38

Resiliencia Operativa en Sectores Críticos

Un valor esencial para la industria

El contexto geopolítico, la creciente especialización de los atacantes y el cambio de paradigma en Operational Technologies (OT), impulsado por la integración de nuevas tecnologías en los sistemas de producción, como por ejemplo, inteligencia artificial (IA), Cloud e Internet of Things (IoT), incrementan su exposición al riesgo, convirtiéndolos en objetivos cada vez más atractivos para ser atacados.

El aumento de los ciberataques, dirigidos a sectores críticos como la energía, el agua, el transporte, la alimentación, el sector espacial, la defensa y la salud, representa una amenaza significativa para la continuidad operativa. Estos incidentes no solo interrumpen las operaciones, sino que también pueden causar daños físicos a la infraestructura con impactos económicos y sociales.

Las consecuencias de un incidente pueden ser graves y de amplio alcance. Van desde pérdidas financieras significativas, paralización de la operación hasta daños materiales, riesgos para las personas y pérdida reputacional. Por ello, la gestión y mitigación de estos riesgos se ha convertido en una prioridad estratégica para las organizaciones.

El reciente ciberataque sufrido por parte de una empresa del sector de la automoción el pasado agosto del 2025, tuvo un coste estimado para la economía británica de 2.550 millones de dólares y afectó a más de 5.000 organizaciones en todo país. La producción estuvo paralizada casi seis semanas, reanudándose a principios de noviembre, lo que muestra el impacto económico y operativo de estos ataques.

Algunos otros casos relevantes son el sabotaje atribuido a ciberatacantes rusos contra una planta de tratamiento de agua en Texas (2024) o un ataque de ransomware a un oleoducto, que forzó el cierre temporal del principal oleoducto de la Costa Este de Estados Unidos durante seis días.

¿EN QUÉ CONSISTEN LAS TECNOLOGÍAS DE OPERACIÓN (OT)?

Cuando hablamos de los sistemas OT, nos referimos a los sistemas responsables de gestionar y controlar las operaciones industriales. Estos sistemas comprenden diversos tipos de hardware y software que permiten la monitorización y la automatización de los procesos productivos. Entre sus componentes principales se encuentran:

- Sistemas de Control industrial (ICS) que supervisan y controlan la infraestructura.
- Los sistemas SCADA que recopilan datos en tiempo real de sensores y dispositivos de campo.
- Los Controladores Lógicos Programables (PLCs), entre otros.

Estos sistemas garantizan que las operaciones industriales se ejecuten de forma eficiente, fiable y segura.

¿POR QUÉ LOS ENTORNOS INDUSTRIALES SON TAN CRÍTICOS?

Los entornos industriales constituyen la base de las infraestructuras críticas y servicios esenciales. Su operación

Aníbal Díaz
Sr. Manager OT Cyber Security

es indispensable para mantener la estabilidad económica y social.

Además, se diferencian significativamente de los sistemas tradicionales (IT) en ciertos aspectos relevantes, como son:

- La indisponibilidad de estos sistemas es inaceptable, ya que deben opera 24x7.
- El equipamiento suele ser antiguo y carece de medidas de seguridad desde su diseño.
- Estos sistemas están diseñados para operar de manera continuada, en condiciones exigentes y adversas.
- La aplicación de actualizaciones o parches en muchos casos es difícil o casi imposible, por lo que incrementa su vulnerabilidad.

¿CUÁL ES EL IMPACTO DE UN CIBERATAQUE EN UN ENTORNO OT?

Un ciberataque puede afectar no solo a los sistemas, sino también a las personas, al medio ambiente y a la producción. Algunos de los principales impactos son:

§ **Daños a equipos, instalaciones y productos:** Un ciberataque puede causar fallos o daños físicos en maquinaria e infraestructuras y deteriorar materias primas o mercancías.
§ **Interrupción de las operaciones y la producción:** Los atacantes pueden detener los sistemas de control, causando retrasos y pérdidas económicas.
§ **Incumplimiento legal y regulatorio:** Estos sistemas están sujetos a regulaciones estrictas en materia de ciberseguridad; un ciberataque puede derivar en incumplimientos legales, multas y sanciones.
§ **Daños personales, materiales y medioambientales:** En industrias con procesos peligrosos, un ciberataque que altere el funcionamiento seguro de los sistemas puede poner en riesgo la vida y la salud de los trabajadores o personas cercanas.
§ **Modificaciones en la calidad del producto:** Los atacantes pueden interferir en los parámetros de producción, alterando las condiciones de fabricación, generando productos que no cumplen con los estándares.
§ **Interrupción de servicios esenciales:** Los sistemas que gestionan servicios esenciales como agua, energía, transporte o salud, un ataque que interrumpa estos servicios puede afectar a la población generando problemas sociales y económicos.

¿CUÁL ES LA MEJOR ESTRATEGIA PARA AFRONTAR LOS RIESGOS EN OT?

El enfoque que proponemos es una visión estratégica que integre tanto los riesgos IT como OT.

Para ello, recomendamos emplear metodologías y acciones, que alineen el conocimiento técnico IT/OT del sector con una perspectiva financiera del riesgo, como son:

- La realización de evaluaciones de seguridad y riesgos periódicas en sistemas y arquitectura OT, para obtener una visión clara del nivel de madurez y del estado de la seguridad, basada en las mejores prácticas internacionales, como son ISA/IEC 62443 o NIST, entre otras.
- La alineación con estándares nacionales y europeos relevantes, como la NIS2.
- La definición y caracterización de escenarios de riesgo OT específicos.
- La cuantificación financiera del impacto potencial de dichos escenarios de riesgo, facilitando la toma de decisiones informadas.
- La gestión del riesgo 360º: desde los planes de acción hasta el análisis y diseño de coberturas adecuadas para la transferencia del riesgo de ciberseguridad OT.

Esta aproximación permite beneficiarse a las empresas de una visión estratégica para reducir, mitigar y transferir el riesgo, mediante la definición de planes de acción con objetivos y acciones concretas o mediante pólizas, con condiciones adaptadas a sus necesidades y obteniendo la visión de cual es el impacto financiero en un evento de ciberseguridad.