EL 80% DE LOS CIBERATAQUES A PLANTAS INDUSTRIALES SE ORIGINAN EN REDES IT DESPROTEGIDAS Y CONECTADAS A ENTORNOS OPERACIONALES

* Según el Cyber Defense Center de Minsait, en 2025 se han identificado 23 grupos de amenazas activos dirigidas a entornos industriales, un incremento del 15% respecto al año 2022.
* Ocho de cada diez incidentes en plantas industriales se originan en redes TI mal segmentadas, y los ataques más comunes incluyen phishing dirigido a personal operativo, exposición de interfaces industriales sin autenticación y accesos no autorizados a dispositivos críticos como PLCs y RTUs.
* Los sectores más atacados en México son: energía (34%), agua y saneamiento (21%), manufactura (19%), salud (13%) y logística (8%).

**Ciudad de México, 5 de agosto de 2025.** – En México, los ciberataques dirigidos a entornos operacionales (OT) han experimentado un aumento significativo en los últimos años. En 2024, cerca del 25% de las organizaciones industriales en el país sufrieron ataques que supusieron una parada en la producción y la operación. La principal causa de esta tendencia, que se inicia a partir de la digitalización y de la convergencia de IT y OT en este ámbito, es una segmentación de redes no adecuada . Es decir, los entornos OT se conectan a redes y sistemas corporativos que no están protegidos y, por tanto, suponen una vía de entrada a ciberataques.

En un contexto donde las plantas industriales, hospitales y sistemas energéticos están cada vez más conectados, la seguridad ha dejado de ser un tema exclusivo de las áreas de TI para convertirse en una prioridad estratégica en las organizaciones. “La convergencia entre IT y OT no es una opción; hoy, es una necesidad de negocio. Pero, con ella, la superficie de ataque se ha ampliado exponiendo sistemas legacy e inseguros, entornos complejos y poca visibilidad para la organización. que ponen en riesgo desde la producción hasta vidas humanas”, advierte Erik Moreno, director de Minsait Cyber en México.

Según cifras del Cyber Defense Center de Minsait, en 2025 se han identificado 23 grupos de amenazas activas dirigidas al entorno industrial, frente a 18 identificados durante 2022. Este aumento del 15% evidencia el creciente interés de los atacantes en vulnerar sistemas de control y gestión de procesos, como SCADA o PLC, especialmente donde no hay una adecuada segmentación entre redes IT y OT. De hecho, el 80% de los incidentes registrados en ambientes industriales tienen su origen en redes TI mal protegidas.

Los sectores más afectados en México son energía (34%), agua y saneamiento (21%), manufactura (19%), salud (13%) y logística (8%). Los ataques más comunes incluyen phishing dirigido a personal de planta, exposición de interfaces industriales sin autenticación y accesos no autorizados a dispositivos críticos como PLCs y RTUs. Sin embargo, el verdadero punto de vulnerabilidad es la cadena de suministro, donde los atacantes buscan infiltrarse a través de terceros menos protegidos para llegar al núcleo operacional de grandes compañías.

“Hoy, la resiliencia operacional no solo compete al CIO o al CISO. También es prioridad para directores de planta, responsables de mantenimiento y la alta dirección”, explicó Moreno. “Hablamos de mantener operaciones críticas sin interrupciones. Eso, en sí mismo, es ciberseguridad”.

**Un enfoque industrial centrado en la resiliencia**

Para responder a este escenario, Moreno plantea **cuatro pilares** estratégicos que contribuyen a fortalecer la protección de los entornos OT:

1. Alinear la ciberseguridad con los objetivos operacionales, adoptando un enfoque donde no interrumpa la producción, sino que sea un habilitador de su continuidad.
2. Consolidar la visibilidad de activos y riesgos en plataformas unificadas, que permita priorizar y actuar con eficiencia.
3. Blindar los sistemas “*legacy”* que no pueden actualizarse fácilmente y protegerlos mediante controles compensatorios.
4. Simplificar y centralizar la gobernanza, integrando OT e IT en una estrategia global dentro de la organización.

Sobre estos principios, la estrategia de ciberseguridad industrial debe apoyarse en capacidades especializadas que combinen el conocimiento profundo del entorno con tecnología adaptada al contexto operacional .

