Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Stats and Facts – Spanish

HECHOS

- **La Confiabilidad de un Sensor Depende de la Calidad de sus Datos:** un sensor mal calibrado, comprometido o que no funciona correctamente no reporta una condición insegura, sino que solo reporta un número. Los trabajadores que actúan basándose en datos falsos se enfrentan a peligros que son invisibles hasta que se convierten en lesiones.
- **El Acceso Remoto es una Puerta de Doble Sentido:** los sistemas que permiten a los usuarios autorizados monitorear las condiciones de forma remota también pueden ser accedidos por personas no autorizadas. Sin una autenticación adecuada y sin cortafuegos, el acceso remoto es un canal abierto a todos los sistemas críticos para la seguridad a los que se conecta.
- **La Integridad de los Datos es un Problema de Seguridad:** Las lecturas de los sensores alteradas o falsificadas pueden ocultar condiciones peligrosas —niveles bajos de oxígeno, altas concentraciones de sustancias químicas, fallas en los equipos— hasta que sea demasiado tarde para que un trabajador pueda reaccionar.
- **Los Dispositivos del IoT Suelen estar sin Administrar:** Muchos sensores industriales del IoT no reciben parches regularmente ni se monitorean en busca de comportamientos anormales, lo que crea vulnerabilidades persistentes en los sistemas de los que dependen los trabajadores para obtener información de seguridad.
- **La Automatización Puede Fallar de Manera Silenciosa:** Un sistema de seguridad comprometido o mal configurado puede seguir pareciendo funcional sin ofrecer protección real. Una luz verde en un tablero de control no equivale a una condición de seguridad confirmada.

ESTADÍSTICAS

- El coste medio de una filtración de datos en el sector manufacturero alcanzó los 4,97 millones de dólares en 2024, sin incluir las multas reglamentarias ni las pérdidas por interrupción de la actividad empresarial, según un estudio sobre ciberseguridad industrial.
- El 77 % de las empresas industriales se encuentra aún en las fases iniciales de la implementación de la seguridad de la tecnología operativa (OT), y ninguna de ellas está totalmente protegida, según un estudio del sector sobre seguridad de OT/IoT.
- Se prevé que en 2029 habrá 15 140 millones de dispositivos IoT instalados en

todo el mundo, lo que ampliará significativamente la superficie de ataque en entornos críticos para la seguridad.

- El 5 de febrero de 2021, un pirata informático obtuvo acceso remoto no autorizado a la planta de tratamiento de aguas de Oldsmar (Florida) y aumentó la concentración de hidróxido de sodio de 100 a 11 100 partes por millón, un nivel capaz de provocar quemaduras químicas graves o la muerte. Un trabajador atento se percató de ello y revirtió el cambio antes de que llegara a los consumidores.
- El sector manufacturero fue el más afectado por el ransomware en 2025, con un aumento interanual del 58 % en el número de víctimas entre las organizaciones industriales, según GuidePoint Security.
- 34 de las 39 vulnerabilidades del IoT más explotadas se conocen desde hace más de tres años de media, lo que significa que la mayoría de los ataques exitosos aprovechan debilidades ya documentadas y evitables, según el Informe sobre seguridad de dispositivos IoT de 2024 de Asimily.