas, con un número limitado de interconexiones y fronteras operativas bien definidas. Sin embargo, la digitalización, la conectividad con sistemas corporativos, el acceso remoto para operación y mantenimiento, la incorporación de analítica avanzada y la integración de datos operativos con procesos de negocio han erosionado esa separación tradicional.

En paralelo, el panorama de amenaza ha cambiado. Hoy no solo preocupan los ataques oportunistas, sino también campañas dirigidas, ransomware con impacto operativo, abuso de accesos remotos, compromiso de terceros y movimientos laterales que aprovechan credenciales, redes planas y activos con capacidades limitadas de protección. El supuesto clásico de que “lo que está dentro de la red de control es confiable” ya no resulta sostenible.

En este contexto, Zero Trust ha ganado relevancia como principio rector de la ciberseguridad moderna. No obstante, en OT no puede implantarse de forma completa ni como una copia de los patrones de TI corporativa. Algunos de sus mecanismos pueden ser inviables, innecesarios o incluso introducir nuevos riesgos cuando interfieren con la disponibilidad, el determinismo, la seguridad del proceso o la capacidad de respuesta del operador. El reto, por tanto, no consiste en importar un catálogo de tecnologías, sino en identificar qué principios de Zero Trust aportan una reducción efectiva del riesgo y aplicarlos con la intensidad y los mecanismos que permita cada entorno operacional. La tesis de este trabajo es que ISA/IEC 62443 proporciona precisamente el marco para realizar esa adaptación: el análisis de riesgos determina las necesidades reales de protección y la arquitectura por zonas y conduits, los niveles de seguridad y los requisitos técnicos permiten materializar una aproximación a Zero Trust sin comprometer las funciones esenciales de la infraestructura.



01. Zero Trust en entornos OT: principios y límites de aplicación

El modelo Zero Trust parte de una idea sencilla: no debe existir confianza implícita por el mero hecho de que un usuario, un equipo o una comunicación se encuentre dentro de una red determinada. La Cybersecurity and Infrastructure Security Agency (CISA) organiza este enfoque en torno a pilares como identidad, dispositivos, redes, aplicaciones/cargas de trabajo y datos, apoyados por capacidades transversales de visibilidad, analítica, automatización y gobernanza (CISA, 2023). Por su parte, NIST remarca que Zero Trust busca reducir las zonas de confianza implícita, basar el acceso en autenticación y autorización granulares y preservar la disponibilidad minimizando demoras temporales asociadas a los mecanismos de verificación (NIST, 2020).

La dificultad aparece cuando estos principios se trasladan al mundo OT. La propia CISA advierte que su Zero Trust Maturity Model no aborda de forma específica los retos asociados a tecnologías operacionales, determinadas clases de IoT o los condicionantes de dispositivos con opciones limitadas de autenticación, visibilidad y seguridad (CISA, 2023). Esta advertencia es especialmente relevante en infraestructuras críticas, donde conviven PLC, RTU, HMIs, estaciones de ingeniería, sistemas de protección, equipos de comunicación y activos distribuidos con larga vida útil, soporte desigual y dependencia de enlaces de telecontrol.

Por ello, en OT Zero Trust debe entenderse como un principio arquitectónico y de gobierno más que como una receta uniforme o un estado final que deba alcanzarse de manera absoluta. No siempre será viable instalar agentes, realizar autenticación contextual continua sobre todos los activos, cifrar todas las comunicaciones o exigir el mismo nivel de telemetría que en una red IT moderna. Tampoco sería adecuado aplicar controles cuya introducción pudiera degradar una función esencial o generar un riesgo operacional superior al que pretenden reducir. Sí es viable, en cambio, aproximarse a los principios de Zero Trust eliminando confianza implícita entre zonas, reforzando identidades humanas y de servicio, controlando rigurosamente el acceso remoto, limitando la conectividad a lo estrictamente necesario, aplicando mínimo privilegio, manteniendo trazabilidad, protegiendo la integridad de cambios y utilizando controles compensatorios allí donde los activos no admiten capacidades avanzadas. La cuestión clave deja de ser "¿podemos aplicar todo Zero Trust?" y pasa a ser "¿qué controles necesitamos realmente, en qué parte del sistema y con qué nivel de robustez para reducir el riesgo sin comprometer la operación?". Esa es precisamente la lógica que permite estructurar ISA/IEC 62443.



