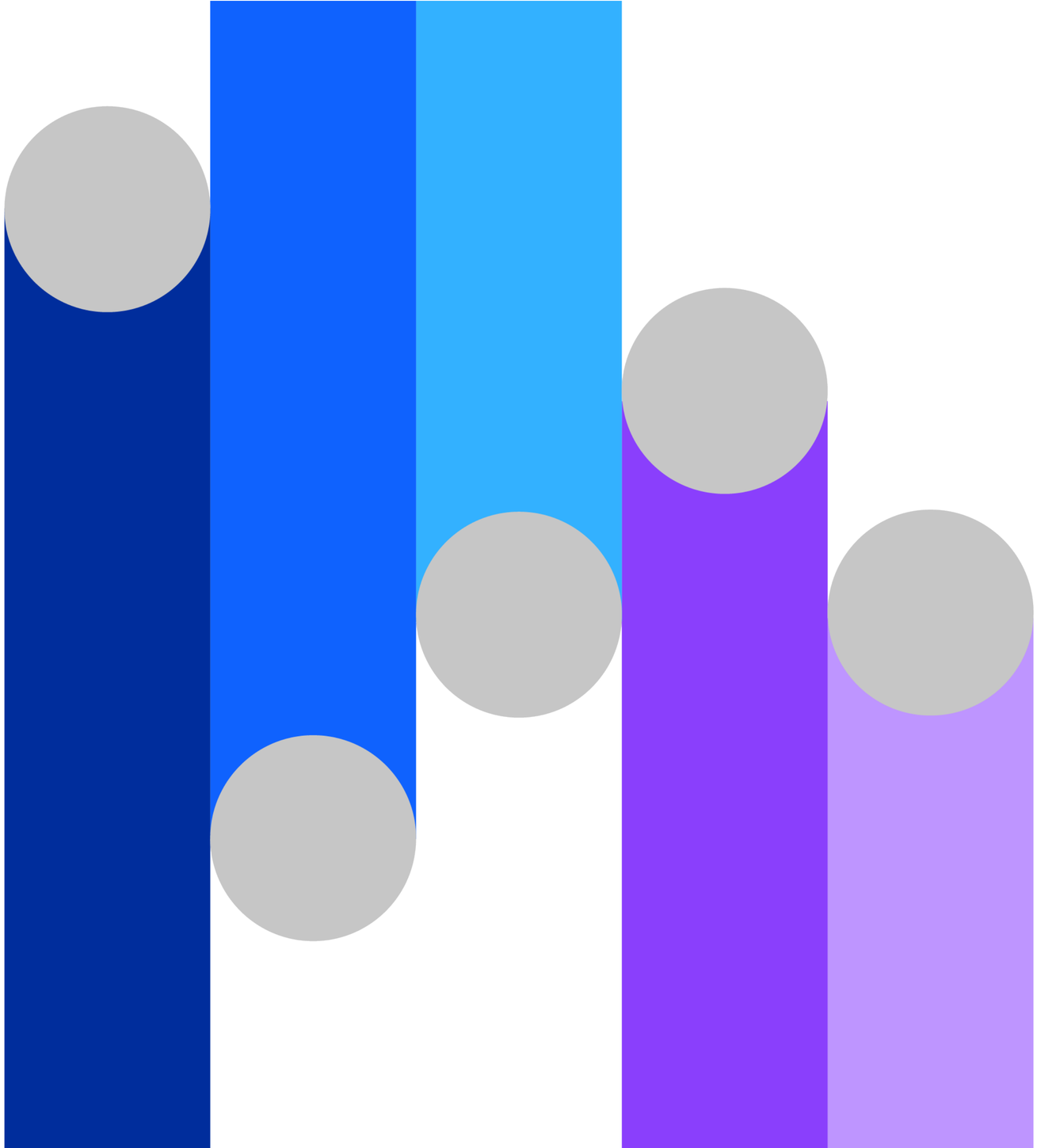
IBM® **Security**

Cinco obstáculos comunes en la seguridad de datos que debe evitar

Aprenda a mejorar su postura de cumplimiento y seguridad de datos



IBM

Índice

00

Introducción

La seguridad de datos debe ser una prioridad para las empresas, y por una buena razón

