Número 115 | Junio 2026

NTT DATA

Radar

El magazine de ciberseguridad

Cuando las máquinas aprenden a atacar infraestructuras reales

Por Luís Guillen

La convergencia de la inteligencia artificial y los sistemas de tecnología operacional ha creado un nuevo campo de batalla híbrido, donde no basta con proteger datos: ahora está en juego la continuidad del mundo físico. No es lo mismo un robo de datos de una tarjeta de crédito que una interrupción del suministro eléctrico de una población, la parada de una planta de tratamiento de aguas o desencadenar un fallo en cadena en una refinería.

En el primer caso hablamos de un incidente grave mientras que en el segundo hablamos de un escenario potencialmente catastrófico, con impacto directo sobre la seguridad de las personas. Durante años, la ciberseguridad separó el mundo digital del mundo físico, pero hoy, esa frontera prácticamente ha desaparecido, y la inteligencia artificial está terminando de derribar los últimos límites.

Los sistemas de tecnología operacional son el tejido nervioso de la industria. Hablamos de controladores lógicos programables (PLC), sistemas SCADA, sensores industriales y toda la infraestructura digital que gobierna procesos físicos incluyendo componentes que controlan los edificios inteligentes y material médico, es decir desde la apertura de una válvula o la gestión del tráfico ferroviario hasta el funcionamiento de ascensores, circuitos de televisión, sistemas de imagen médica o respiradores conectados.
Durante décadas, estos entornos vivieron relativamente aislados de las redes corporativas.

Su seguridad se basaba, en buena medida, en esa separación, el famoso air gap, la brecha física que los blindaba frente a amenazas externas. Ese modelo ya es historia. La presión hacia la eficiencia operativa, la monitorización remota y la integración con sistemas empresariales ha ido erosionando esa distancia. Hoy, la mayoría de los entornos OT / IoT están conectados, de una forma u otra, a redes que tienen contacto con el exterior. Y eso los convierte en objetivos.

La IA como multiplicador de amenazas

Si la exposición de estos entornos ya era preocupante, la irrupción de la inteligencia artificial en el ecosistema de los ciberataques eleva la amenaza a una dimensión completamente nueva. No hablamos de ciencia ficción. Hablamos de herramientas que ya existen, que se perfeccionan cada mes y que están al alcance de actores con recursos que, hasta hace poco, solo tenían los estados más avanzados.

La IA permite a los atacantes automatizar el reconocimiento de infraestructuras, identificar vulnerabilidades específicas en protocolos industriales como Modbus, DNP3 o IEC 61850 y generar exploits adaptados a entornos concretos con una velocidad que ningún equipo humano puede igualar.

Pero quizá lo más inquietante no es la velocidad, sino la sutileza. Los modelos de aprendizaje automático pueden analizar el comportamiento normal de un sistema OT / iOT durante semanas o meses, aprender sus patrones operativos y diseñar ataques que pasen desapercibidos para los sistemas de detección tradicionales. Un pequeño desvío en la presión de una tubería. Una variación imperceptible en la frecuencia de una turbina. Anomalías que ningún operario humano detectaría a tiempo.

El lado luminoso, la IA como escudo

Sería, sin embargo, un error reducir el papel de la inteligencia artificial al de mera amenaza. La misma tecnología que puede ser weaponizada por actores maliciosos es también la herramienta más poderosa con la que cuenta el sector para defenderse.

Los sistemas de detección de anomalías basados en IA pueden monitorizar en tiempo real miles de variables en un entorno industrial, establecer líneas base de comportamiento normal y alertar ante cualquier desviación, por pequeña que sea, antes de que se convierta en un incidente.

La gestión de vulnerabilidades, la correlación de eventos en entornos híbridos y la respuesta automatizada ante incidentes son áreas donde la inteligencia artificial no solo mejora la eficiencia, sino que puede ser el único medio viable de actuar a la velocidad que los ataques más sofisticados exigen.

Un analista humano no puede procesar, en segundos, millones de registros de un sistema SCADA. Un modelo bien entrenado, sí.

El reto que nadie quiere nombrar

Pero hay un problema estructural que sigue latente en la industria, los entornos OT no fueron diseñados con la ciberseguridad en mente. Muchos de los sistemas en funcionamiento tienen décadas de antigüedad, corren sobre sistemas operativos sin soporte, carecen de capacidades de cifrado y no pueden ser parcheados sin interrumpir procesos productivos críticos. Integrar soluciones de IA en estos entornos es, técnicamente, un reto mayúsculo. Y culturalmente los equipos de operaciones y los de seguridad todavía hablan idiomas distintos, con prioridades que a menudo se contraponen.