“Ya no basta con tener un Centro de Operaciones de Seguridad (SOC, por sus siglás en inglés) estándar. Se requiere añadir capacidades OT e inteligencia adaptada al lenguaje del entorno industrial, monitoreo constante de protocolos específicos, identificación de comportamientos anómalos y respuestas automatizadas que no interrumpan los procesos”, subraya Moreno. Y añade “nuestro servicio de detección y respuesta avanzada, Smart MDR, está preparado para actuar en este ámbito, detectando incidentes en 15 minutos y reduciendo las alertas falsas a tan sólo un 2% y el número de alertas de escaso valor en más del 80%.A partir de soluciones personalizadas y punteras, las organizaciones industriales pueden contar con una protección unificada, ágil y contextualizada que reduce riesgos operacionales, reputacionales y económicos. “El verdadero valor está en que la tecnología se adapte al entorno, y no al revés. Solo así se puede garantizar una respuesta efectiva”, según el director de Minsait Cyber en México

**La resiliencia como nuevo estándar de negocio**

Erik Moreno subraya que, la ciberseguridad OT no puede seguir siendo un apéndice del mundo TI. Requiere su propio enfoque, cultura y herramientas. De su correcta implementación depende no solo la protección de activos, sino la continuidad misma de las operaciones industriales.

En este sentido, el directivo de Minsait Cyber indica que en los entornos de producción es necesario adoptar una estrategia integral que contemple todo el ciclo de vida de los activos; establecer una gobernanza clara entre IT y OT; priorizar la segmentación de redes, la gestión de accesos remotos y la protección de endpoints industriales; invertir en herramientas diseñadas para OT que permitan detección y respuesta efectiva sin interrumpir la operación; y fortalecer la cultura de ciberseguridad entre los equipos.

“Hoy más que nunca, asegurar la continuidad operacional exige un modelo de protección 360º, basado en inteligencia contextual, automatización y coordinación entre equipos expertos. En este nuevo escenario, OT, IT y la gestión de identidades definen la nueva resiliencia que , ya no es una meta técnica,es una ventaja competitiva”, concluye Moreno.

**Acerca de Minsait Cyber**

Minsait Cyber (minsaitcyber.com) es la compañía del Grupo Indra especializada en ciberseguridad, líder en España y Portugal, tanto en volumen de facturación como en talento experto, con más de 2.000 especialistas. Ante los desafíos y amenazas de seguridad que plantea la digitalización de las organizaciones, proporciona respuestas efectivas a través de una oferta end to end que incluye servicios y soluciones de ciberseguridad 360º e Identidad Digital, para minimizar el riesgo y maximizar la protección de sus negocios. Su oferta de valor se basa en tres pilares principales: servicio integral, cobertura internacional, y conocimiento y especialización sectorial. La pertenencia a Indra Group, holding empresarial que promueve el progreso tecnológico y cuenta con operaciones comerciales en más de 140 países, proporciona a Minsait Cyber un profundo conocimiento de las diferentes industrias, así como una sólida presencia global.

**Acerca de Minsait**

Minsait ([www.minsait.com](http://www.minsait.com)) es la compañía del Grupo Indra líder en nuevos entornos digitales y tecnologías disruptivas. Presenta un alto grado de especialización, amplia experiencia en el negocio tecnológico avanzado, conocimiento sectorial y un talento multidisciplinar formado por miles de profesionales en todo el mundo. Minsait está a la vanguardia de la nueva digitalización con capacidades punteras en inteligencia artificial, cloud, ciberseguridad y otras tecnologías transformadoras. Con ello, impulsa los negocios y genera grandes impactos en la sociedad, gracias a una oferta digital de servicios de alto valor añadido, soluciones conectadas a medida para todos los ámbitos de actividad y acuerdos con los socios más relevantes del mercado.

**Acerca de Indra Group**

Indra Group ([www.indracompany.com](https://www.indracompany.com/)) es un holding empresarial que promueve el progreso tecnológico, del que forman parte Indra, una de las principales compañías globales de defensa, tráfico aéreo y espacio; y Minsait, líder en nuevos entornos digitales y tecnologías disruptivas. Indra Group impulsa un futuro más seguro y conectado a través de soluciones innovadoras, relaciones de confianza y el mejor talento. La sostenibilidad forma parte de su estrategia y de su cultura, para dar respuesta a los retos sociales y ambientales presentes y futuros. A cierre del ejercicio 2024, Indra Group tuvo unos ingresos de 4.843 millones de euros, presencia local en 46 países y operaciones comerciales en más de 140 países

Contacto de Comunicación

**Karla Zepeda**

**Kzepeda@indracompany.com**

**+52 55 5072 8304**