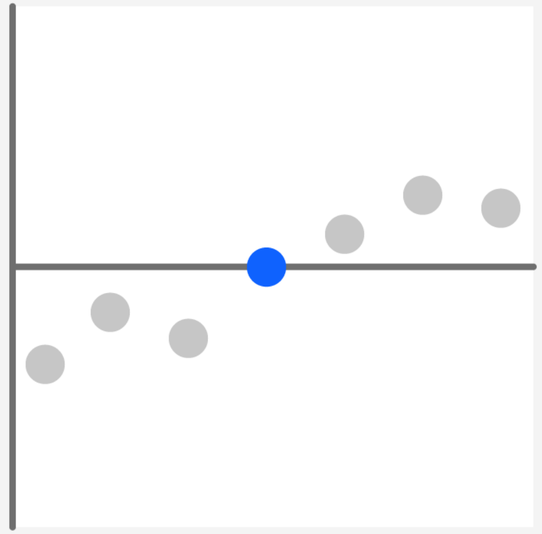
Aunque el panorama de TI sea cada vez más descentralizado y complejo, es importante entender que muchas vulneraciones de datos son evitables. Aunque los retos y objetivos individuales en materia de ciberseguridad pueden diferir de una empresa a otra, las organizaciones suelen cometer los mismos errores generalizados cuando comienzan a abordar la seguridad de datos. Además, muchos directores de empresas suelen aceptar estos errores como prácticas comerciales normales.

Hay varios factores internos y externos que pueden llevar a que se produzcan ciberataques, entre ellos:

- La erosión de los perímetros de la red.
- Las mayores superficies de ataque que ofrecen muchos entornos de TI complejos.
- Las crecientes demandas que imponen los servicios en la nube en las prácticas de ciberseguridad
- Una naturaleza cada vez más sofisticada de los ciberdelitos.
- Una falta constante de habilidades en materia de ciberseguridad.
- La falta de concientización de los empleados en cuanto a los riesgos de seguridad de datos.

USD 4,45 millones

El costo promedio global de una vulneración de datos creció en 2023, con un aumento del 15 % en un período de 3 años.[1]



Siguiente capítulo

01

Obstáculo 1: No poder ir más allá del cumplimiento

Obstáculo 1: No poder ir más allá del cumplimiento

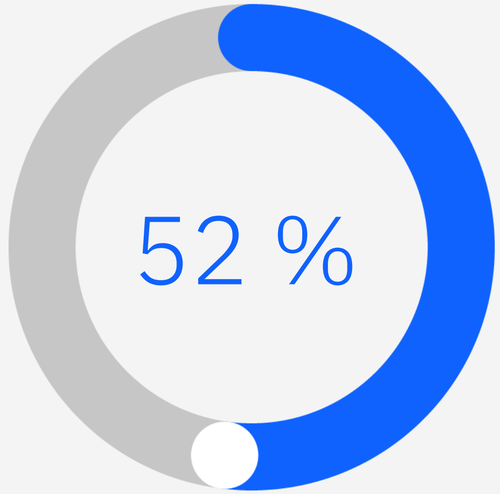
El cumplimiento no necesariamente es igual a la seguridad de datos. Las organizaciones que concentran sus recursos limitados de seguridad de datos en cumplir con una auditoría o certificación pueden caer en la complacencia. Muchas de las mayores vulneraciones de datos se produjeron en organizaciones que, en teoría, cumplían perfectamente con todo. Los siguientes ejemplos muestran cómo centrarse solamente en el cumplimiento puede hacer menguar la seguridad efectiva.

Cobertura incompleta
Las empresas suelen esforzarse para abordar los problemas de configuración de bases de datos y las políticas de acceso obsoletas antes de llevar a cabo una auditoría anual. Las evaluaciones de vulnerabilidades y riesgos deben ser actividades constantes.

Esfuerzo mínimo
Muchas empresas adoptan soluciones de seguridad de datos solo para cumplir con los requisitos legales o de los socios de negocios. Esta mentalidad de “implementemos un estándar mínimo y volvamos al trabajo” puede ser perjudicial frente a las buenas prácticas de ciberseguridad. La seguridad de datos efectiva es una maratón, no una carrera de velocidad.

Urgencia que se desvanece
Las empresas pueden caer en la complacencia en cuanto a la administración de los controles cuando las normativas maduran, como la Ley Sarbanes-Oxley (SOX), el Reglamento General de Protección de Datos (RGPD), la norma relativa a la seguridad de los datos del sector de las tarjetas de pago (PCI DSS) y la Ley de Derechos de Privacidad de California (CPRA), antes conocida como la CCPA. Mientras que, con el correr del tiempo, los directivos pueden ser cada vez menos considerados con la privacidad, la seguridad y la protección de los datos regulados, los riesgos y los costos asociados con el incumplimiento permanecen.