A esto se suma la escasez de talento especializado. Los profesionales que combinan conocimiento profundo de sistemas industriales, operación OT y ciberseguridad todavía no son numerosos, porque se trata de un perfil muy específico y de madurez relativamente reciente en el mercado. Sin esta capacidad interna o externa, incluso las soluciones más sofisticadas pueden terminar convirtiéndose en cajas negras difíciles de gestionar cuando se produce un incidente crítico.

Una cuestión de prioridad estratégica

La protección de los entornos OT frente a amenazas potenciadas por IA no puede seguir siendo un asunto relegado a los departamentos técnicos. Es una cuestión de seguridad nacional, de continuidad económica y de responsabilidad social. Los ataques registrados en los últimos años contra infraestructuras críticas contra redes eléctricas, plantas de tratamiento de agua o sistemas de salud no son hechos aislados, sino señales claras de un riesgo creciente.

La respuesta no puede llegar cuando el ataque ya se ha producido, debe construirse antes, mediante el cumpliendo de marcos regulatorios que establecen requisitos mínimos en función de la criticidad del entorno, con inversión sostenida en formación especializada, con una colaboración real entre el sector público y privado que vaya más allá de los informes de buenas intenciones y con una industria tecnológica que diseñe soluciones pensando en la complejidad real de los entornos OT / iOT y no solo en los escenarios ideales y elegantes de un laboratorio.

La inteligencia artificial ha llegado al mundo industrial para quedarse. La pregunta no es si transformará la ciberseguridad OT, sino si seremos capaces de dirigir esa transformación antes de que lo hagan otros en nuestro lugar.

Luís Guillen
Cybersecurity Director

La primavera de 2026 no llegó sola

Cibercrónica Alicia Isabel Martínez Vera

Mientras Europa comenzaba a prepararse para el verano y las empresas aceleraban sus procesos de digitalización, el ciberespacio volvió a demostrar que no existen estaciones tranquilas. Desde mediados de abril hasta hoy, el panorama de la ciberseguridad ha estado marcado por ransomware cada vez más agresivo, filtraciones masivas de datos, ataques a cadenas de suministro y una nueva generación de amenazas impulsadas por inteligencia artificial.

La sensación dominante durante estas semanas ha sido clara: los atacantes ya no buscan únicamente robar información; buscan paralizar operaciones, erosionar la confianza y convertir la dependencia digital en un arma.

Durante el mes de abril se siguió con una tendencia que ya se había insinuado durante 2025: los proveedores tecnológicos se consolidaron como el punto de entrada favorito para los ciberdelincuentes. Informes de inteligencia y análisis sectoriales alertaron sobre un incremento de ataques dirigidos a terceros con acceso privilegiado a infraestructuras corporativas.

Uno de los episodios más simbólicos fue el ataque sufrido por Inditex. El gigante textil confirmó el acceso no autorizado a bases de datos alojadas en servidores de un proveedor externo, reabriendo el debate sobre la seguridad de los ecosistemas interconectados y la dificultad de controlar riesgos fuera del perímetro corporativo.

Casi al mismo tiempo, la cadena de gimnasios Basic-Fit sufría una intrusión que terminó exponiendo datos personales de miles de usuarios europeos. Nombres, correos electrónicos, teléfonos y datos bancarios quedaron comprometidos en uno de los ataques más mediáticos del sector retail y servicios en lo que iba de año.

Detrás de estos incidentes se repetía el mismo patrón: los atacantes no siempre golpeaban directamente a la víctima principal. Entraban por integraciones olvidadas, aplicaciones conectadas o proveedores con defensas más débiles. El perímetro tradicional había desaparecido definitivamente.

Otra tendencia inquietante: el uso masivo de inteligencia artificial por parte de actores maliciosos.

Los expertos comenzaron a advertir que el phishing había cambiado para siempre. Los antiguos correos plagados de errores ortográficos dieron paso a mensajes impecables, personalizados y casi imposibles de distinguir de una comunicación legítima. La IA generativa empezó a utilizarse para automatizar campañas de ingeniería social, clonar voces y generar mensajes hiperrealistas a gran escala.

En paralelo, el ransomware evolucionó hacia modelos prácticamente autónomos. Algunas campañas detectadas en abril mostraban malware capaz de identificar sistemas críticos, cifrar información y exfiltrar datos sin apenas intervención humana.

Si el mes de abril estuvo marcado por las brechas corporativas, mayo dejó una imagen distinta: las administraciones públicas volvieron a convertirse en objetivo prioritario del ransomware.

El caso más visible fue el del Ayuntamiento de Valdemoro. El municipio madrileño sufrió un ataque que paralizó parcialmente servicios esenciales, afectando al padrón municipal, sistemas de gestión y plataformas de pago.

Días después se supo que el grupo Kairos reivindicaba la intrusión y afirmaba haber obtenido cerca de 1,8 TB de información sensible. El incidente reflejaba una tendencia cada vez más frecuente: la “doble extorsión”.

