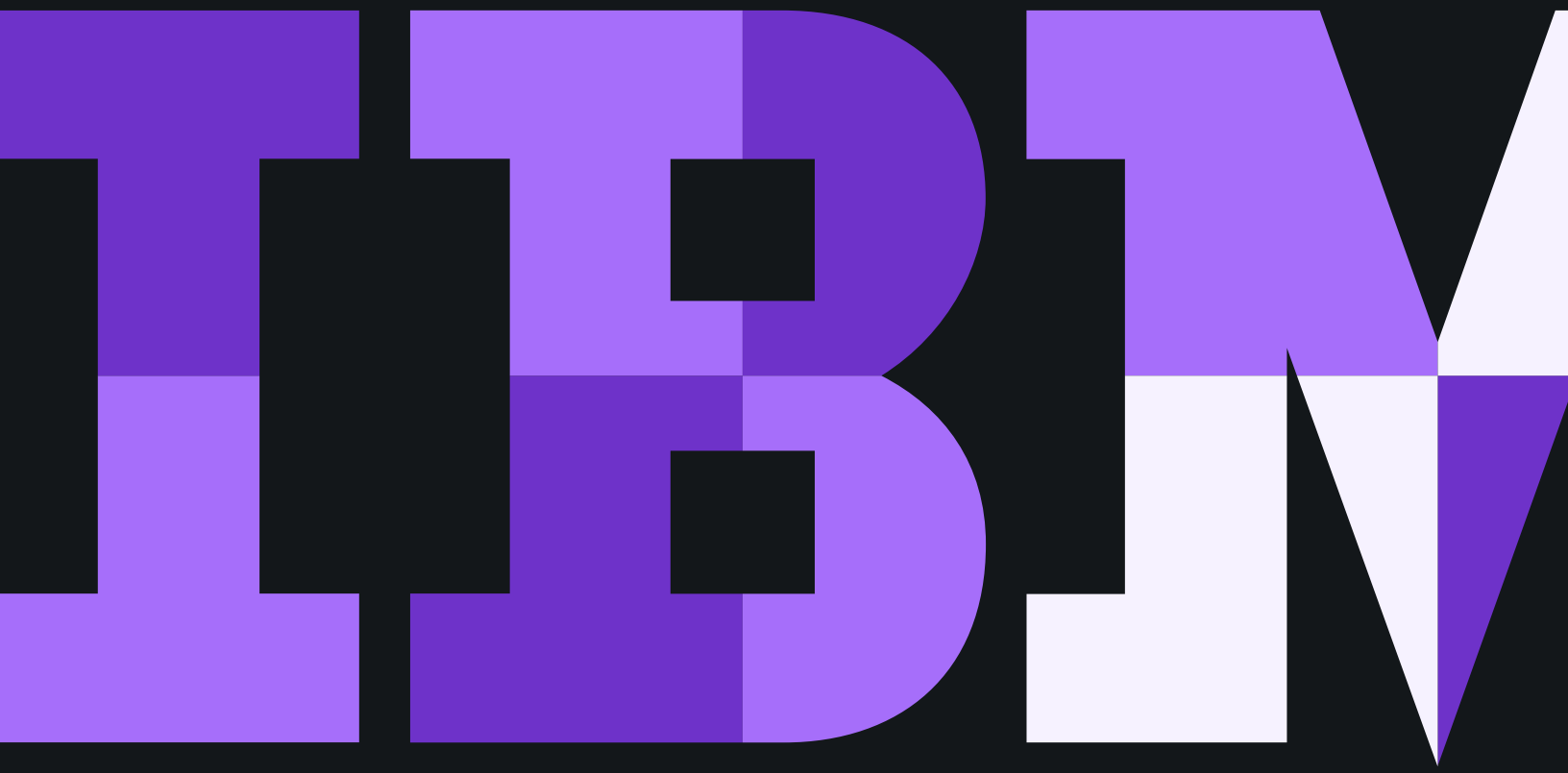
IBM Security

Enero de 2020

Estrategias para la gestión de riesgos en seguridad cibernética

Evalúe y haga progresar su seguridad y su postura de cumplimiento



IBM

Contenido

El escenario de ciberseguridad actual

Todos tenemos a las infracciones de datos, los ataques de ransomware, las fallas en la privacidad y otros desafíos de seguridad cibernética en la pantalla del radar, pero aún muchas empresas tienen dificultades en el momento de prepararse de manera eficaz contra ellos. Muchas organizaciones no cuentan con una estrategia de seguridad clara y alineada, tienen un conocimiento limitado de la madurez de su seguridad cibernética y no practican suficientemente sus planes como para responder ante un incidente de seguridad cibernética, si es que efectivamente tienen un plan de respuesta ante incidentes. De hecho, podría decirse que el enfoque de la mayoría de las organizaciones en cuanto a la gestión de riesgos es bastante riesgosa.

Las organizaciones suelen enfrentar fuerzas disruptivas que aumentan el riesgo de TI: fusiones, adquisiciones y desinversiones; tecnologías en desarrollo tales como la nube, IoT y cuántica; y cambios en las normas de cumplimiento. A la vez, las organizaciones deben innovar y avanzar mientras abordan la seguridad y el cumplimiento. Los desafíos que pueden retrasar a las empresas incluyen:

- Requisitos reglamentarios complejos
- Falta de alineación de la estrategia de seguridad así como de la madurez de seguridad cibernética y del cumplimiento
- Cambios frecuentes en la organización
- Interrupciones de las habilidades de seguridad
- Incertidumbre en relación con las “prácticas recomendadas” de seguridad

279 días

El tiempo promedio global para identificar y contener una violación

25.575 registros

El tamaño promedio global de una violación de datos

Pérdida de negocio

El mayor contribuyente de costos de una violación de datos[1]

Hacer frente a los riesgos con acción