Omisión de datos no regulados
Los activos, como la propiedad intelectual, pueden poner su organización en riesgo si se pierden o se comparten con personal no autorizado. Centrarse solamente en el cumplimiento puede tener como resultado organizaciones de seguridad de datos que pasan por alto la protección de datos valiosos.



El 52 % de las organizaciones dicen que la complejidad creada por el cambio en las cargas de trabajo a la nube pública también ha dificultado el cumplimiento.[2]

Ver el cumplimiento como una oportunidad de innovar y elevar sus estándares de seguridad para respaldar su negocio.

Solución: Reconocer y aceptar que el cumplimiento es un punto de partida

Las organizaciones de seguridad de datos deben establecer programas estratégicos que protejan constantemente los datos críticos de sus empresas, en contraposición con solo responder a los requisitos de cumplimiento.

Los programas de seguridad de datos y de cumplimiento deben incluir estas prácticas esenciales:

- Descubrir y clasificar sus datos confidenciales en aplicaciones locales, los almacenes de datos en la nube y de software como servicio (SaaS).
- Evaluar el riesgo con perspectivas y análisis contextuales.
- Proteger los datos confidenciales a través de la encriptación y las políticas de acceso flexibles.
- Supervisar los patrones de acceso a datos y consumo para descubrir rápidamente actividades sospechosas.
- Responder a las amenazas en tiempo real.
- Simplificar el cumplimiento y la generación de informes.

El elemento final puede incluir obligaciones legales relacionadas con el cumplimiento regulatorio, posibles pérdidas que una empresa puede sufrir y los costos potenciales de dichas pérdidas más allá de las multas por incumplimiento.

En definitiva, debe pensar en forma holística sobre el riesgo y el valor de los datos que quiere proteger.

02

Obstáculo 2: No poder reconocer la necesidad de tener una seguridad de datos centralizada

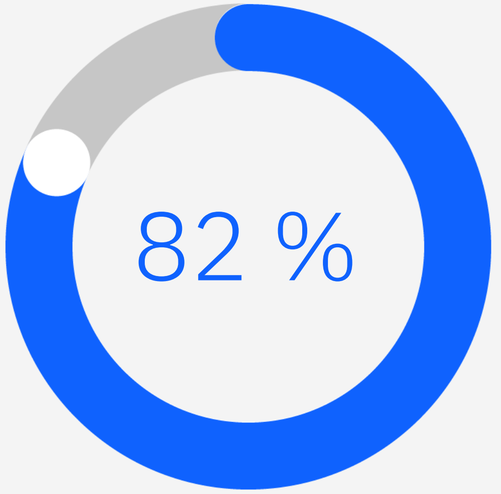
Obstáculo 2: No poder reconocer la necesidad de tener una seguridad de datos centralizada

Sin mandatos de cumplimiento más amplios que abarquen la privacidad y la seguridad de datos, los directivos de las organizaciones pueden perder de vista la necesidad de contar con una seguridad de datos constante para toda la empresa.

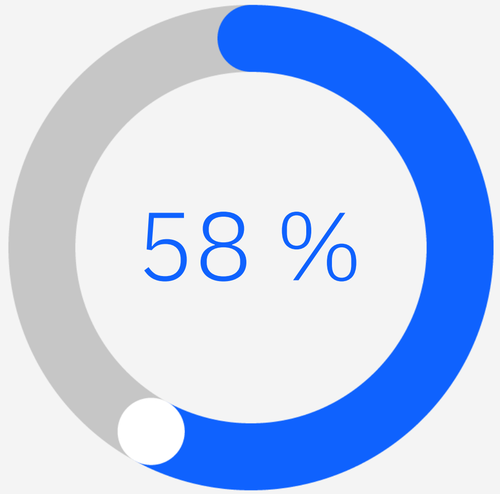
Para las empresas con entornos multinube híbridos, que constantemente cambian y crecen, pueden aparecer nuevos tipos de fuentes de datos en forma semanal o diaria y propagar datos confidenciales.

Los directivos de las compañías que crecen y amplían sus infraestructuras de TI pueden no reconocer el riesgo que implican sus superficies de ataque cambiantes. Pueden carecer de la visibilidad y el control adecuados, ya que los datos confidenciales se mueven en un entorno de TI cada vez más complejo y dispar. No adoptar controles integrales de privacidad, seguridad y protección de datos —en especial, dentro de entornos complejos— puede demostrar ser una omisión muy costosa.

