

Ciber Intelligence Center (CIC)

Estrategia y Road Map

Implementación

Operación y Mantenimiento

Definición y valor del concepto

Las **amenazas cibernéticas** están impactando negativamente y de una forma cada vez más agresiva a las organizaciones. Amenazas que van desde el secuestro de la información, fraudes financieros y fuga de información, **hasta la interrupción total del negocio.**

Es una realidad que los enfoques tradicionales no están siendo efectivos y por ende, es necesario robustecer los programas de ciberseguridad a través de la incorporación de prácticas integrales que generen inteligencia activa dentro de la organización, con la finalidad de minimizar la probabilidad de ocurrencia así como de aminorar el impacto de las amenazas.

Diagnóstico básico ¿Su empresa lo necesita?

Deloitte ocupado por la seguridad de las empresas ha generado un ecosistema que ayude a la alta dirección a responder preguntas como son:

- > ¿Hoy mi empresa está **comprometida**?
- > ¿Quién me **quiere atacar o robar** mi información?
- > ¿Por qué es de **interés** mi información?
- > ¿**Qué métodos** están utilizando los atacantes?
- > ¿Soy **resiliente** ante estas nuevas amenazas?



Estrategia y Road Map

1. Entendimiento del ambiente corporativo:
 - + Identificación de Información sensible, "Joyas de la Corona".
 - + Estructura organizacional.
 - + Servicios críticos de Información.



Implementación

2. Habilitación de estrategia definida:
 - + Identificación de ciberamenazas específicas de la industria.
 - + Habilitación de tecnologías dentro de la infraestructura de cliente.
 - + Generación de Inteligencia accionable para la organización.



Operación y Mantenimiento

3. Operación desde nuestro CIC:
 - + Integración de procesos.
 - + Entrega de reportes ejecutivos.
 - + Ventana 7*24.



CiberThreatHunting

Ayuda a conocer si la empresa está comprometida así como saber de manera recurrente si los controles de seguridad están siendo suficientes.

Red Team

Generación de simulaciones de amenazas orientadas a comprobar que los protocolos de seguridad están activos y son suficientes.

Servicios

Monitoreo y casos de uso

Generación de alarmas apegadas a las necesidades del negocio para la identificación proactiva de posibles fraudes o intrusiones a la red. Estas alarmas son monitoreadas en una ventana 7*24 por nuestros especialistas desde nuestro Centro de Inteligencia.

Respuesta a Incidentes

Habilita o revisa los protocolos de respuesta ante incidentes con alto impacto en la organización.

Threat Intelligence

Contamos con una base de datos de los indicadores de compromiso que afectan a las organizaciones a nivel mundial.

Beneficios y Valor

Protección del negocio	Alineación estratégica
Brindar confianza a los accionistas	Conciencia en ciberamenazas
Minimizar la probabilidad de riesgos	Prevención de incidentes

Santiago Gutiérrez
Socio Líder de Riesgo Cibernético
sangutierrez@deloittemx.com

Iván Campos
Socio de Riesgo Cibernético
icampos@deloittemx.com

Fernando Bojorges
Socio de Riesgo Cibernético
fbojorges@deloittemx.com

Erick Robles
Socio de Riesgo Cibernético
errobles@deloittemx.com

Sergio Solis
Socio de Riesgo Cibernético
sesolis@deloittemx.com