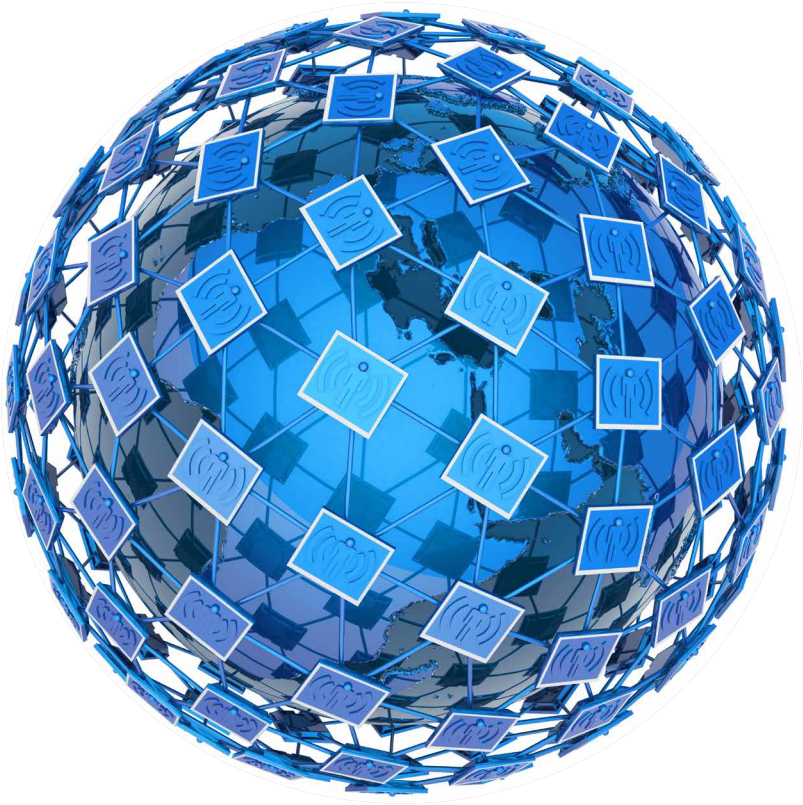
Deloitte.



Ayudamos a las organizaciones a proteger su crecimiento, rendimiento y valor

Cyber Risk Services

La Ciberseguridad presenta enormes desafíos para las organizaciones, además de que implica costos y consecuencias elevadas cuando no se cuenta con ella.

Un ciber ataque puede causar daño a la marca y a las finanzas de las organizaciones en cuestión de horas. Si bien las violaciones a datos masivos son comunes, un gran número de atacantes van por más allá que a obtener datos y/o beneficios económicos. Su intención muchas veces puede ser crear caos generalizado, destruir o interrumpir operaciones, y/o debilitar la posición competitiva o de mercado que posea su objetivo.

Mientras que los atacantes se adaptan y desarrollan sus tácticas a un ritmo alarmante, los líderes encargados de la seguridad también deben enfrentarse a la creciente presión de sus directores y ejecutivos, a un ambiente regulatorio en constante evolución, y a un entorno tecnológico complejo y rápidamente cambiante.

Dentro de los sectores público y privado, los líderes de TI podrían argumentar que es arduo colocarse al frente de un programa de Ciberseguridad.

A la vez que los retos parecen infinitos, los presupuestos y el talento no lo son. Si la intención es siempre hacer frente a los atacantes, cada vez más sofisticados, es probable que no exista nunca una cantidad de recursos suficientes para ello.

Ligar el desempeño organizacional al programa de Cyber Risk

Las organizaciones pueden transformar sus programas de seguridad de TI hacia programas de Ciber Riesgo.

Para la mayoría de ellas, éste es un imperativo debido al ritmo actual del cambio y la innovación.

Hoy en día, casi todas las iniciativas estratégicas están relacionadas a la tecnología. Incluso los esfuerzos para atraer o reposicionar al talento de nuevas maneras, pueden implicar vulnerabilidades antes desconocidas. La tendencia hacia operaciones más flexibles, interconectadas, habilitadas digitalmente y basadas en datos genera nuevas oportunidades para los enemigos cibernéticos y aumenta el impacto potencial de la falla tecnológica.

Aunque es improbable evitar todos los ciberincidentes, con la ayuda de un programa ejecutivo bien gestionado, es posible mantener los riesgos en niveles reducidos. El programa de Ciber Riesgo, en lugar de ser un costo alto para la empresa, es un elemento necesario para alcanzar los objetivos estratégicos y ligar el desempeño organizacional.

Más allá de la Seguridad Informática: Ser **Secure.Vigilant.Resilient.™**

Las empresas necesitan ser más diligentes y deliberadas en ser **seguras**, enfocándose en las políticas y controles para prevenir el robo o abuso de sus activos y operaciones más susceptibles al riesgo. En función de los riesgos particulares que enfrentan, invertir en ser **vigilantes** –mantener conciencia de las amenazas y detectando actividades irregulares– debe ser importante. Debido a que los incidentes suelen ocurrir, tener la capacidad de **responder** y **recuperarse** rápidamente es el tercer elemento esencial de un programa eficaz de Ciber Riesgo.

Deloitte ofrece una cartera completa de servicios para ayudar a las organizaciones a establecer su apetito de Cyber Risk. Además diseña e implementa un programa Secure.Vigilant.Resilient.™ y asiste en la gestión, mantenimiento y adaptación de sus programas.

Seguro.

Significa tener control sobre los riesgos prioritarios para defenderse contra amenazas conocidas y emergentes.

Vigilante.

Significa poseer inteligencia de amenazas y conocimiento de la situación para identificar cualquier comportamiento dañino.

Resiliente.