Operar soluciones de ciberseguridad en silos puede causar otros problemas. Por ejemplo, las organizaciones con un centro de operaciones de seguridad (SOC) y una solución de gestión de eventos e información de seguridad (SIEM) puede olvidar alimentar esos sistemas con información recopilada de su solución de seguridad de datos. Asimismo, una falta de interoperabilidad entre los equipos de seguridad, procesos y herramientas puede impedir el éxito de cualquier programa de ciberseguridad.



El 82 % de las vulneraciones involucraron datos almacenados en la nube.[1]



El 58 % de las organizaciones dice que entre el 21 % y el 50 % de los datos confidenciales en la nube no están lo suficientemente protegidos.[2]

La protección de los datos confidenciales debe llevarse a cabo junto con sus iniciativas de ciberseguridad más amplias.

Solución: Saber dónde residen sus datos confidenciales, incluidos en las aplicaciones locales, los repositorios alojados en la nube y los SaaS

La protección de los datos confidenciales debe llevarse a cabo junto con sus iniciativas de ciberseguridad más amplias.Además de entender dónde se almacenan sus datos confidenciales, debe saber también cuándo y cómo se accede a ellos, aunque esta información cambie rápidamente. Asimismo, debe trabajar para integrar perspectivas y políticas de seguridad y protección de datos con su programa de ciberseguridad general, a fin de permitir la comunicación completamente alineada entre tecnologías. Una solución de seguridad de datos que opera en entornos y plataformas dispares puede ayudar en este proceso.

¿Cuándo es el momento adecuado para integrar la seguridad de datos con otros controles de ciberseguridad como parte de una práctica de ciberseguridad más holística? Estos son algunos signos que sugieren que su organización debe estar preparada para dar este próximo paso.

Riesgo de perder datos valiosos

El valor de los datos personales, confidenciales y patentados de su organización es tan significativo que su pérdida podría causar un daño notorio a la viabilidad de su empresa.

Obstáculo 2: No poder reconocer la necesidad de tener una seguridad de datos centralizada

Consecuencias regulatorias
Su organización recopila y almacena datos con requisitos legales, como números de tarjetas de crédito, otra información de pago o datos personales.

Falta de supervisión de ciberseguridad
Su organización ha crecido hasta un punto en el que es difícil hacer un seguimiento de todos los endpoints de la red y protegerlos, incluidas las instancias en la nube. Por ejemplo, ¿tiene una idea clara de dónde, cuándo y cómo se almacenan los datos, se comparten y se accede a ellos en sus aplicaciones locales, de almacenes de datos en la nube y de SaaS?

Evaluación inadecuada
Su organización ha adoptado un enfoque fragmentado en el que no se entiende bien qué se gasta en sus actividades de ciberseguridad. Por ejemplo, ¿tiene procesos implementados para medir con precisión su retorno de la inversión (ROI) en cuanto a los recursos que se asignan para reducir el riesgo de seguridad de datos?

Si cualquiera de estas situaciones se aplica a su organización, debe pensar en dominar habilidades de ciberseguridad y adquirir las soluciones necesarias para integrar la seguridad de datos en su práctica actual más amplia de seguridad.

Obstáculo 3: No poder definir quién tiene la responsabilidad de los datos

Obstáculo 3: No poder definir quién tiene la responsabilidad de los datos

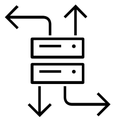
Aunque muchas empresas sean conscientes de la necesidad de contar con seguridad de datos, no tienen a nadie específicamente responsable de proteger datos confidenciales. Esta situación suele verse durante un incidente de seguridad de datos o de auditoría cuando la organización tiene la presión de descubrir quién es responsable.

Los altos ejecutivos pueden hablar con el director de información (CIO), quien podría decir: “Nuestro trabajo es mantener los sistemas en funcionamiento. Ve a hablar con alguien de mi equipo de TI”. Esos empleados de TI pueden ser responsables de varias bases de datos en las que residen datos confidenciales y, aun así, carecer de un presupuesto de ciberseguridad.

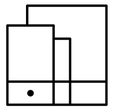
Por lo general, los miembros de la organización del director de seguridad de la información (CISO) no son directamente responsables de los datos que fluyen a través de la empresa en general. Quizá aconsejen a los distintos gerentes de la línea de negocios (LOB) dentro de una empresa, pero, en muchas compañías, nadie es explícitamente responsable de los datos en sí. Para una organización, los datos son uno de sus activos más valiosos. Sin embargo, sin responsabilidad de la propiedad, proteger los datos confidenciales de manera adecuada es todo un desafío.

