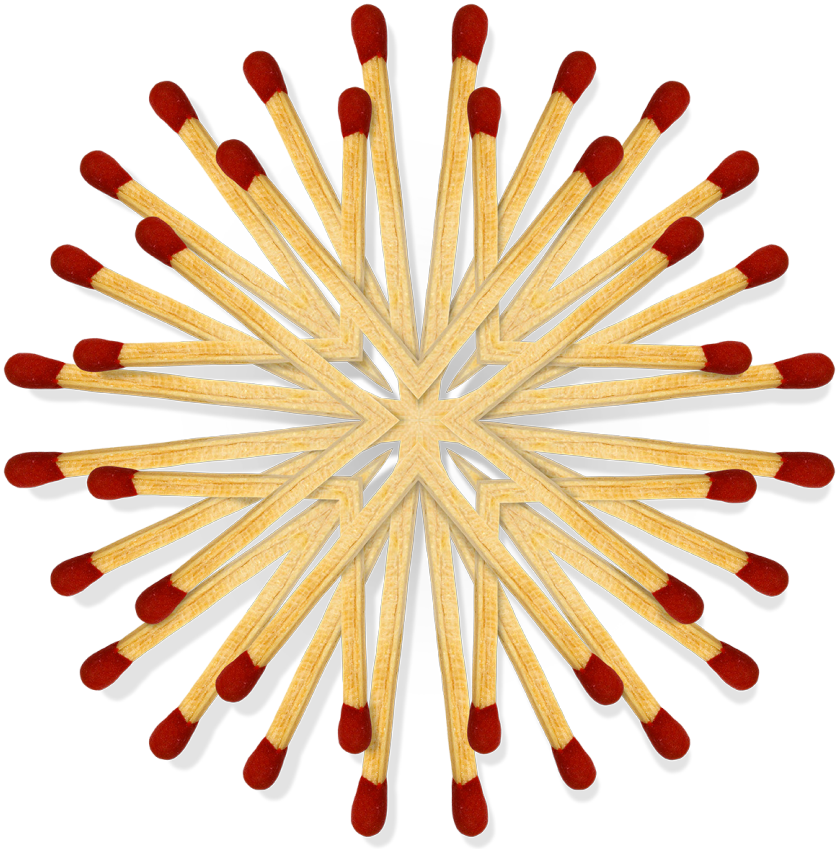
Deloitte.



Servicios de Cyber Risk

Asistiendo a las Organizaciones para proteger su negocio, crecimiento y valor

La ciberseguridad nunca ha sido más desafiante y los costos y consecuencias de la falta de seguridad se encuentran asimismo en su punto más alto. Un ataque cibernético puede causar daño en la reputación e impacto financiero en cuestión de horas. Si bien las brechas de seguridad masivas sobre los datos son habituales, los atacantes van más allá del rédito económico, buscan crear caos, causar una disrupción en las operaciones o comprometer la posición en el mercado de su empresa.

En todos los sectores, ya sean gubernamentales o industriales, muchos líderes de IT también dirían que son épocas complejas para estar al frente de un programa de ciberseguridad. Mientras que los atacantes se adaptan y desarrollan sus tácticas a un ritmo alarmante, los líderes de seguridad enfrentan la creciente presión de los directores y ejecutivos, un entorno normativo en constante cambio y un deterioro de control directo sobre el entorno tecnológico que cada vez es más complejo y cambia rápidamente. Si bien los desafíos pueden parecer infinitos, los presupuestos y el talento no lo son. Si el objetivo es enfrentarse continuamente contra atacantes, que utilizan tácticas cada vez más sofisticadas, probablemente nunca habría una cantidad adecuada de recursos.

Interconexión y cyber risk

En cambio, una organización puede transformar su programa de Seguridad de IT en un programa de Cyber Risk. Para la mayoría de las organizaciones, éste es un imperativo del negocio debido al ritmo del cambio y la innovación tecnológica.

La mayoría de las iniciativas estratégicas son soportadas por la tecnología. Los esfuerzos para ampliar, reestructurar o incorporar nuevas fuentes de talento, pueden introducir vulnerabilidades inesperadas. La tendencia hacia ser más flexible, estar interconectados, contar con operaciones habilitadas digitalmente, crea una nueva oportunidad para los adversarios cibernéticos y aumenta el impacto potencial de la insuficiencia de la tecnología.

Aunque no es posible prevenir todos los incidentes con un programa ejecutivo bien liderado, es posible gestionar el riesgo tecnológico a niveles aceptables.
El programa de cyber risk, en lugar de ser un costo cada vez mayor para la empresa, es un elemento necesario de las inversiones realizadas para alcanzar los objetivos estratégicos de la organización.

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

Las organizaciones necesitan ser diligentes para ser *Secure*, enfocándose en la definición de políticas y controles para evitar el robo o abuso sobre los activos críticos y las operaciones.

En función de los riesgos particulares que enfrentan, las inversiones para ser *Vigilant* – identificar las amenazas y detectar actividad irregular- son igual de importantes. Asimismo, debido a los incidentes que a veces se producen, debemos ser más *Resilient* - tener la capacidad de responder y recuperarse rápidamente de los incidentes – como tercer parte esencial de un programa eficaz de cyber risk.

Secure.

