GESTIÓN DE CIBERRIESGOS DE TERCERAS PARTES

Este servicio **analiza** y **gestiona ciber-riesgos de tu empresa** y de **terceras partes** que conforman tu **ecosistema** como **proveedores o aliados de negocio**, con la finalidad de obtener **métricas de riesgo** por cada compañía, así como la **generación** de un **indicador** general de tu organización con base en el **nivel** de **ciberseguridad**

BENEFICIOS

Te permitirá obtener una **postura de ciberseguridad** desde una perspectiva externa:

- Identificación de amenazas potenciales
- Establecer líneas de acción oportunas
- Identificación de vulnerabilidades
- Visibilidad de proveedores y aliados de negocio

Obtendrás información rápidamente, ya que la información se encuentra en el ciberespacio.

Operarás de manera NO intrusiva, no requieres gestionar permisos de 3ros (proveedores, distribuidores y concesionarios) para llevar a cabo el análisis e identificar sus riesgos.

DS / Gestión de Ciberriesgos de Terceras Partes / JUN24 / V1

¿CÓMO FUNCIONA?

A través del monitoreo continuo del ciberespacio, se lleva a cabo una medición para generar una postura de ciberseguridad de tus terceras partes, y por medio de la recopilación de información de grandes fuentes de datos públicas, analítica avanzada de datos y algoritmos de aprendizaje automático, se generará una puntuación de riesgo única la cual se compone de las siguientes categorías:

1. Actividad maliciosa
2. Actividad anómala
3. Vulnerabilidades
4. Fuentes de información propietaria
5. Listas Negras
6. Gobierno de terceros

Más información en **telnor.com/empresa**, consulta a tu **Ejecutivo de Cuenta** o llama al **800 123 1212**

Scitum

TELNOR
tu mundo es posible

COMPONENTES DEL SERVICIO

ETAPA 1

Diagnóstico de Ciberpostura (para 3eros)

Análisis de la información recolectada desde el ciberespacio tanto de la empresa como de los terceros.

ETAPA 2

Valoración de la situación actual

Identificación de los riesgos asociados a los terceros, determinación del impacto al negocio o las consecuencias y priorización de estos.

ETAPA 3

Definición de iniciativas de seguridad

Informe final de resultados, identificación de acciones inmediatas, definición de las iniciativas a corto, mediano y largo plazo.

ETAPA 4

Gestión de los ciberriesgos de terceros

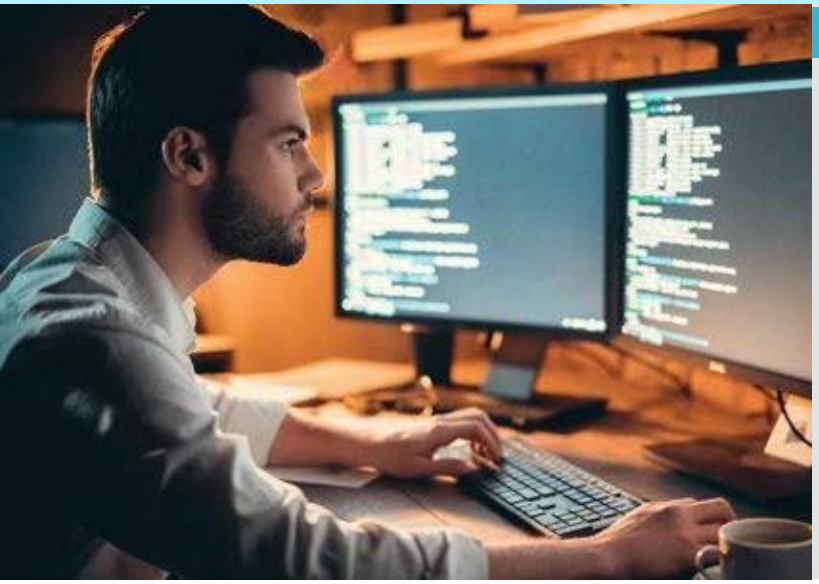
Monitoreo de indicadores por categoría de riesgo, notificación de cambio en los umbrales definidos de riesgo y revisiones periódicas.

OFERTA COMERCIAL

El servicio se ofrece como proyecto a la medida.

Servicios **a la medida**

1. **INTEGRACIÓN DE 3ras PARTES**
2. **MONITOREO CONTINUO**
3. **INVESTIGACIÓN**
4. **REMEDIACIÓN DE CIBERRIESGOS**
5. **OBSERVACIÓN Y DIAGNÓSTICO FINAL**



¿POR QUÉ TELNOR-SCITUM?

- **Más de 22 años de experiencia**
- **Personal especializado**. Más de 650 colaboradores que acreditan más de 1,500 certificaciones en mejores prácticas y tecnologías de fabricantes líderes en ciberseguridad.
- **Operación de clase mundial**, alineada a estándares internacionales metodologías propias, marcos de referencia y mejores prácticas.
- **Las recomendaciones para la mitigación de vulnerabilidades** identificadas se hacen desde el punto de vista de tecnología, procesos y gente.
- **Realizamos un conjunto de actividades** de **manera coordinada y recurrente** para dirigir y controlar una organización con el enfoque a riesgos, con el fin de tomar decisiones informadas y priorizar el usos de los recursos.

Más información en **telnor.com/empresa**, consulta a tu **Ejecutivo de Cuenta** o llama al **800 123 1212**

Scitum | TELNOR tu mundo es posible