A medida que avanzaba el mes, otra realidad comenzó a hacerse evidente: las filtraciones de datos habían dejado de ser excepcionales. Datos publicados en España mostraron que durante 2025 se notificaron más de 2.600 brechas de seguridad, afectando a más de 200 millones de registros. La cifra equivalía, simbólicamente, a más de cuatro brechas por ciudadano. Los ataques ya no afectaban únicamente a grandes multinacionales. Cualquier organización con datos, conectividad y dependencia tecnológica podía convertirse en objetivo.

Mientras los ataques aumentaban, también lo hacía la presión regulatoria. Durante abril, las instituciones europeas reforzaron el debate sobre la aplicación de la directiva NIS2 y la necesidad de armonizar obligaciones de ciberseguridad en toda la Unión Europea.

Si hubiera que resumir estas últimas semanas en una sola idea, sería esta: la confianza digital se ha convertido en el principal objetivo de los atacantes.

Las empresas ya no solo temen perder datos; temen detener operaciones, perder reputación y ver comprometida la relación con clientes y socios. Los ciberdelincuentes han aprendido que el impacto psicológico y operativo puede ser tan valioso como el económico.

Entre mediados de abril y mayo de 2026, el panorama dejó una conclusión inequívoca: la ciberseguridad ha entrado definitivamente en una nueva etapa. Una etapa donde la IA ofensiva, el ransomware automatizado y la explotación de terceros están redefiniendo el riesgo digital global.

Alicia Isabel Martinez Vera
Cybersecurity Consultant

ZERO TRUST y defensa en profundidad con ISA 62443

Artículo por Jhon Jaire Medina Davis

La ciberseguridad de las infraestructuras críticas ya no puede apoyarse únicamente en el perímetro. La convergencia IT/OT, el telecontrol de instalaciones distribuidas, el acceso remoto de terceros, la presencia de activos legacy y la exigencia de continuidad del servicio obligan a adoptar modelos más granulares y basados en riesgo. En este contexto, Zero Trust aporta un principio valioso: eliminar la confianza implícita y verificar de forma continua identidades, dispositivos, comunicaciones y accesos. Sin embargo, su traslación directa desde IT hacia OT resulta limitada por restricciones de disponibilidad, determinismo, operación en remoto y ciclos de vida tecnológicos muy largos. Este artículo argumenta que la manera más eficaz de llevar Zero Trust al entorno industrial no consiste en replicar controles IT, sino en integrarlo con la Defensa en Profundidad y materializarlo mediante la metodología de ISA/IEC 62443. Se explica la relación entre ambos conceptos, su vínculo con la seguridad y la disponibilidad del proceso, la cobertura que ofrecen los siete requerimientos fundacionales de ISA 62443-3-3 y la importancia del análisis de riesgos conforme a ISA 62443-3-2 para definir zonas, conduits, niveles de seguridad objetivo y controles proporcionados. El enfoque se presenta con un lenguaje especialmente próximo a operadores, permitiendo traducir principios estratégicos en medidas técnicas y organizativas auditables, priorizadas y alineadas con la realidad operativa de los sistemas industriales.

Las infraestructuras criticas operan sobre sistemas de automatización y telecontrol cuyo diseño histórico ha priorizado la seguridad y la disponibilidad del proceso, así como la continuidad del servicio.

Durante años, esta realidad favoreció arquitecturas relativamente cerradas, con un número limitado de interconexiones y con fronteras operativas bien definidas. Sin embargo, la digitalización industrial, la conectividad con sistemas corporativos, el acceso remoto para operación y mantenimiento, la incorporación de analítica avanzada y la necesidad de integrar 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 como una copia de los patrones de TI corporativa. El reto no consiste en importar un catálogo de tecnologías, sino en reinterpretar sus principios para un entorno donde un retraso de autenticación, una exploración agresiva o un reinicio no planificado pueden traducirse en pérdida de visibilidad del proceso, maniobras operativas incorrectas, degradación de la calidad interrupciones del servicio.

La tesis de este trabajo es que la convergencia práctica entre Zero Trust y Defensa en Profundidad ya está contenida en ISA/IEC 62443, siempre que su metodología se aplique correctamente y con una lectura claramente orientada al riesgo.

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 criticas, donde conviven PLC, RTU, HMIs, estaciones de ingeniería, 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. No siempre será viable instalar agentes, hacer autenticación contextual continua sobre todos los activos o exigir el mismo nivel de telemetría que en una red IT moderna.

Sí es viable, en cambio, eliminar la confianza implícita entre zonas, reforzar las identidades humanas y de servicio, controlar rigurosamente el acceso remoto, limitar la conectividad a lo estrictamente necesario, exigir trazabilidad, proteger la integridad de cambios y utilizar controles compensatorios allí donde los activos no admiten controles avanzados. En otras palabras, en OT Zero Trust no se implementa "igual que en IT"; se implementa de forma adaptada, conservando el principio y ajustando el mecanismo a la criticidad y a la operabilidad del proceso.