Figura 1: Convergencia conceptual entre Zero Trust, Defensa en Profundidad e ISA/IEC 62443.

02. Defensa en profundidad y su relación con la seguridad y disponibilidad del proceso

La Defensa en Profundidad resulta especialmente adecuada para infraestructuras críticas porque se alinea con la forma en que tradicionalmente se gestiona la seguridad, la continuidad operativa y la resiliencia de los procesos. Igual que en un análisis de riesgo operacional, se parte de que ninguna salvaguarda aislada basta para controlar escenarios de consecuencia elevada; lo robusto es la combinación de barreras técnicas, físicas, operativas y organizativas. En subestaciones eléctricas, estaciones de compresión, plantas de tratamiento, terminales, centros de control, infraestructuras de transporte y emplazamientos remotos, el riesgo no depende de un único equipo o de un único control, sino de la interacción entre múltiples medidas que deben permanecer eficaces en el tiempo. Desde esta perspectiva, la lógica de la ciberseguridad industrial converge de forma natural con la lógica de la operación segura: evitar que una sola falla, error o acción maliciosa comprometa la seguridad, la continuidad del servicio o la integridad operativa del proceso.

En términos prácticos, la Defensa en Profundidad en OT combina capas de gobierno, protección física de emplazamientos remotos, segmentación entre entornos corporativos y operacionales, hardening de servidores y estaciones, protección de PLC, RTU y dispositivos de campo, control de accesos remotos de terceros, monitorización, respuesta a incidentes y capacidades de respaldo y recuperación. Su objetivo no es solo bloquear un acceso no autorizado, sino impedir que una única debilidad —por ejemplo, una cuenta compartida, una estación de ingeniería mal ubicada, una pasarela de telecontrol expuesta o una DMZ permisiva— permita comprometer varias capas a la vez. La resiliencia surge precisamente de la combinación ordenada de barreras y de la independencia relativa entre ellas.

La relación con la seguridad y la disponibilidad del proceso es directa. Un incidente cibernético puede alterar consignas, degradar la calidad de la información, inhibir alarmas, bloquear comunicaciones con instalaciones remotas, modificar parámetros operativos o impedir la actuación oportuna del personal. Dependiendo del sector, ello puede traducirse en pérdida de suministro eléctrico, alteración de procesos de tratamiento, indisponibilidad de estaciones de compresión o bombeo, pérdida de señalización o supervisión en transporte, parada de instalaciones industriales o degradación de funciones de seguridad. Por eso, en infraestructuras críticas, la ciberseguridad no debe considerarse un dominio paralelo, sino una condición necesaria para preservar la operación dentro de sus límites previstos, sostener la continuidad de los servicios esenciales y mantener la eficacia de las barreras técnicas y organizativas del proceso.



03. ISA/IEC 62443 como metodología de implementación

La principal fortaleza de ISA/IEC 62443, en este contexto, es que permite convertir la aspiración de Zero Trust en decisiones de seguridad proporcionadas a la realidad operacional. La serie no obliga a desplegar un conjunto uniforme de controles ni parte de la premisa de que todos los activos puedan soportar las mismas capacidades; articula gobierno, análisis de riesgos, arquitectura y requisitos técnicos para seleccionar medidas acordes con el riesgo y con las restricciones del IACS. En la parte 2-1, dirigida al asset owner, la norma define el programa de seguridad como la combinación de capacidades basadas en procesos, personas y tecnología destinadas a reducir el riesgo cibernético del IACS, reconociendo además que estas deben convivir con las restricciones de disponibilidad y rendimiento propias del entorno industrial (ISA, 2024). De esta forma, el objetivo no es alcanzar una aplicación teórica o absoluta de Zero Trust, sino mantener el riesgo en niveles tolerables mediante controles técnica y operacionalmente viables.