Mantenerse al día con las amenazas de seguridad cibernética y el cumplimiento reglamentario no es fácil. Muchas empresas contratan la ayuda de asesores fiables para comprender mejor su seguridad cibernética y su postura de cumplimiento, aprender las prácticas recomendadas y perseguir sus objetivos de negocio frente a la incertidumbre cibernética. Con un asesor confiable, usted puede anticipar mejor la disrupción, adaptarse a un escenario de seguridad cambiante y ver nuevas innovaciones a fin de obtener una ventaja competitiva sin perder de vista la seguridad.

Las organizaciones líderes buscan referencias precisas de dónde se encuentran y desarrollan planes para gestionar mejor el riesgo, el cumplimiento y la gobernanza. Estas evaluaciones pueden incluir cuantificación de riesgos, identificación de riesgos de seguridad de terceros; pruebas de penetración para encontrar debilidades en el sistema propio de uno; así como simulaciones de violaciones cibernéticas para poner a prueba al personal y a la tecnología, identificar requisitos y generar memoria muscular para prepararse para los ataques cibernéticos.

Cada vez más, los rangos cibernéticos se están convirtiendo en parte de las estrategias de gestión de riesgos de las organizaciones líderes. Permiten que las organizaciones reúnan sus equipos de seguridad y ejecutivos clave para experimentar una violación de seguridad simulada en un entorno contenido. Una experiencia de rango cibernético puede ayudar a las organizaciones a evaluar las brechas en su plan de respuesta ante incidentes y evaluar en forma crítica cómo sus equipos de seguridad y cumplimiento deberían integrar la respuesta ante incidentes en toda su organización.

Finastra prueba su preparación para los ataques cibernéticos con IBM

Finastra, con base en Londres, una de las empresas de tecnología financiera más grandes del mundo, se comprometió con IBM Security para llevar a cabo un evento de rango cibernético a fin de probar sus capacidades para luchar contra una violación de datos intercontinental.