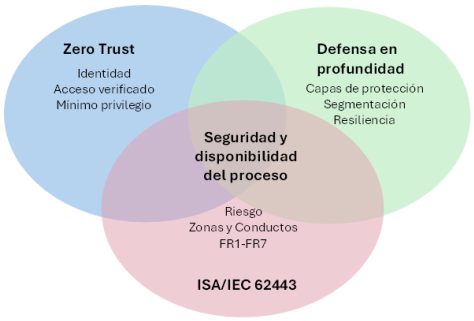


Figura 1: Convergencia conceptual entre Zero Trust, Defensa en Profundidad e ISA/IEC 62443.

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

La Defensa en Profundidad resulta especialmente adecuada para infraestructuras criticas porque se alinea con la forma en que tradicionalmente se gestiona la seguridad y la continuidad operativa del proceso. 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, operativas y organizativas. En plantas de tratamiento, estaciones de bombeo, depósitos, redes de distribución y sistemas de saneamiento, 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 calidad, 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 estaciones remotas, modificar parámetros operativos o impedir la actuación oportuna del personal.

En el sector agua, ello puede traducirse en dosificación incorrecta de reactivos, maniobras inadecuadas de bombeo, pérdida de visibilidad sobre depósitos y estaciones, afectación de la calidad del agua tratada o interrupciones del servicio. Por eso, en infraestructuras críticas de agua y saneamiento, la ciberseguridad no debe considerarse un dominio paralelo, sino una condición necesaria para preservar la operación dentro de sus límites previstos y mantener la eficacia de las barreras técnicas y organizativas del proceso.

ISA/IEC 62443 Como metodología de implementación

La principal fortaleza de ISA/IEC 62443 es que convierte conceptos estratégicos en una metodología aplicable. La serie no es un listado plano de controles; articula gobierno, análisis de riesgos, arquitectura y requisitos técnicos de manera coherente. 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 sus políticas deben convivir con las del ISMS corporativo sin perder de vista las restricciones de disponibilidad y rendimiento propias del entorno industrial (ISA, 2024).

La parte 3-2 es el puente metodológico esencial. 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 operadores del sector agua, esto significa partir de la criticidad real de cada función de proceso —por ejemplo, captación, dosificación, bombeo, almacenamiento, distribución o telecontrol— y analizar qué consecuencias tendría su degradación sobre la seguridad operativa, la calidad del agua, el cumplimiento y la continuidad del servicio. El análisis de ciberseguridad no arranca en abstracto: arranca desde el conocimiento del proceso y de sus consecuencias.

Por último, la parte 3-3 establece los requisitos técnicos de sistema organizados en siete requerimientos fundacionales. Esta estructura facilita traducir el SL-T en controles concretos, con la granularidad suficiente para definir medidas realistas y auditables. De este modo, Zero Trust aporta los principios, la Defensa en Profundidad aporta la lógica de capas e ISA/IEC 62443 aporta el método para convertir ambos en arquitectura, procedimientos, evidencias y hoja de ruta de mejora.

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

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. Lejos de ser un marco ajeno a Zero Trust, la norma ya incorpora sus principios esenciales cuando exige identificación robusta, mínimo privilegio, integridad, control de flujos, visibilidad y disponibilidad.

Al mismo tiempo, la forma en que dichos requisitos se distribuyen en zonas, conduits, funciones y procedimientos los convierte 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 acceso remoto a ETAP/EDAR; MFA en telemantenimiento.
FR2 UC	Privilegio mínimo, roles y segregación de funciones.	Evita que una misma identidad pueda escalar o afectar varias capas.	Roles diferenciados para operación central, mantenimiento, laboratorio 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 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, red 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.
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 estaciones remotas.

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 no obliga a elegir entre Zero Trust y Defensa en Profundidad. Por el contrario, ofrece un lenguaje común para ambos. 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. Esta cobertura es especialmente valiosa en OT porque evita aproximaciones parciales centradas únicamente en firewalls o autenticación, y obliga a considerar simultáneamente control de acceso, arquitectura de comunicaciones, integridad del sistema y resiliencia.

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 el caso del sector agua, ese análisis debe aterrizarse además sobre efectos concretos como pérdida de control sobre la dosificación, indisponibilidad del telecontrol, afectación de la calidad del agua o interrupción del servicio en estaciones remotas y plantas principales.

Este enfoque conecta de forma muy natural con HAZOP y LOPA. Desde la práctica del análisis de riesgos operacionales, 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 operación comprometida alterara consignas de dosificación?, ¿qué impacto tendría la pérdida de comunicaciones con estaciones remotas de bombeo o depósitos?, ¿qué pasaría si un acceso remoto no supervisado ejecutara maniobras fuera de secuencia?, ¿qué capa se perdería si la visibilidad del operador queda degradada por malware o por la indisponibilidad del historiador? 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. Una red de proceso en planta, una red de telecontrol con estaciones remotas, una DMZ industrial 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 dominios de proceso y telecontrol 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”.