La parte 3-2 es el puente metodológico esencial para decidir hasta dónde y cómo aplicar esos principios. Exige realizar una evaluación inicial del riesgo cibernético del sistema bajo consideración, particionar los activos en zonas y conduits según el riesgo y efectuar un análisis detallado que permita determinar un Security Level Target (SL-T) para cada zona o conduit (ISA, 2020). Para un operador de infraestructura crítica, esto significa partir de la criticidad real de las funciones que soportan el servicio —por ejemplo, generación o distribución eléctrica, compresión y transporte de gas, tratamiento y bombeo, señalización y control de tráfico, o supervisión de procesos industriales— y analizar qué consecuencias tendría su degradación sobre la seguridad operativa, el medio ambiente, el cumplimiento y la continuidad del servicio. El resultado no es un nivel uniforme de protección, sino una necesidad de seguridad diferenciada: algunas zonas requerirán controles más exigentes y otras podrán operar con mecanismos menos intrusivos o con medidas compensatorias. El análisis de ciberseguridad no arranca en abstracto ni desde una arquitectura Zero Trust ideal; arranca desde el proceso, sus consecuencias y el riesgo que la organización necesita reducir.

Por último, la parte 3-3 establece los requisitos técnicos de sistema organizados en siete requerimientos fundacionales. Esta estructura permite traducir el SL-T en capacidades concretas de identificación y autenticación, control de uso, integridad, confidencialidad, restricción de flujos, respuesta a eventos y disponibilidad, seleccionadas de acuerdo con la necesidad real de cada zona o conduit. Esto proporciona una vía práctica para acercar el entorno OT a los principios de Zero Trust sin exigir que cada activo implemente por sí mismo todas sus capacidades: cuando existen limitaciones tecnológicas u operativas, la protección puede alcanzarse a nivel de sistema mediante arquitectura, segmentación y controles compensatorios. De este modo, Zero Trust aporta los principios, la Defensa en Profundidad aporta la lógica de capas e ISA/IEC 62443 aporta el método basado en riesgo para decidir qué aplicar, dónde aplicarlo y hasta qué nivel.

Metodología de implementación basada en ISA/IEC 62443

Del riesgo de procesos hasta los controles técnicos y organizativos.

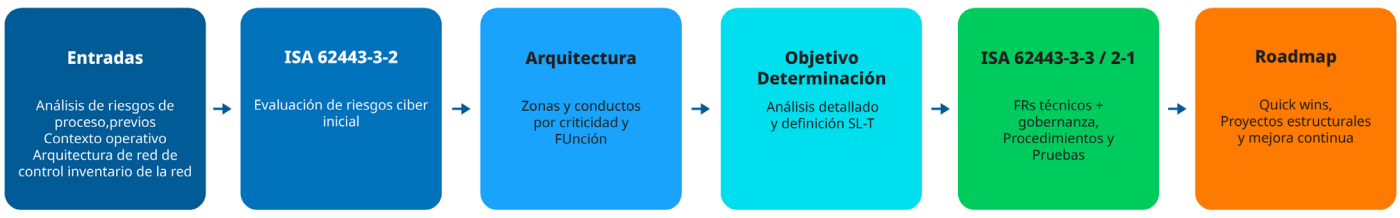


Figura 2: Secuencia recomendada para implantar controles Zero Trust y Defensa en Profundidad mediante ISA/IEC 62443.

04. Los siete requerimientos fundacionales como marco de convergencia

La convergencia entre Zero Trust y Defensa en Profundidad se observa con claridad al analizar los siete requerimientos fundacionales de ISA/IEC 62443-3-3. La norma no pretende reproducir un modelo Zero Trust completo, pero sí proporciona capacidades que permiten materializar muchos de sus principios de manera compatible con OT: identificación y autenticación, mínimo privilegio, integridad, control de flujos, trazabilidad, detección y disponibilidad. La diferencia esencial es que dichas capacidades no se aplican de manera indiscriminada; se seleccionan y dimensionan en función del riesgo, del SL-T, de las características de la zona o conduit y de las restricciones de la operación. Al mismo tiempo, su distribución en distintas capas del sistema convierte esta aproximación en una implementación natural de la Defensa en Profundidad.