En entornos de TI complejos, es crítico contabilizar los datos en las siguientes ubicaciones:

Compartidos en todas las unidades de negocio



Ubicados en infraestructuras multinube híbridas



Almacenados en dispositivos móviles

Solución: Contratar un CDO o DPO dedicado al bienestar y la seguridad de activos de datos críticos y confidenciales

Un director de datos (CDO) o delegado de protección de datos (DPO) puede manejar estas tareas. De hecho, las empresas con sede en Europa o que hacen negocios con la Unión Europea se enfrentan a mandatos del RGPD que les exigen tener un DPO. Este requisito previo reconoce que los datos confidenciales —en este caso, la información personal— tiene un valor que va más allá de la LOB que usa esos datos. Además, el requisito hace hincapié en que las empresas tienen un puesto específicamente diseñado para ser responsable de los activos de datos.

Tenga en cuenta los siguientes objetivos y responsabilidades para elegir un CDO o DPO:

Conocimiento técnico y sentido empresarial.
Evaluar el riesgo y hacer un caso empresarial práctico que los líderes empresariales no familiarizados con la tecnología puedan entender con respecto a las inversiones adecuadas en seguridad de datos.

Implementación estratégica
Dirigir un plan a nivel técnico que aplique controles de detección, respuesta y seguridad de datos para ofrecer protecciones.

Liderazgo del cumplimiento
Entender los requisitos de cumplimiento y saber dirigir dichos requisitos a los controles de seguridad de datos para que su empresa cumpla.

Obstáculo 3: No poder definir
quién tiene la responsabilidad de los datos

Supervisión y evaluación
Supervisar el panorama de amenazas y medir la efectividad de su programa de seguridad de datos.

Flexibilidad y escalamiento
Saber cuándo y cómo ajustar la estrategia de seguridad de datos, como ampliar las políticas de acceso a los datos y consumo de datos en nuevos entornos integrando herramientas más avanzadas.

División del trabajo
Establecer expectativas con los proveedores de servicios en la nube con respecto a los acuerdos de nivel de servicios (SLAs) y las responsabilidades asociadas con riesgo y remediación de la seguridad de datos.

Plan de respuesta ante vulneraciones de datos
Finalmente, estar listo para desempeñar un papel clave en el diseño de un plan estratégico de respuesta y mitigación de vulneraciones.

En definitiva, el CDO o DPO debe fomentar la colaboración en cuanto a seguridad de datos entre todos los equipos y en toda la empresa, ya que todos necesitan trabajar juntos para proteger de manera efectiva los datos corporativos. Esta colaboración puede ayudar al CDO o DPO a supervisar los programas y las protecciones que su organización necesita para poder proteger sus datos confidenciales.

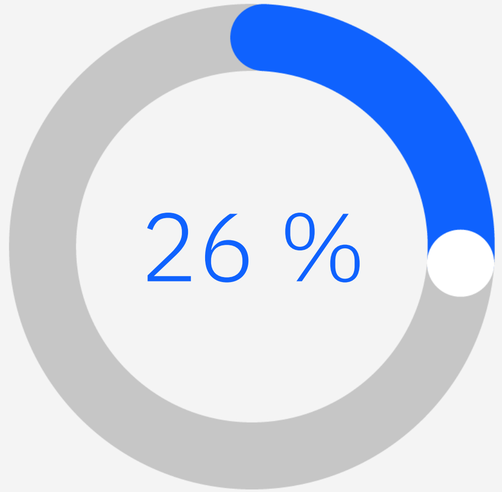
Obstáculo 4: No poder abordar las vulnerabilidades conocidas

Obstáculo 4: No poder abordar las vulnerabilidades conocidas

Las vulneraciones de alto perfil en las empresas muchas veces han sido la consecuencia de vulnerabilidades conocidas que no se parchearon, ni siquiera después del lanzamiento de los parches. No implementar los parches a vulnerabilidades conocidas rápidamente pone los datos de su organización en riesgo, ya que los ciberdelincuentes buscan activamente estos puntos de ingreso sencillos.

Sin embargo, a muchas empresas les resulta difícil implementar los parches rápidamente, debido al nivel de coordinación que se necesita entre los grupos de TI, de seguridad y operativos. Asimismo, los parches suelen requerir pasar por pruebas para ver si no rompen un proceso o introducen una nueva vulnerabilidad.