Hallazgos frecuentes y beneficios de una implantación correcta

La experiencia acumulada en evaluaciones de madurez, revisión documental, visitas a planta, análisis de arquitectura y revisión técnica de configuraciones muestra patrones recurrentes.

En instalaciones industriales 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 telecontrol utilizada 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 telecontrol permisiva	Acceso directo desde IT 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.

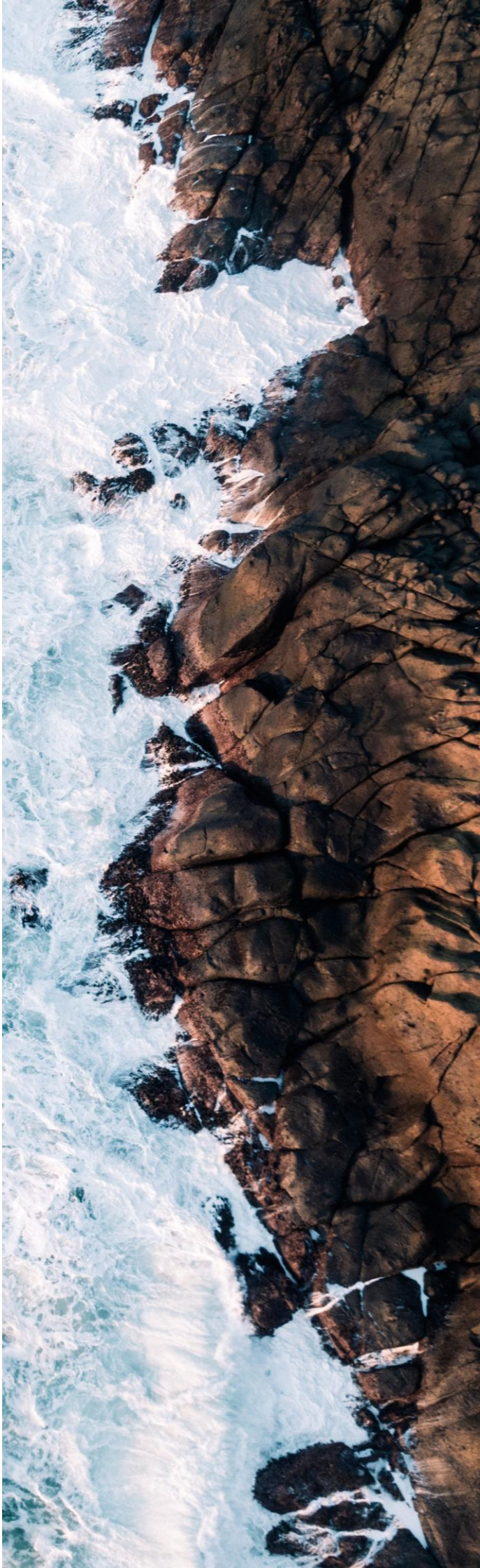
Conclusión

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 critica. Su valor reside en que enlaza gobierno, análisis de riesgos, zonas y conduits, niveles de seguridad objetivo y requisitos técnicos en una metodología verificable. Aplicada con rigor, no solo mejora la protección cibernética del IACS, sino que preserva la seguridad y la disponibilidad del proceso, favorece decisiones de inversión basadas en riesgo y transforma la ciberseguridad industrial en una disciplina auditable y gestionable.

Para organizaciones del sector industrial, el mensaje es claro: la pregunta ya no es si conviene incorporar principios Zero Trust, sino cómo hacerlo sin comprometer disponibilidad, continuidad del servicio ni mantenibilidad. La respuesta práctica pasa por adoptar una Defensa en Profundidad basada en riesgo y ejecutarla mediante ISA/IEC 62443.

Jhon Jairo Medina Davis
Cybersecurity Technical Manager



Tendencias OT: Cifrado cuántico en entornos industriales

Tendencias por Miren Ordoñez de Arce

En el mundo de la ciberseguridad industrial (OT), donde conviven fábricas, plantas energéticas o sistemas de transporte, la protección de la información nunca ha sido tan crítica. A medida que la digitalización avanza —con sensores, PLCs y redes industriales cada vez más conectadas — también crecen los riesgos. Y en el horizonte aparece una nueva disrupción: la computación cuántica.

Aquí es donde entra en juego una de las tendencias más comentadas: el cifrado cuántico, una tecnología que promete redefinir cómo protegemos las comunicaciones en entornos industriales.

¿Por qué preocupa tanto la computación cuántica?

Hoy en día, la mayoría de los sistemas de cifrado (como los que protegen comunicaciones industriales o redes corporativas) se basan en problemas matemáticos difíciles de resolver. Sin embargo, los futuros ordenadores cuánticos podrían romper muchos de estos sistemas en cuestión de minutos.

