Centros de operación de ciberseguridad

Sus activos digitales en manos expertas

EY
Shape the future with confidence

Nuestro modelo de servicio híbrido integra especialistas en operaciones de ciberseguridad (SOC/CERT) y threat hunting, junto con expertos en los principales estándares internacionales en seguridad de la información (CIS, NIST, PCI, CSCF Swift),

A continuación, presentamos los aspectos diferenciales de nuestra solución de servicios profesionales que ofrecen un valor único:

- Industralización y mejora de la eficiencia
- Ciberseguridad de próxima generación (ciberinteligencia)
- Equipo flexible de especialistas
- Plan de transformación y evolución
- Cuadros de mandos a todos los niveles
- Evaluaciones de resiliencia

¿Qué hace único nuestro enfoque en ciberseguridad?

Gestión de la prestación de servicios

Gestión de la prestación de servicios	Gestión de la evolución del servicio	Cuadros de mando e informes

Servicios a ofrecer

Ataques	Incidentes	Vulnerabilidades	Amenazas
Operaciones de defensa cibernética 24x7	**Respuesta a incidentes cibernéticos 24x7**	**Gestión de vulnerabilidades**	**Inteligencia de amenazas**
Nivel 1/2	Nivel 3	Equipo rojo	Inteligencia de amenazas productos
Triaje y gestión de alertas	Análisis Técnico e Investigaciones	Análisis de vulnerabilidades	Caza de amenazas
Gestión de Playbooks	Manejo de incidentes	Gestión de vulnerabilidades	Estrategias de respuesta temprana a amenazas

Entrega de soluciones

Ingeniería cibernética 24x7

Gestión de soluciones de nivel 1/2	Evolución de la solución e implementación de casos de uso	Implementación de soluciones y arquitectura

Automatización de SOC

Plataforma de orquestación y automatización	RPA (en inglés)	Secuencias de comandos para la automatización

Nuestra experiencia

Especialista SOC:

- Utiliza los principales estándares.
- Diseña implementa y opera servicios SOC de extremo a extremo.

Alcance integral de los servicios:

- Servicios y soluciones que se adaptan a su propósito.

Transformación empresarial habilitada por la tecnología:

- Facilitadores: SOAR / orquestación, aprendizaje automático, análisis y automatización.
- Tecnología de última generación.
- Ecosistema de alianzas.

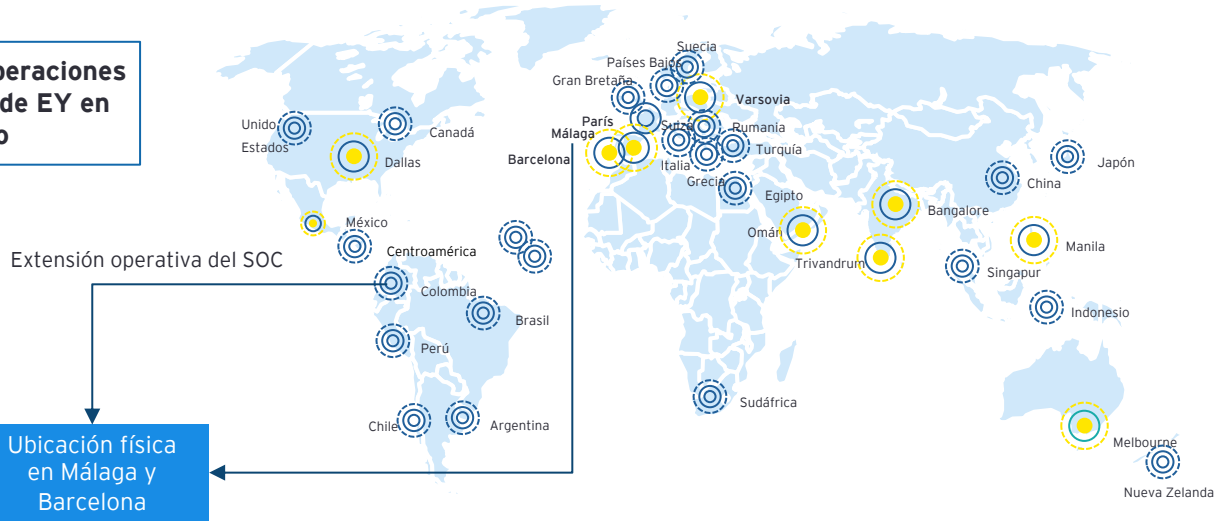
Capacidades globales con entrega local:

- Gente.
- Capacidad.
- Ecosistema de servicios.
- Soluciones con contexto de negocio.