En entornos de nube, a veces es difícil saber si el componente de un servicio o aplicación contratados debe parchearse. Aunque una vulnerabilidad se encuentre en un servicio, sus usuarios suelen no tener el control sobre el proceso de remediación del proveedor de servicios.



El 26 % de las nuevas vulnerabilidades tenían brechas conocidas.[3]

Tome una actitud proactiva mediante la realización de evaluaciones de vulnerabilidades de sus almacenes de datos para ayudar a mitigar el riesgo.

Solución: Establecer un programa de gestión de vulnerabilidades efectivo con la tecnología adecuada para respaldar su crecimiento

Por lo general, la gestión de vulnerabilidades implica tener algunos de los siguientes niveles de actividad:

- Mantener un inventario preciso y una línea base para sus activos de datos.
- Llevar a cabo evaluaciones y exploraciones de vulnerabilidades frecuentes en toda su infraestructura, incluidos los activos en la nube.
- Priorizar la remediación de vulnerabilidades que considera la probabilidad de la vulnerabilidad que se explota y el impacto que ese evento tendría en su empresa.
- Incluir la gestión y la respuesta a vulnerabilidades como parte del SLA con proveedores de servicios externos.
- Ocultar los datos confidenciales o personales siempre que sea posible. Encriptación, tokenización y redacción son las tres opciones para lograrlo.
- Emplear una adecuada gestión de claves de encriptación que garantice que las claves de encriptación se almacenen de manera segura y pasen por un ciclo adecuado para proteger sus datos encriptados.

Aunque cuente con un programa de gestión de vulnerabilidades maduro, ningún sistema puede ser seguro en su totalidad. Asuma que puede haber intrusiones, incluso en los entornos mejor protegidos, y que sus datos requieren otro nivel de protección. El conjunto adecuado de técnicas y capacidades de encriptación de datos puede ayudar a proteger sus datos contra amenazas nuevas y emergentes.

05

Obstáculo 5: No poder priorizar y usar la moderna supervisión de actividad de datos

Obstáculo 5: No poder priorizar y usar la moderna supervisión de actividad de datos

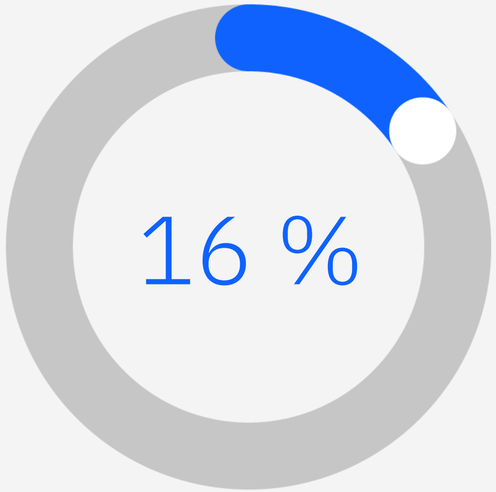
La supervisión de acceso y uso de datos es una parte fundamental de la estrategia de seguridad de datos. El líder de una organización debe saber quién, cómo y cuándo la gente accede a los datos. Esta supervisión debe englobar si estas personas deben tener acceso o no, si ese nivel de acceso es correcto y si representa un elevado riesgo para la empresa.

Los usuarios privilegiados suelen ser infractores en amenazas internas. Un plan de protección de datos debe incluir supervisión en tiempo real para detectar las cuentas de usuarios privilegiados que se usan para actividades sospechosas o no autorizadas.

Para evitar una posible actividad maliciosa, una solución debe llevar a cabo las siguientes tareas:

- Bloquear y poner en cuarentena actividades sospechosas basadas en violaciones de políticas.
- Suspender o cerrar sesiones basadas en conductas anómalas.
- Usar flujos de trabajo predefinidos y específicos para la normativa en todos los entornos de datos.
- Enviar alertas accionables a los sistemas de seguridad y operaciones de TI.

Ser responsable de la información relacionada con el cumplimiento y la seguridad de datos, y saber cuándo y cómo responder a posibles amenazas puede ser difícil. Con usuarios autorizados que acceden a múltiples fuentes de datos, incluidas las aplicaciones de bases de datos, de sistemas de archivos, de entornos principales, de entornos de nube y de SaaS, proteger los datos de todas estas interacciones puede parecer abrumador. El desafío reside en supervisar, capturar, filtrar, procesar y responder de manera efectiva a un gran volumen de actividad de datos. Sin tener implementado un plan correcto, su organización puede tener más información de actividad de la que puede procesar razonablemente y, a su vez, reducir el valor de la supervisión de las actividades de datos.