Esto plantea un escenario preocupante para la industria: datos de producción, recetas, configuraciones de maquinaria o incluso infraestructuras críticas podrían quedar expuestos.

¿Qué es exactamente el cifrado cuántico?

Cuando hablamos de cifrado cuántico, en realidad nos referimos sobre todo a una tecnología concreta: la Distribución Cuántica de Claves (QKD). De forma sencilla, QKD permite que dos sistemas compartan una clave secreta para cifrar información, pero con una diferencia clave: utiliza principios de la física cuántica en lugar de matemáticas tradicionales.

Esto tiene una consecuencia muy potente:

- Si alguien intenta interceptar la clave, el propio sistema lo detecta automáticamente, porque medir un estado cuántico altera su comportamiento.

Es decir, no solo protege la información, sino que avisa de intrusiones en tiempo real.

¿Cómo encaja esto en entornos OT?

Aunque pueda parecer algo futurista, el cifrado cuántico ya se está explorando en escenarios industriales reales. Por ejemplo, se ha estudiado su uso en procesos tan concretos como la transferencia segura de programas a PLCs en fábricas.

En entornos OT, sus aplicaciones más claras son:

- Protección de comunicaciones entre plantas y centros de control
- Seguridad en redes de energía o infraestructuras críticas
- Intercambio seguro de datos entre proveedores y sistemas industriales

Esto es especialmente relevante porque muchos sistemas industriales tienen ciclos de vida muy largos (10-20 años), lo que significa que deben prepararse hoy para amenazas futuras.

¿Qué ventajas aporta frente a la seguridad tradicional?

El cifrado cuántico introduce un cambio de paradigma:

- Seguridad basada en la física, no en matemáticas. No depende de que un problema sea “difícil”, sino de leyes físicas imposibles de romper.
- Detección de espionaje. Cualquier intento de interceptación deja rastro inmediato.
- Preparación para el “Q-Day”. Ese momento en que los ordenadores cuánticos puedan romper el cifrado actual.

Pero... no todo es tan sencillo

Como toda tecnología emergente, el cifrado cuántico también tiene retos importantes:

- Coste e infraestructura: requiere hardware especializado y, en muchos casos, fibra óptica dedicada.
- Limitaciones de distancia: la transmisión cuántica aún tiene restricciones técnicas.
- Integración con sistemas legacy: algo especialmente complejo en OT.

Por eso, en la práctica, muchas organizaciones están combinando QKD con otras soluciones como la criptografía post-cuántica (basada en software).

¿Moda o realidad inminente?

Aunque todavía no es una tecnología masiva, el cifrado cuántico ya está saliendo del laboratorio. Proyectos europeos como EuroQCI o iniciativas industriales muestran que se está convirtiendo en una prioridad estratégica, especialmente para sectores críticos.

En el contexto OT, esto no es solo una tendencia tecnológica, sino una cuestión de resiliencia: proteger hoy los sistemas que deberán seguir funcionando dentro de décadas.

Conclusión: la seguridad industrial entra en una nueva era

El cifrado cuántico representa un cambio profundo en cómo entendemos la ciberseguridad. Para el mundo industrial, implica pasar de proteger sistemas frente a amenazas actuales, a prepararse para amenazas que aún no han llegado.

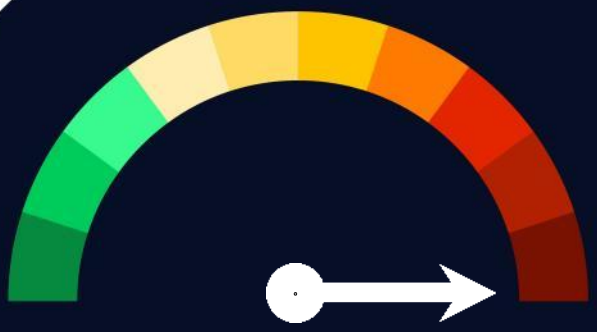
No sustituirá de la noche a la mañana a las soluciones actuales, pero sí marca una dirección clara: la seguridad del futuro será "quantum-safe" o no será.

Miren Ordoñez de Arce
Cybersecurity Lead Analyst

Vulnerabilidades

Inyección SQL en MegaCMS de CRM Sistemas de Fidelización

Fecha: 29 de abril de 2026
CVE: CVE-2026-3325



CVSS: 10

CRÍTICA

Descripción

Se ha descubierto una vulnerabilidad de severidad crítica que afecta a MegaCMS, software para la gestión de sistemas de reservas, ticketing y venta online.

La vulnerabilidad se produce por una validación y depuración inadecuadas de un campo de la entrada del usuario. Mediante una solicitud POST, el parámetro 'id_territorio', utilizado inmediatamente después del envío del formulario de registro, podría ser manipulado por un atacante no autenticado para ejecutar consultas SQL arbitrarias.

