Cyber-Physical Risks: When Data Attacks Meet Physical Safety Stats and Facts – Spanish

HECHOS

- **Sistemas de Control Comprometidos:** Los ciberataques contra los sistemas de control industrial pueden alterar el comportamiento de los equipos, lo que puede provocar movimientos peligrosos, fallos en las paradas de emergencia o liberaciones incontroladas de energía.
- **Acceso Remoto no Autorizado:** Los intrusos que logran acceder a equipos conectados o a sistemas de seguridad pueden anular los controles y desactivar las protecciones sin que los trabajadores se den cuenta.
- **Manipulación de Sensores y Datos:** Los datos alterados o falsos de los sensores pueden inducir a error a los operadores, lo que da lugar a decisiones inseguras y a un reconocimiento tardío de los peligros.
- **Fallo de los Sistemas de Apagado y Seguridad:** Los ataques dirigidos a los enclavamientos de seguridad o a los sistemas de apagado de emergencia pueden impedir que se activen las protecciones críticas durante los incidentes.
- **Respuesta Tardía ante Peligros:** La interrupción de los sistemas de comunicación puede ralentizar la respuesta de emergencia, lo que aumenta la gravedad de los incidentes.
- **Dependencia de los sistemas Conectados:** La mayor dependencia de los sistemas digitales significa que las fallas o las brechas pueden afectar directamente las operaciones físicas y la seguridad de los trabajadores.
- **Error Humano bajo Estrés Cibernético:** La confusión durante los incidentes cibernéticos puede llevar a acciones incorrectas, lo que aumenta el riesgo de lesiones físicas.

ESTADÍSTICAS

- En Estados Unidos, aproximadamente el 32 % de las organizaciones industriales informaron de incidentes cibernéticos que afectaron a los sistemas de tecnología operativa (OT), lo que aumentó el riesgo de repercusiones en la seguridad física (IBM Security e informes del sector, 2023-2024).
- Los datos de EE. UU. muestran que más del 40 % de los ciberataques dirigidos a infraestructuras críticas implican intentos de interrumpir operaciones físicas, incluidos los sectores de la energía, la manufactura y los servicios públicos (informes de la CISA y el DHS, 2022-2024).
- En América del Norte, alrededor del 25 % de las organizaciones informaron que los incidentes cibernéticos tuvieron consecuencias directas operativas o

relacionadas con la seguridad, incluyendo paradas de equipos o condiciones inseguras (SANS Institute, 2023).

- Los informes de EE. UU. indican que más del 50 % de los incidentes de ciberseguridad industrial implican sistemas de control comprometidos, lo que puede afectar directamente a la maquinaria y a la seguridad de los trabajadores (Informe de ciberseguridad industrial de Dragos, 2023-2024).
- En Canadá, aproximadamente el 30 % de las organizaciones de infraestructura crítica informaron de incidentes de ciberseguridad que afectaron a las operaciones, incluyendo interrupciones que podrían afectar a la seguridad de los trabajadores (Public Safety Canada, 2022–2024).
- Los datos de EE. UU. muestran que los ataques de ransomware representaron más del 20 % de los incidentes cibernéticos en los sectores industriales, causando a menudo paradas y condiciones operativas inseguras (Informe del FBI IC3, 2023).