El 16 % de los incidentes observados mostraban abuso de cuentas válidas, en donde los adversarios obtenían las credenciales de cuentas existentes y abusaban de ellas con el objetivo de obtener el acceso.[3]

Usar una solución de supervisión de actividades de datos puede ayudar a los analistas de seguridad de datos a ahorrar un valioso tiempo.

Solución: Desarrollar una estrategia integral de cumplimiento y seguridad de datos

Para ese fin, cuando comience el proceso de seguridad de datos, debe medir el tamaño y el alcance de sus tareas de supervisión para hacer frente de manera adecuada a los requisitos y los riesgos. Esta actividad suele implicar adoptar un enfoque por fases que permita el desarrollo y el escalamiento de buenas prácticas en toda su empresa. Además, es fundamental tener conversaciones con las partes interesadas clave de la empresa y de TI al inicio del proceso para entender los objetivos empresariales a corto y largo plazo.

Estas conversaciones también deben capturar la tecnología que se necesitará para respaldar estas iniciativas clave. Por ejemplo, si su empresa está planeando establecer oficinas en un nuevo destino mediante una combinación de aplicaciones locales, de repositorios de datos en la nube y de SaaS, su estrategia de seguridad de datos debe evaluar de qué manera ese plan impactará en la postura de cumplimiento y seguridad de datos de la organización.
En este caso, los datos que son propiedad de la compañía ahora estarán sujetos a nuevos requisitos de cumplimiento y seguridad de datos, como el RGPD, la CPRA, la Ley General de Protección de Datos de Brasil (LGPD), etc.

También debe priorizar y enfocarse en una o dos fuentes que probablemente tengan los datos más confidenciales. Asegúrese de que sus políticas de seguridad de datos sean claras y detalladas para estas fuentes antes de extender estas prácticas al resto de su infraestructura.

Debe buscar una solución automatizada de supervisión de actividades de datos o archivos con análisis enriquecidos que pueda enfocarse en los riesgos clave y en las conductas inusuales de usuarios privilegiados.

Obstáculo 5: No poder priorizar y usar la moderna supervisión de actividad de datos

Aunque es esencial recibir alertas automatizadas cuando una solución de supervisión de actividades de datos o archivos detecta una conducta anormal, también debe poder tomar medidas rápidas cuando se descubren las anomalías o desviaciones de sus políticas de acceso a datos.Las acciones de protección deben incluir enmascaramiento o bloqueo dinámico de datos.

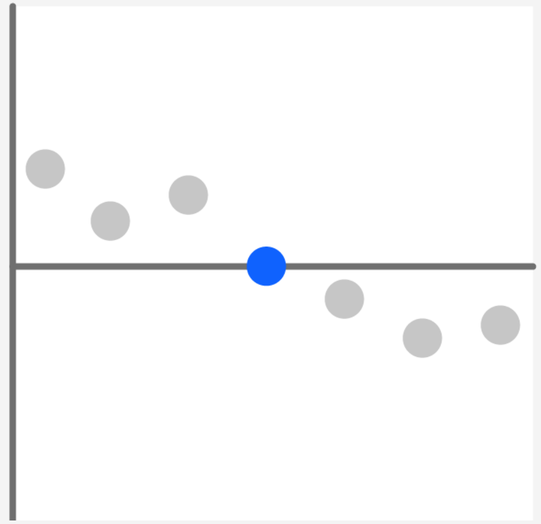
A medida que desarrolla sus planes de protección y supervisión de actividades de datos, suele ser útil considerar las siguientes preguntas:

- ¿Cuáles son mis dos fuentes de datos confidenciales más importantes?
- ¿Cuáles son las cinco o diez fuentes de datos que debo priorizar a continuación, según su volumen de datos confidenciales?
- ¿Ciertos endpoints o activos de la nube están asociados con datos con mayor riesgo?
- ¿Los datos confidenciales se mueven libremente entre entornos locales, híbridos y en la nube?
- ¿A qué usuarios debe otorgársele acceso a la fuente de datos y con qué condiciones?
- ¿Qué usuarios o cuentas privilegiadas de alto riesgo deben desactivarse o requieren una evaluación más minuciosa?
- ¿Mi solución de seguridad de datos admite supervisión de actividades en tiempo real y protección automatizada de datos?
- ¿La supervisión en tiempo real se implementa para hacer un seguimiento de los datos en los archivos que residen en almacenes de datos, como las bases de datos de lenguaje de consulta estructurado (SQL), las distribuciones de Hadoop, las plataformas Not only SQL (NoSQL), etc.?
- ¿Mi solución de supervisión tiene en cuenta los almacenes de datos que abarcan entornos multinube híbridos y me permite generar informes personalizados que se dirijan a las personas correctas y en el momento indicado?
- ¿Tengo las capacidades de análisis de riesgo y supervisión filtrada que se necesitan para priorizar de manera efectiva las tareas de riesgo, vulnerabilidades y remediación?