FR	Aporte a Zero Trust	Aporte a Defensa en Profundidad	Ejemplo típico en OT
FR1 IAC	Identidad verificada; autenticación fuerte; cuentas únicas; refuerzo de accesos remotos.	Primera barrera frente a accesos no autorizados humanos o de dispositivos.	Cuentas nominativas en SCADA y centros de control; MFA en accesos de tele mantenimiento.
FR2 UC	Privilegio mínimo, roles y segregación de funciones.	Evita que una misma identidad pueda escalar o afectar varias capas.	Roles diferenciados para operación, ingeniería, mantenimiento y proveedores; control de USB y portátiles.
FR3 SI	Verificación de integridad del sistema y de cambios relevantes.	Reduce la probabilidad de alteración maliciosa o accidental de activos críticos.	Hardening, control de configuraciones, protección de PLC/RTU y validación de cambios en consignas, lógicas y firmware.
FR4 DC	Protección de información en tránsito y reposo según criticidad.	Añade una capa de protección sobre parámetros, ficheros y accesos remotos.	Cifrado selectivo de accesos remotos, custodia segura de backups y ficheros de configuración.
FR5 RDF	Segmentación granular y conectividad mínima entre dominios de confianza.	Materializa zonas y conduits, como barreras arquitectónicas.	DMZ industrial, separación entre red corporativa, centros de control, redes de proceso y telecontrol; reglas por excepción.
FR6 TRE	Observabilidad, detección y reacción oportuna.	Añade capas de detección y contención para reducir permanencia del atacante.	Monitorización de red OT, correlación de eventos y respuesta ante accesos anómalos o pérdida de comunicaciones con emplazamientos remotos.
FR7 RA	Mantiene resiliencia y soporta decisiones de acceso sin comprometer continuidad.	Asegura que el sistema siga operando o pueda recuperarse de forma segura.	Redundancia, backups verificados, inventario, continuidad del servicio y recuperación de centros de control y emplazamientos remotos.

Tabla 1: Relación entre los FR de ISA/IEC 62443, Zero Trust y Defensa en Profundidad.

Leídos en conjunto, los siete FR permiten afirmar que ISA/IEC 62443 ofrece un mecanismo práctico para aproximar los principios de Zero Trust a OT sin convertirlos en un requisito absoluto o uniforme. FR1 y FR2 materializan identidad y privilegio mínimo; FR3, FR4 y FR5 aportan integridad, protección de la información y segmentación; FR6 y FR7 extienden la arquitectura hacia la detección, la respuesta y la continuidad operativa. La diferencia frente a una traslación directa de Zero Trust desde IT es que la aplicación concreta de estos requisitos se fundamenta en el riesgo y debe respetar las funciones esenciales del sistema. Esta cobertura es especialmente valiosa en OT porque evita aproximaciones parciales centradas únicamente en firewalls o autenticación, pero también evita imponer controles desproporcionados que puedan afectar a la operación. El objetivo es alcanzar la protección necesaria para cada contexto, no maximizar indiscriminadamente el número de controles.

05. La importancia del análisis de riesgos y del SL-T

Una de las causas más frecuentes de fracaso en programas de ciberseguridad industrial es intentar implantar controles antes de entender con precisión el riesgo que se desea reducir. ISA/IEC 62443-3-2 evita este error al exigir una evaluación inicial del riesgo del sistema bajo consideración, con foco en el peor impacto no mitigado sobre seguridad, medio ambiente, continuidad, producción, calidad, finanzas, cumplimiento y reputación (ISA, 2020). En una infraestructura crítica, ese análisis debe aterrizarse sobre consecuencias operativas concretas: pérdida de control o visibilidad, indisponibilidad de telecontrol, interrupción del suministro o del servicio, alteración de parámetros críticos, afectación de sistemas de protección o degradación de la capacidad de respuesta ante una condición anómala.