La vulnerabilidad ya ha sido corregida en la última versión del software y se propone como solución actualizar a esta última versión.

Solución

- El parche se incluye en la última versión disponible del software.
- Se recomienda actualizar lo antes posible a la última versión y monitorizar intentos de explotación en los logs de los servidores web.

Productos afectados

- MegaCMS en la versión 12.0.0.
- Algunos ejemplos: Webs de hoteles o servicios turísticos, plataformas de eventos o de venta de entradas.

Referencias

- incibe.es
- app.opencve.io

Vulnerabilidades

Integer Overflow en Blink / Google Chrome

Fecha: 6 de mayo de 2026
CVE: CVE-2026-7896

CVSS: 8.8

ALTA

Descripción

Se ha identificado una vulnerabilidad crítica de tipo Integer Overflow en Blink, el motor de renderizado utilizado por Google Chrome.

Esta vulnerabilidad se produce durante el procesamiento de contenido HTML especialmente diseñado, pudiendo provocar un desbordamiento de enteros que derive en corrupción del heap.

Un atacante remoto podría explotar esta vulnerabilidad mediante una página web maliciosa, sin requerir interacción adicional por parte del usuario más allá de visitar o abrir dicha página con una versión vulnerable de Chrome.

La explotación exitosa podría permitir la ejecución de código arbitrario en el contexto del navegador afectado.

Solución

Se recomienda:

- Actualizar Google Chrome a la versión 148.0.7778.96/97 o posterior, según sistema operativo.

Productos afectados

Algunos de los productos afectados son:

- Google Chrome para Windows, Linux y MacOS anterior a 148.0.7778.96

Nota: Otros navegadores basados en Chromium podrían verse impactados si incorporaban una versión vulnerable de Blink, pero conviene validarlo con los avisos específicos de cada fabricante.

Referencias

- app.opencve.io
- nvd.nist.gov
- chromereleases.googleblog.com

Redis ha corregido fallos que permitían ejecución de código en sus servidores

Fecha: 6 de mayo de 2026
CVE: CVE-2026-23479 y 4 mas

Alta

Descripción

Redis ha identificado y corregido un total de 5 vulnerabilidades que permitían a un atacante ejecutar código de manera remota en sus servidores.

El fallo se debía a diversas vulnerabilidades de gestión de memoria:

La CVE-2026-23479 y la CVE-2026-23631 (vinculada a Lua) permitían la liberación de memoria en uso (use-after-free), mientras que la CVE-2026-25243 facilitaba accesos inválidos mediante el comando RESTORE. Asimismo, las CVE-2026-25588 y CVE-2026-25589 extendían estos riesgos de ejecución de código a los módulos RedisTimeSeries y RedisBloom mediante el procesamiento de datos maliciosos.

Productos afectados

- Las cinco vulnerabilidades afectan a las versiones de Redis OSS/CE y Redis Software hasta la 8.0.6 inclusive.
- Las versiones corregidas incluyen Redis OSS/CE 6.2.22, 7.2.14, 7.4.9, 8.2.6, 8.4.3 y 8.6.3.
- En cuanto a Redis Software, las compilaciones parcheadas incluyen la 8.0.10-64, 7.22.2-79, 7.8.6-253, 7.4.6-279 y 7.2.4-153

Solución

- Se recomienda actualizar los módulos RedisTimeSeries a las versiones v1.12.14, v1.10.24 o v1.8.23, y RedisBloom a las versiones v2.8.20, v2.6.28 o v2.4.23

Referencias

- gbhackers.com
- nist.gov

Actualización en n8n por Prototype Pollution encadenable a RCE

Fecha: 06 de mayo de 2026
CVE: CVE-2026-42231

Crítica

Descripción

Se ha lanzado una actualización de seguridad de n8n para solventar una vulnerabilidad crítica que podría permitir la ejecución remota de código.

Se trata de una vulnerabilidad de tipo Prototype Pollution en el tratamiento de datos XML dentro de n8n, plataforma open source de automatización de *workflows* basada en Node.js.

Esta vulnerabilidad permitiría a un usuario autenticado, enviar contenido XML especialmente diseñado con el objetivo de contaminar el prototipo global de objetos JavaScript.

La explotación exitosa podría permitir al atacante encadenar esta contaminación con otros nodos de la plataforma, como el nodo Git y sus operaciones SSH, llegando a ejecutar código arbitrario en el host afectado.

Productos afectados

Los productos afectados son:

- n8n en versiones anteriores a 1.123.32
- n8n 2.17.x anterior a 2.17.4
- n8n 2.18.x anterior a 2.18.1

El aviso oficial identifica el paquete afectado como npm n8n.

Solución

Se recomienda:

- Actualizar n8n a 1.123.32, 2.17.4, 2.18.1 o versiones posteriores.