Cuanto más específico pueda ser sobre la supervisión de prioridades y los requisitos de protección, más efectiva será la solución para que pueda aplicar sus recursos disponibles de detección y respuesta.

USD 1,76 millones

Los ahorros promedio para las organizaciones que usan la IA y la automatización de seguridad de manera exhaustiva es de USD 1,76 millones, en comparación con las organizaciones que no lo hacen.[1]



06

¿Qué sigue?

¿Cómo puede evitar estos obstáculos comunes en la seguridad de datos, en especial, a medida que más empresas buscan entornos multinube híbridos? Todo empieza por reconocer el problema y preparar a su organización para que tome un enfoque proactivo y holístico, a fin de proteger los datos, independientemente de dónde residan.

Si su negocio tiene un entorno de TI híbrido y complejo, usted no puede darse el lujo de implementar un enfoque en silos para la seguridad de datos. Necesita sumar estrategias de cumplimiento y seguridad de datos que abarquen toda la infraestructura de datos y admitan todos los tipos de datos.

Los pasos siguientes que debe dar para proteger los valiosos datos de su organización:

- Crear un plan de cumplimiento y seguridad de datos que complemente los objetivos comerciales y tecnológicos a corto y largo plazo de su organización.
- Implementar ese plan con las personas, los procesos y las herramientas correctos.
- Planificar sus recursos para garantizar que su programa de cumplimiento y seguridad de datos pueda escalarse de manera efectiva a medida que su organización adopta tecnologías modernas.

La plataforma IBM Security® Guardium® es una solución de cumplimiento y seguridad de datos que está diseñada para ayudar a las organizaciones a adoptar un enfoque más inteligente y flexible para proteger datos confidenciales y críticos, sin importar dónde residan. Vea por qué puede ser una buena opción para su organización.

Más información →

Contáctenos →

Un estudio sobre la solución Guardium reveló un ROI de 406 % con beneficios de USD 5,86 millones en un período de tres años.[4]

07

¿Por qué IBM Security?

IBM® Security ayuda a proteger a las empresas y gobiernos más grandes del mundo con una cartera integrada de productos y servicios de seguridad infundidos con capacidades dinámicas de IA de seguridad y automatización. Esta cartera, respaldada por la mundialmente reconocida investigación de IBM® X-Force®, permite que las organizaciones prevean amenazas, protejan los datos a medida que se mueven y respondan con velocidad y precisión sin contener la innovación empresarial. Miles de organizaciones confían en IBM como su socio para evaluar, elaborar estrategias, implementar y gestionar transformaciones de seguridad.

IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo; supervisa más de 150 mil millones de eventos de seguridad cada día en más de 130 países, y se le han concedido más de 10.000 patentes de seguridad en todo el mundo.

Capítulo anterior

1. Cost of a Data Breach Report 2023, IBM, julio de 2023.

2. La necesidad de contar con el cumplimiento de datos en la actual era de la nube, Enterprise Strategy Group de TechTarget, abril de 2023.

3. Índice de X-Force Threat Intelligence de 2023, IBM Security, febrero de 2023.

4. The Total Economic Impact™ (TEI) de IBM Security Guardium Data Protection, un estudio de Forrester Consulting encargado por IBM, junio de 2023.

Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F.
IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América
Septiembre de 2023

Este documento está vigente a partir de la fecha inicial de publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Declaración de buenas prácticas de seguridad: Ningún sistema o producto de TI debe considerarse completamente seguro, y ningún producto, servicio o medida de seguridad puede ser completamente efectiva para prevenir el uso o acceso inadecuado. IBM no garantiza que ningún sistema, producto o servicio sea inmune o hará que su empresa sea inmune a la conducta maliciosa o ilegal de cualquier parte.

El cliente es responsable de garantizar el cumplimiento de las leyes y reglamentos aplicables. IBM no brinda asesoría legal ni declara o garantiza que sus servicios o productos aseguren que el cliente cumpla con cualquier ley o reglamento.