Ser *Secure* significa tener controles priorizados por riesgo para defenderse contra amenazas conocidas y emergentes.

Vigilant.

Ser *Vigilant* significa realizar inteligencia sobre las amenazas y ser conciente de la situación para identificar patrones nocivos de comportamiento

Resilient.

Ser *Resilient* significa tener capacidad de recuperación y minimizar el impacto de los incidentes.

Estrategia y gobierno

Definir y mantener una postura de *Secure. Vigilant. Resilient.*™ requiere un esfuerzo continuo para definir un programa liderado por ejecutivos de cyber risk, realizar un seguimiento del progreso y adaptar el programa continuamente a las estrategias cambiantes de negocio y a la evolución de las amenazas.

Estrategia y Evaluación. Proyectos para desarrollar planes de trabajo viables, apoyando la evolución de los programas de seguridad de IT, convirtiéndolos en programas *Secure*, *Vigilant* y *Resilient*.

Arquitectura de Seguridad Empresarial. Definición de la arquitectura de la próxima generación para apoyar la innovación empresarial y mitigar amenazas emergentes.

Gobierno, Riesgo y Cumplimiento. Servicios de gestión de riesgo para el directorio y la alta gerencia a través de la implementación de tecnología e integración de datos.

Riesgo de Terceros. Servicios que ayudan en la gestión de los riesgos operativos y de cyber seguridad a través de toda la organización.

Identidad y Control de Acceso. Servicios que ayudan a controlar la proliferación de las identidades digitales y el acceso a recursos críticos, tanto internos como basados en la nube.

Protección de Datos. Servicios que ayudan a los clientes a implementar programas para proteger la privacidad e implementar tecnologías para proteger los datos sensibles.

Seguridad en Aplicaciones. Implementación de soluciones que establezcan controles en las aplicaciones y transacciones.

Integridad de Aplicaciones. Servicios para asegurar la integridad de las transacciones a través de todo el entorno, desde el escritorio hasta el centro de datos, en las instalaciones y en la nube.

Seguridad de Infraestructura. Servicios que se centran en desarrollar la protección base de los sistemas centrales y dispositivos.

Optimización de las Operaciones de Seguridad. Servicios para desarrollar capacidades para simplificar el mantenimiento de controles de seguridad, mejorar la detección de amenazas y violaciones de las políticas, y priorizar la gestión de incidentes.

Monitoreo de Riesgos sobre Aplicaciones. Implementación de soluciones que permiten evaluar el riesgo sobre las aplicaciones críticas de negocio y los procesos y mejorar las prácticas de seguridad en el ciclo de vida de desarrollo de aplicaciones.

Análisis e Inteligencia de Amenazas. Proporciona una visión sobre el panorama de amenazas actual y una estrategia para mejorar la detección de amenazas y el manejo de incidentes.

Gestión de Vulnerabilidades. Servicios que ayudan a minimizar las brechas explotables en las configuraciones de software y hardware.

Respuesta ante Incidentes. Servicios que ayudan a los clientes en la planificación, respuesta y recuperación de incidentes que tienen el potencial de interrumpir aplicaciones, dañar la reputación y destruyen el valor de la empresa para los accionistas.

Wargaming. Es una técnica interactiva que sumerge a las posibles personas que responden a incidentes en un escenario simulado para ayudar a las organizaciones a evaluar y mejorar su preparación para la respuesta ante los mismos.

Resiliencia. Servicios centrados en aumentar la capacidad de una organización para recuperarse de interrupciones a través de la tecnología y en armar planes de continuidad de negocio.

Servicios Gestionados

Deloitte ofrece servicios gestionados que pueden ayudarlo a operar de manera más eficiente, solucionar la escasez de talento, lograr capacidades más avanzadas y tener un seguimiento de sus objetivos generales del programa de Cyber Risk.

- **Monitoreo de aplicaciones**
- **Gestión de identidades y control de accesos**
- **Prevención de fuga de información**

- **Operaciones de seguridad gestionada**
- **Análisis e inteligencia de amenazas**
- **Activación de software seguro**
- **Gestión de vulnerabilidades**

- **Respuesta ante incidentes**
- **Resiliencia-as-a-service**

El diferencial de Deloitte

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

- **Avanzar continuamente en su programa *Secure, Vigilant y Resilient*,**
- **Unificar esfuerzos de riesgo de cumplimiento y tecnología,**
- **Lograr los aspectos fundamentales más rápido,**
- **Concéntrese en lo que importa,**
- **Apoyar las iniciativas estratégicas de negocio.**

Contáctenos:

Martín Carmuega
Socio
Líder Risk Advisory
+54 11 4320 4003
mcarmuega@deloitte.com

Andrés Gil
Socio
Líder Cyber Risk Services
+54 11 4320 2779
angil@deloitte.com

Julio Ardita
Socio
Cybsec by Deloitte
+54 11 4371 4444
jardita@Deloitte.com

Facundo Jamardo
Socio
Cyber Risk Services
+54 11 4320 4067
fjamardo@deloitte.com

Sebastián Peroni
Socio
Cyber Risk Services
+54 11 4320 4086
speroni@deloitte.com

Luciano Martins
Director
Cyber Risk SErvices
+54 11 4320 4006
lmartins@Deloitte.com

Si su dispositivo móvil lo permite, escanee el código y acceda a nuestra web.