Referencias

- incibe.es
- security.snyk.io

Eventos

Infosecurity Europe 2026
2 de junio - 4 de junio

Infosecurity Europe 2026 se celebrará del 2 al 4 de junio de 2026 en Londres, consolidándose como uno de los eventos de referencia en ciberseguridad a nivel europeo. El encuentro reunirá a expertos, CISOs, fabricantes tecnológicos y líderes de la industria para analizar amenazas emergentes, inteligencia artificial aplicada a la seguridad, protección de identidades digitales, Zero Trust y resiliencia empresarial. El evento contará con más de 300 expositores, workshops especializados y sesiones técnicas orientadas a la protección de infraestructuras críticas y entornos cloud.

Enlace

Cyb3rWall 2026
2 de junio - 4 de junio

El Congreso C1b3rWall 2026 se celebrará del 2 al 4 de junio de 2026 en la Escuela Nacional de Policía de Ávila, consolidándose como uno de los mayores encuentros de ciberseguridad y capacitación digital en España. Organizado por la Policía Nacional junto con la Universidad de Salamanca, esta sexta edición se desarrollará bajo el lema “Cibercrimen 3.0”, reuniendo a expertos nacionales e internacionales, fuerzas y cuerpos de seguridad, empresas tecnológicas, universidades y profesionales del ámbito de la seguridad digital.

Enlace

DES 2026 – Digital Enterprise Show
9 de junio - 11 de junio

El Digital Enterprise Show (DES) 2026 se celebrará del 9 al 11 de junio en Málaga, reuniendo a más de 15.000 directivos internacionales y líderes tecnológicos. Aunque centrado en transformación digital e inteligencia artificial, el evento tendrá un importante foco en ciberseguridad, resiliencia digital y protección empresarial frente a amenazas emergentes. Participarán más de 500 expertos internacionales abordando temas como seguridad cloud, IA ofensiva, gobernanza del dato y protección de infraestructuras digitales.

Enlace

CCI – La Voz de la Industria Asturias
18 de junio

El Centro de Ciberseguridad Industrial celebrará en Gijón el evento ‘La Voz de la Industria Asturias’, una jornada especializada en ciberseguridad industrial y protección de infraestructuras críticas. El encuentro reunirá a expertos OT, responsables de seguridad industrial y empresas del sector energético, manufacturero y tecnológico para debatir sobre amenazas a entornos industriales, continuidad operativa y regulación europea en materia de ciberseguridad.

Enlace

Recursos

- **NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick Start Guide (QSG) – NIST**

Publicado por el National Institute of Standards and Technology (NIST), este recurso ofrece una guía práctica para integrar la gestión del riesgo de ciberseguridad dentro de la estrategia global de riesgo empresarial (ERM). El documento está orientado a responsables de seguridad, directivos y equipos de gobierno corporativo que buscan alinear la resiliencia digital con los objetivos estratégicos de negocio. La guía profundiza en aspectos como la gobernanza del riesgo, la definición de apetito de riesgo, la gestión de riesgos tecnológicos asociados a IA, IoT, OT y cadena de suministro, así como la asignación de responsabilidades organizativas en materia de ciberseguridad. Se trata de un recurso especialmente útil para organizaciones que trabajan bajo marcos NIST o que buscan adaptar sus programas de seguridad a modelos de gestión empresarial más maduros.

Enlace

- **The State of Cloud and AI Security 2025 – Cloud Security Alliance (CSA)**

Publicado por la Cloud Security Alliance en colaboración con Tenable, este informe analiza cómo las organizaciones están adaptando sus estrategias de seguridad frente al crecimiento acelerado de entornos híbridos, multicloud e inteligencia artificial. Basado en una encuesta global a más de 1.000 profesionales, el documento identifica las principales brechas entre adopción tecnológica y madurez en ciberseguridad. El informe aborda riesgos asociados a IA generativa, gestión de identidades, protección de datos en cloud, exposición de configuraciones erróneas y automatización de amenazas. Además, ofrece recomendaciones prácticas para fortalecer la resiliencia organizativa y mejorar la visibilidad sobre superficies de ataque cada vez más complejas.

Enlace

- **CIS Critical Security Controls v8 – Center for Internet Security (CIS)**

Los CIS Critical Security Controls v8 constituyen un conjunto de buenas prácticas priorizadas para ayudar a organizaciones a prevenir, detectar y responder ante amenazas cibernéticas. El marco está diseñado para ofrecer controles accionables y medibles que permitan reducir riesgos de forma progresiva y efectiva. La guía incluye recomendaciones sobre gestión de activos, protección de identidades, monitorización continua, hardening de sistemas, seguridad cloud, respuesta ante incidentes y formación en concienciación. Su enfoque práctico y escalable lo convierte en uno de los estándares más utilizados por empresas y organismos públicos para estructurar programas de ciberseguridad.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com