Vea el video

Los pilares de la gestión del riesgo de seguridad: Evaluación, reducción y gestión

Para minimizar el riesgo de seguridad, conozca sus debilidades y cómo abordarlas:

Evalúe su seguridad cibernética y su cumplimiento normativo actuales

Determine cómo reducir mejor el riesgo

Administre la exposición al riesgo en el futuro

Este tipo de introspección de seguridad puede beneficiarse ampliamente de una perspectiva externa y experimentada: un asesor confiable que puede ayudarle a responder las preguntas correctas, usar un enfoque comprobado para el éxito y obtener resultados. **Debe descubrir las vulnerabilidades de seguridad ocultas que podrían dejar a su negocio expuesto a violaciones de datos, falta de cumplimiento reglamentario u otros riesgos que tienen el potencial de lastimar su reputación y sus ingresos.**

Al usar metodologías comprobadas basadas en incontables compromisos y prácticas recomendadas de la industria, los asesores confiables pueden ayudarle a identificar tanto riesgos como soluciones para reducir dichos riesgos.

La seguridad es un desafío continuo. Un asesor puede proporcionar monitoreo, gestión y capacitación de seguridad continuos para ayudarle a mantener una seguridad sólida y un cumplimiento de las normas, puede fomentar una cultura de seguridad, ayudar a abordar nuevas amenazas y ajustar su programa de seguridad y cumplimiento con el tiempo.

Una estrategia de seguridad exitosa comienza por el comienzo. Los asesores confiables pueden proporcionar recomendaciones para ayudarle a dar prioridad a los recursos, alinear la toma de decisiones y generar soporte de los ejecutivos para las iniciativas de seguridad y cumplimiento que más importan. Esto puede incluir la nube, IoT, dispositivos móviles y otras iniciativas de manera que la seguridad sea una parte integral de su estrategia digital y sus iniciativas de transformación.

Los asesores confiables brindan recomendaciones para ayudarle a priorizar recursos, alinear la toma de decisiones y generar respaldo ejecutivo

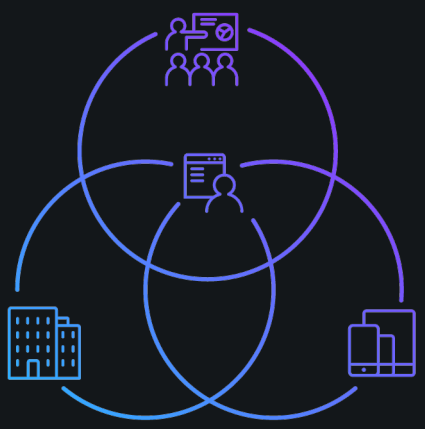
Navegue por lo inesperado

El riesgo está en todos lados. Está fuera de su negocio, asechando en forma de ransomware oculto y ataques de fuerza bruta designados para desviar su atención mientras se roban sus datos. Está dentro de su negocio, agazapado detrás de una identidad fiable o es introducido por un simple error humano. Y está apostado en las sombras de la oportunidad, desde fábricas automatizadas hasta centros de atención al cliente con IA.

Necesita un asesor confiable que eche luz sobre el riesgo y lo lleve al descubierto. **Necesita una visión confiable del riesgo en su organización que permita la gestión mejorada de la gobernanza, el riesgo y el cumplimiento.** Nadie espera ser víctima de un ataque cibernético hasta que es víctima de uno. Un asesor de seguridad puede ayudar a identificar, cuantificar y priorizar los riesgos, y luego administrarlos.

La gestión confiable de riesgos no es responsabilidad de una sola persona ni de un equipo. Requiere un enfoque sistémico y alineado que abarque todas las unidades comerciales, líderes y procesos, que entrecruce a todas las personas, máquinas y elementos de la organización.

La gestión confiable de riesgos requiere un enfoque sistémico y alineado que abarque todas las unidades comerciales, líderes y procesos, que entrecruce a todas las personas, máquinas y elementos de la organización



Confíe en IBM Security

Con IBM Security, nunca deberá hacer frente al riesgo usted solo. Nuestros servicios ayudan a garantizar la implementación de las capacidades de seguridad y cumplimiento adecuadas para gestionar de manera eficaz el riesgo, abarcando los procesos, las personas y la tecnología. A medida que el escenario de seguridad cambia debido a nuevos vectores de amenaza, nuevas reglamentaciones de cumplimiento e incluso lo imprevisto, la experiencia de seguridad de IBM estará allí para ayudarle a mantener el riesgo bajo control.