Significa tener la habilidad para enfrentar eventos de interrupción de los servicios que ofrece la empresa, a través de un programa de continuidad de negocio que permite identificar los impactos y criticidades de sus procesos, definiendo estrategias claras y pruebas de los planes desarrollados.

Estrategia y gobernabilidad.

Lograr y mantener una postura Secure.Vigilant.Resilient.™ requiere un esfuerzo ininterrumpido para definir un programa estratégico y normativo de Ciber Riesgo, además de darle seguimiento al progreso y adaptar el programa de manera continua dadas las cambiantes estrategias de negocio y la evolución de las ciberamenazas.

Servicios de gestión.

Los servicios a la medida y administrados de Deloitte pueden ayudarle a operar de manera más eficiente, abordar la escasez de talento, lograr capacidades más avanzadas y mantener sus objetivos generales del programa de Ciber Riesgo.

Seguro.

- Los servicios de **Gestión de Identidades y Accesos,** ayudan a manejar las múltiples identidades digitales y el acceso de recursos críticos, tanto internos como basados en la nube.
- Los servicios de **Protección de Datos**, ayudan a los clientes a implementar programas para respetar la privacidad de los individuos e implementar tecnologías para proteger datos susceptibles, al mismo tiempo que se le da cumplimiento a la LFPDPPP.
- Las soluciones de **Seguridad de Aplicaciones** establecen controles a través de los procesos y transacciones de extremo a extremo.
- Los servicios de **Integridad de Aplicaciones Empresariales,** aseguran la integridad de las transacciones a través del ecosistema de aplicaciones, desde el escritorio hasta el centro de datos, en instalaciones propias y en la nube.
- Los servicios de **Seguridad de Infraestructura**, se centran en desarrollar la protección fundamental de sistemas centrales y dispositivos.

Vigilante.

- Los servicios de **Optimización de las Operaciones de Seguridad**, desarrollan capacidades para simplificar el mantenimiento de controles de seguridad, mejorar la detección de amenazas y violaciones a la política, y priorizar el tratamiento de ciberincidentes.
- Las soluciones de **Monitoreo de Riesgos de Aplicación,** ofrecen visibilidad sobre el riesgo de las aplicaciones críticas y procesos de negocio, y mejoran las prácticas de seguridad en el ciclo vital del desarrollo de aplicaciones.
- **Analíticos e Inteligencia de Amenazas**, concientiza sobre el panorama de amenazas actual y otorga visión para mejorar la detección de amenazas y manejo de incidentes.
- Los servicios de **Gestión de Vulnerabilidades**, ayudan a minimizar las brechas explotables en las configuraciones de *software* y *hardware*.

Resiliente.

- Los servicios de **Respuesta a Ciber Incidentes**, ayudan a los clientes en la planificación, respuesta y recuperación de éstos, mismos que tienen el potencial de interrumpir operaciones, dañar la reputación y destruir valor para los accionistas.
- **Ciber Juegos de Guerra** es una técnica interactiva que sumerge a los posibles equipos de respuesta de ciberincidentes en un escenario simulado para ayudar a las organizaciones a evaluar y mejorar su preparación a la respuesta de estos incidentes.
- La oferta de **Resiliencia Técnica** se centra en aumentar la capacidad de una organización para recuperarse de las interrupciones a través de la tecnología.

Estrategia y gobernabilidad.

- Los proyectos de **Estrategia y evaluación** desarrollan planes de trabajo viables para apoyar la evolución de los programas de seguridad de TI hacia programas Secure.Vigilant. Resilient.™
- **Arquitectura de Seguridad Empresarial** define la arquitectura de próxima generación para apoyar la innovación empresarial y mitigar las amenazas emergentes.
- Los servicios de **Gobierno, Riesgo y Cumplimiento** proveen transparencia a las juntas directivas, a la administración y a los gerentes de línea a través de la implementación de tecnología e integración de datos.
- Los servicios de **Riesgo de Terceros** ayudan a las organizaciones en la gestión de ciberriesgos y riesgos operativos de toda la empresa.

Servicios de gestión.

- Gobierno, riesgo y cumplimiento
- Monitoreo de aplicaciones
- Gestión de identidad
- Prevención de pérdida de datos
- Operaciones de seguridad administrada
- Análisis e inteligencia de amenazas
- Habilitación de software de seguridad
- Gestión de vulnerabilidades
- Respuesta a ciberincidentes
- Resiliencia como servicio

¿Por qué escoger a Deloitte?

Nuestra práctica de Cyber Risk Services se basa en la amplia experiencia de Deloitte en temas de riesgo, regulación y tecnología, que le ayudará a:

Mejorar de forma constante con el programa Secure.Vigilant.Resilient.™. Independientemente del punto en el que se comience, crea una base extensible para capacidades futuras.

Unificar los esfuerzos de cumplimiento y de riesgo tecnológico, para ayudar a abordar los mandatos regulatorios sin perder de vista los problemas de riesgo más grandes para el negocio.

Implementar capacidades fundamentales de seguridad más rápido, al hacer uso de nuestros aceleradores de compromiso, nuestra amplia experiencia en la industria y de nuestro profundo conocimiento en los dominios de Cyber Risk.

Concentrarse en lo que importa mediante iniciativas que impulsen la atención de sus principales riesgos de negocio, informados por la conciencia actual del panorama de amenazas.

Apoyar las iniciativas estratégicas de negocio para hacer frente a los ciberriesgos asociados.

Para saber más sobre cómo su organización puede llegar a ser segura, vigilante y resiliente, por favor póngase en contacto con:

Santiago Gutiérrez
sangutierrez@deloittemx.com

Fernando Bojorges
fbojorges@deloittemx.com

Iván Campos
icampos@deloittemx.com

Ana Torres
anatorres@deloittemx.com