Este enfoque conecta de forma muy natural con metodologías usadas para análisis de riesgos de procesos en industrias criticas como HAZOP (Hazard and Operability) y LOPA (Layer of Protection Analysis). El valor no está solo en listar amenazas, sino en comprender escenarios: causa, desviación, consecuencias, salvaguardas existentes, independencia de las capas y riesgo residual. Trasladado a ciberseguridad, el análisis debe responder preguntas como: ¿qué ocurriría si una estación de ingeniería comprometida modificara parámetros de un proceso crítico?, ¿qué impacto tendría la pérdida de comunicaciones con subestaciones, estaciones remotas o instalaciones distribuidas?, ¿qué pasaría si un acceso remoto no supervisado ejecutara una maniobra fuera de secuencia?, ¿qué capa se perdería si la visibilidad del operador queda degradada por malware o por la indisponibilidad de un servidor esencial? Esta lectura permite identificar no solo vulnerabilidades, sino necesidades exactas de reducción de riesgo.

La determinación del SL-T por zona o conduit es una consecuencia práctica de ese análisis. No todas las zonas requieren el mismo nivel de exigencia ni las mismas contramedidas. Un centro de control, una red de proceso, una red de telecontrol con emplazamientos remotos, una DMZ industrial, un sistema de protección o un servidor historiador pueden compartir relación funcional, pero no idéntico perfil de amenaza, criticidad ni tolerancia al fallo. Cuando el SL-T se define correctamente, la organización evita tanto la subprotección como la sobreprotección. Esto tiene beneficios muy concretos: racionaliza inversiones, facilita fases de implantación, mejora la conversación con operaciones y mantenimiento, y permite justificar técnicamente por qué se exige MFA en un acceso remoto, por qué se separan determinados dominios operacionales o por qué se refuerza una política de medios extraíbles.

Además, la norma exige documentar el análisis de riesgos y conservarlo como un activo vivo para auditorías, pruebas, revisiones futuras y evolución del diseño (ISA, 2020). Esa documentación constituye una de las mayores fortalezas del enfoque. Permite pasar de decisiones intuitivas a decisiones demostrables; de “creemos que estamos protegidos” a “sabemos qué riesgo reduce cada control y por qué está donde está”.

06. Hallazgos frecuentes y beneficios de una implantación correcta

La experiencia acumulada en evaluaciones de madurez, revisión documental, visitas a instalaciones, análisis de arquitectura y revisión técnica de configuraciones muestra patrones recurrentes. En entornos industriales e infraestructuras críticas aparecen con frecuencia usuarios genéricos en puestos SCADA, credenciales expuestas, estaciones de ingeniería o telecontrol actuando como puentes entre segmentos, reglas de firewall excesivamente permisivas, DMZ industriales mal implementadas, accesos remotos de terceros sin gobierno suficiente, uso no gobernado de USB, inventarios desactualizados y diagramas de red que no reflejan el estado real de la instalación. Ninguno de estos problemas es extraordinario; precisamente por eso son tan peligrosos.

Cuando la metodología de ISA/IEC 62443 se aplica correctamente, estos hallazgos dejan de tratarse como incidencias aisladas y pasan a interpretarse como síntomas de una arquitectura sin límites de confianza claros, sin asignación correcta de responsabilidades o sin una reducción de riesgo suficiente. En ese momento resulta posible priorizar quick wins —cuentas únicas, endurecimiento de accesos remotos, refuerzo de DMZ, control de puertos, segmentación básica, centralización de registros— y, al mismo tiempo, definir mejoras estructurales de medio plazo como rediseño por zonas y conduits, segregación entre redes corporativas, de proceso y de telecontrol, gobierno del ciclo de vida de vulnerabilidades, procedimientos de backup/restore y ejercicios de respuesta a incidentes OT.



El beneficio no es solo técnico. También mejora la trazabilidad, reduce la dependencia del conocimiento tácito, facilita auditorías, ordena la relación entre IT y OT y proporciona a la dirección una base objetiva para decidir dónde invertir primero. En otras palabras, el valor real del enfoque no está en acumular controles, sino en construir una postura de seguridad coherente con el proceso y sostenible en el tiempo.

