MARSH

# ICS/SCADA cyber threat landscape and best practices

Los entornos OT/ICS operan plantas, energía, petróleo y gas, minería, manufactura e infraestructura crítica. A diferencia de TI, en OT un incidente puede traducirse en interrupción física, parálisis productiva, impacto en seguridad y pérdidas financieras. Para la Dirección, el riesgo OT debe gestionarse como una prioridad de continuidad y resiliencia empresarial.

## 1 OT/ICS protege operaciones críticas

OT gestiona operaciones industriales. Un incidente puede detener producción, comprometer seguridad y afectar infraestructura crítica.

## 2 Latinoamérica enfrenta mayor exposición

79% de organizaciones industriales y de infraestructura crítica en LATAM experimentan ransomware; solo 7 de 32 países tienen planes de protección.

## 3 TI, terceros y accesos remotos son vías de entrada

Más de 200 initial access brokers apuntaron a 17 países de LATAM en 2025. VPN, proveedores y accesos remotos son puntos críticos.

## 4 La falta de visibilidad aumenta el riesgo

Propiedad fragmentada, activos no inventariados, sistemas heredados, parches irregulares y bajo monitoreo dificultan detectar y responder.

## 5 Los controles OT deben priorizar resiliencia

SANS recomienda cinco controles críticos: respuesta a incidentes, arquitectura defendible, monitoreo, acceso remoto seguro y gestión de vulnerabilidades por riesgo.