La experiencia de IBM Security puede ayudarle a crear una estrategia de seguridad eficaz, así como evaluar de manera crítica su postura de cumplimiento y seguridad en toda la organización, medir de manera precisa sus capacidades (es decir, qué tan rápido puede responder a la violación de datos) e identificar los eslabones débiles de su cadena de control. IBM Security cuenta con las personas, las metodologías y la experiencia adecuadas para ayudarle a evaluar, reducir y gestionar el riesgo, incluido:

IBM Security Strategy Risk and Compliance Services (SSRC): Le ayudamos a evaluar su gobierno de seguridad actual a través de la comparación con sus objetivos corporativos, lo guiamos por la creación de una estrategia y un programa de gestión de riesgos y respaldamos su jornada para mejorar la madurez de la seguridad. Trabajar con IBM puede ayudarle a administrar mejor sus riesgos, el cumplimiento y la gobernanza a través de:

- Servicios de asesoría de seguridad para directores ejecutivos
- Cuantificación de riesgos
- Evaluación de riesgos de seguridad en fusiones y adquisiciones
- Seguridad y cumplimiento en la nube
- Estrategias de privacidad de datos
- Cumplimiento reglamentario y gobierno
- Evaluación y gestión de riesgos de seguridad d e terceros
- Gestión de riesgos de TI automatizada
- Seguridad de infraestructura crítica
- Evaluación de estrategia de seguridad y reducción de riesgos de SAP
- Gestión de concientización de seguridad para empleados

SSRC puede ayudarle a evaluar, reducir y gestionar el riesgo de seguridad. Ya sea que su negocio necesite asesoramiento experto sobre el cumplimiento normativo, una revisión de la preparación de la privacidad de datos o deba cuantificar el riesgo para el liderazgo, consulte los servicios de IBM Security Strategy Risk and Compliance.

IBM Security Command Centers: Lo que los Command Centers de IBM hacen mejor es ayudarlo a prepararse para su peor día, a la vez que mejoran su cultura y preparación de seguridad general. Los compromisos de rango cibernético sumergen sus equipos interdisciplinarios en situaciones de seguridad simulada para ayudarlos a desarrollar y perfeccionar las capacidades y la confianza que necesitarán para lidiar con los escenarios de fuertes ataques cibernéticos en el mundo real. En nuestros Centros de Información Ejecutiva, puede aprovechar los grupos de cerebros de seguridad de IBM: personas experimentadas en responder a incidentes, que realizan pruebas de penetración, que realizan estrategias de seguridad y líderes que pueden ayudarle a mejorar drásticamente su postura de seguridad y minimizar su exposición al riesgo.

Temas relacionados

Cumplimiento: Debe realizar un seguimiento de cómo su organización maneja los datos, ya sea que estén en reposo o en movimiento, y ser capaz de probar el cumplimiento en cualquier punto. Adelántese a los cambios en la reglamentación con un cumplimiento que sea más fácil de manejar y de implementar. Use soluciones que ayuden a su organización a abordar el cumplimiento de manera que pueda implementar recursos para otras prioridades. Simplifique el cumplimiento con talento y tecnología desde IBM Security.

Liderazgo y cultura: Las innovaciones tecnológicas, las interrupciones del mercado, los cambios en los requisitos de capacidades y otros factores pueden provocar cierta volatilidad que afecte su seguridad y su posición de cumplimiento. Si bien no hay un escudo mágico para proteger a su organización, puede tomar medidas efectivas para mejorar su seguridad y posición de cumplimiento con acceso a las últimas investigaciones e información sobre tendencias de seguridad y soluciones innovadoras.

Fuentes

1. Ponemon Institute and IBM Security, “2019 Cost of a Data Breach Report” (Informe de costos de una violación de datos de 2019) 2019.

IBM Security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Producido en Estados Unidos de América
Enero de 2020

IBM

GDPYL8KD