



# CIBERSEGURIDAD PARA TECNOLOGÍAS OPERACIONALES

Es un conjunto de **servicios administrados** y de **consultoría en ciberseguridad** para proteger de forma integral los **ambientes industriales**, diseñados para evaluar el **nivel de seguridad**, generar visibilidad de los elementos, así como para **monitorearlos** y **protegerlos** ante posibles ataques.

## BENEFICIOS



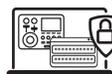
**Obtén visibilidad completa** de cada uno de los dispositivos conectados a la red industrial



**Reduce el riesgo de posibles cambios** (configuración, flujo de comunicación, etc.) en los dispositivos del ambiente industrial.



**Incrementa la seguridad** mediante la segmentación la red TO\*



**Permite el acceso seguro a las configuraciones** de los dispositivos TO.



**Maximiza la continuidad del negocio** al reducir los posibles incidentes de seguridad a través del monitoreo continuo.



**Apoya en las auditorías de cumplimiento** de las regulaciones del sector, así como en la alineación de políticas y procedimientos.

## ¿CÓMO FUNCIONA?

### Consultor Especializado

- Entrevista al cliente.
- Analiza el caso de uso: Visibilidad, Protección y Detección, Auditoría de Cumplimiento, Evaluación de Riesgos, Etc.
- Elaboración de estrategia integral.

### Selección de servicios de interés

- Selección de servicios.
- Desarrollo por fases.
- Definición de alcances, integraciones y particularidades.

### Implementación y operación de los servicios seleccionados

- Contextualización y descubrimiento.
- Segmentación de Red.
- Configuración de políticas.
- Auditorías de cumplimiento.
- Generación de campañas.
- Ejecución de análisis de vulnerabilidades y pruebas de penetración.

\*Al hablar de TO (Tecnologías Operacionales) nos referimos al comúnmente conocido término "Operational Technologies" (OT por sus siglas en inglés).

# SERVICIOS DE CIBERSEGURIDAD PARA TECNOLOGÍAS OPERACIONALES

## Detección y Protección

- Monitoreo de seguridad de red.
- Detección de amenazas avanzadas en terminales.

## Análisis de Vulnerabilidades y Pruebas de Penetración

- Identificación de vulnerabilidades.
- Explotación de vulnerabilidades.

## Visibilidad

- Identificación e inventario de activos.
- Mapeo de los flujos y componentes.

## Auditoría de Cumplimiento y Marco Normativo

- Auditoría de cumplimiento de regulaciones del sector.
- Elaboración de políticas y procedimientos por sector.

## Programa de Concientización

- Planeación, diseño y despliegue de campañas de concientización.
- Disminución del riesgo, con cambio de conducta de los colaboradores para la disminución del riesgo.

## Evaluación de riesgos

- Evaluación de riesgos alineada a las metodologías: NIST SP 800-82, IEC 62443, ISO 27005
- Evaluación integral de riesgos disminución del riesgo.

## OFERTA COMERCIAL

La vía de contratación es a través del ejecutivo de ventas consultivas de ciberseguridad

### Modalidad a la Medida



Servicios a la medida

Dirigida para proteger tecnologías operacionales en sectores:



Data Centers



Salud



Industria



Retail



Energía



Otros

## ¿POR QUÉ TELMEX-SCITUM?



- Especialistas experimentados con más de 750 colaboradores, más de 1,000 certificaciones en mejores prácticas y tecnologías de fabricantes líderes en ciberseguridad.



- Protegiendo a más de 1,300 clientes desde 1998, casos de éxito en todos los sectores.



- Eficiencia Operativa con un SOC de nueva generación. Operación alineada a estándares internacionales y mejores prácticas de la industria.



- Visibilidad Única, con más de 120,000 puntos de visibilidad propio, con el Cibecosistema de colaboración más robusto de LATAM.



- Un portafolio integral con más de 40 servicios clasificados en 6 grupos. Oferta amplia que incluye servicios de consultoría, auditoría y operación de la seguridad con un enfoque holístico en gente, procesos y tecnología.



- Máximas certificaciones con + de 50 socios de negocio tecnológicos.