Hallazgo observado	Riesgo dominante	Respuesta prioritaria alineada con ISA 62443
Usuarios genéricos en SCADA/HMI	Pérdida de trazabilidad y facilidad de escalado.	FR1 y FR2: cuentas únicas, roles, MFA donde proceda y revisión de privilegios.
Estación de ingeniería o sistema de telecontrol utilizado como puente entre segmentos	Movimiento lateral, punto único de fallo y pérdida de control del acceso.	FR5 y FR3: reubicar la estación, segmentar conduits y endurecer el activo.
DMZ industrial o pasarela de interconexión excesivamente permisiva	Acceso directo desde IT o redes externas a servicios OT críticos.	FR5 y FR1: reglas por excepción, MFA, publicación de réplicas y registro de sesiones.
Acceso remoto de terceros sin control suficiente	Maniobras no supervisadas, exposición de credenciales y baja trazabilidad.	FR1, FR2 y FR5: MFA, jump server, ventanas de acceso y registro de sesiones.
Uso de USB y portátiles sin control	Introducción de malware y alteración de configuraciones.	FR2, FR3 y FR7: política de medios extraíbles, validación previa y procedimientos de escaneo seguro.
Inventario y diagramas desactualizados	Decisiones de riesgo basadas en una arquitectura irreal.	ISA 62443-3-2 y 2-1: inventario fiable, documentación viva y revisión periódica de cambios.

Tabla 2: Hallazgos recurrentes en evaluaciones OT y respuesta recomendada.

Conclusión

Zero Trust y Defensa en Profundidad no deben entenderse como enfoques alternativos para la protección de infraestructuras críticas. Zero Trust aporta una disciplina necesaria: cuestionar la confianza implícita, verificar cada acceso relevante y reducir la conectividad a lo estrictamente necesario. La Defensa en Profundidad aporta una lógica de ingeniería bien conocida en el mundo industrial: ninguna barrera aislada es suficiente y la resiliencia depende de la combinación ordenada de capas técnicas, físicas y organizativas.

ISA/IEC 62443 es el marco que permite integrar ambos conceptos sin desalinearlos de la operación real de una infraestructura crítica. Su valor reside en que enlaza gobierno, análisis de riesgos, zonas y conduits, niveles de seguridad objetivo y requisitos técnicos en una metodología verificable. Esto permite determinar qué principios de Zero Trust son aplicables en cada parte del IACS, qué nivel de exigencia es necesario y qué medidas compensatorias deben utilizarse cuando las capacidades nativas del activo o las restricciones operativas impiden aplicar un control de forma directa. Aplicada con rigor, la norma no persigue un Zero Trust absoluto, sino una protección proporcionada al riesgo que preserve la seguridad y la disponibilidad del proceso, favorezca decisiones de inversión justificables y transforme la ciberseguridad industrial en una disciplina auditable y gestionable.

Para operadores de infraestructuras críticas y organizaciones industriales, el mensaje es claro: Zero Trust no debe tratarse como un modelo que pueda trasladarse íntegramente desde IT a OT ni como un objetivo de cumplimiento aislado. Su valor reside en los principios que introduce —eliminación de confianza implícita, verificación, mínimo privilegio y reducción de comunicaciones innecesarias—, siempre que se apliquen de acuerdo con el riesgo y sin comprometer las funciones esenciales del proceso. ISA/IEC 62443 proporciona el mecanismo para realizar esa adaptación: analizar las consecuencias y el riesgo, definir zonas y conduits, establecer el SL-T y seleccionar los requisitos y controles necesarios para cada contexto. La respuesta práctica, por tanto, no es “implantar todo Zero Trust”, sino acercarse a sus principios mediante una Defensa en Profundidad basada en riesgo y ajustada a las necesidades reales de la operación.

Referencias

CISA (2023) Zero Trust Maturity Model, Version 2.0. Cybersecurity and Infrastructure Security Agency.

ISA (2013) ANSI/ISA-62443-3-3. System Security Requirements and Security Levels.

ISA (2020) ANSI/ISA-62443-3-2. Security Risk Assessment for System Design.

ISA (2024) ANSI/ISA-62443-2-1. Security Program Requirements for IACS Asset Owners.

NIST (2020) SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology.



CONTACTO

Jhon Jairo Medina,
Technical Manager Ciberseguridad ICS/OT en NTT DATA

LinkedIn

Contact Us

Para más información, visita nuestra página sobre ciberseguridad OT, IoT e IIoT


NTT DATA