Actúar como puente:

- Ayudar a construir puentes entre la empresa y la organización de seguridad.

Centros de operaciones de seguridad de EY en todo el mundo



EY: socio de ciberseguridad de extremo a extremo

Somos especialistas en seguridad con amplia experiencia en proyectos estratégicos de ciberseguridad, así como en servicios operativos, aportando valor desde el nivel estratégico hasta la implantación y aplicación.

SOC Ing. & Transf.

Implementación y operaciones de SOC y tecnología

- Gestión de SOC.
- Diseño e implementación de SOC.
- Evaluación y mejora de la madurez del SOC.
- Capacidad de los sistemas de seguridad (es decir, SIEM, EDR, IPS).
- Operación y despliegue de herramientas cibernéticas.
- Tecnología y arquitectura de ciberseguridad.
- Informe y cuadro de mando.
- Caso de uso y fábrica de automatización.

SOC 24X7 (L1 y L2)

Detección de ataques y amenazas potenciales

- Monitoreo de alertas 24x7 :
- SIEM-As-A-Service basado en la tecnología IBM Qradar – Splunk – Sentinel.
- Operación del propio SIEM del cliente (Splunk, Elastic, Sentinel, otros).
- Casos de uso de detección basada en amenazas.
- Triaje de alertas, gestión del proceso de triaje y escalamiento.
- Revisión, ajuste y mejora de casos de uso.
- Monitorización específica de activos críticos.
- Gestión posterior a la clasificación de acciones de resolución rápidas/sencillas para abordar alertas de bajo riesgo.

Respuesta a incidentes (L3)

Investigación y recuperación de incidentes

- Triaje y análisis de incidentes.
- Contención y erradicación.
- Remediación y recuperación.
- Investigación de incidentes cibernéticos.
- Análisis de malware.
- Evaluación y soporte de violaciones de datos.
- Forense.

TEM / CTI

Fortalecimiento de la protección y las alertas tempranas

- Escaneo e identificación de vulnerabilidades de activos.
- Ciclo de vida de la gestión de vulnerabilidades.
- Investigación de vulnerabilidades cibernéticas.
- Diseño y planificación de remediaciones.
- Equipos purple/red y ciberejercicios.
- Informes de vulnerabilidades y KPIs.
- Fuentes de inteligencia de amenazas e IoC.
- Productos de inteligencia de amenazas.
- Detección y respuesta a fugas de datos/ciberocupación.
- Amenaza – táctica o técnica – caza.

Contactos clave

Miguel Caldentey
Socio
miguel.caldentey@pa.ey.com

Enrique Mendoza
Senior Manager
enrique.mendoza.diaz1@pa.ey.com

EY | Construyendo un mejor mundo de negocios

EY existe para construir un mejor mundo de negocios, ayudando a crear valor a largo plazo para sus clientes, su gente y la sociedad en general, así como también para construir confianza en los mercados de capitales. Por medio de datos y tecnología, los equipos diversos e incluyentes de EY, ubicados en más de 150 países, brindan confianza a través de la auditoría y ayudan a los clientes a crecer, transformarse y operar. El enfoque multidisciplinario en auditoría, consultoría, legal, estrategia, impuestos y transacciones, busca que los equipos de EY puedan hacer mejores preguntas para encontrar nuevas respuestas a los asuntos complejos que actualmente enfrenta nuestro mundo.

EY se refiere a la organización global y podría referirse a una o más de las firmas miembro de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, una compañía del Reino Unido limitada por garantía, no proporciona servicios a clientes. Para conocer la información sobre cómo EY recaba y utiliza los datos personales y una descripción de los derechos que tienen las personas conforme a la ley de protección de datos, ingrese a ey.com/privacy. Las firmas miembro de EY no ofrecen servicios legales en los casos en que las leyes locales lo prohíban. Para obtener mayor información acerca de nuestra organización, ingrese a ey.com.