Cinco errores comunes en la seguridad de datos que debe evitar

Sepa cómo mejorar su postura de seguridad

IBM **Security**

Contenido

La seguridad de datos debe ser una prioridad principal para las empresas.

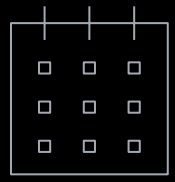
Incluso con el entorno de TI en un proceso de mayor complejidad y descentralización, es importante entender que muchas violaciones de seguridad se pueden prevenir. Si bien los desafíos y metas personales de seguridad pueden diferir de una empresa a otra, las organizaciones suelen cometer los mismos errores comunes al empezar enfrentar los problemas de seguridad. Es más, muchos líderes empresariales suelen aceptar estos errores como una práctica comercial normal.

Existen numerosos factores internos y externos que pueden llevar a ciberataques exitosos, incluyendo:

- Erosión de los perímetros de la red
- Superficies de ataque mayores, propiciadas por entornos de TI complejos
- Las crecientes demandas que los servicios de nube imponen a las prácticas de seguridad
- Una naturaleza cada vez más sofisticada de los crímenes cibernéticos
- Carencia sostenida de habilidades en ciberseguridad
- Falta de conciencia de los empleados con relación a los riesgos en la seguridad de datos

US$ 8,19 millones

Costo promedio de una violación de datos en los Estados Unidos en 2019[1]



245 días

Tiempo promedio para identificar y contener una violación de datos en los Estados Unidos[1]

¿Qué tan sólida es su práctica de seguridad de datos?

Veamos cinco de los errores más prevalentes (y evitables) en seguridad de datos que hacen que las organizaciones sean vulnerables a posibles ataques y cómo puede evitarlos.

Acelerar la regulación

Centralizar la seguridad

Establecer la propiedad

Evaluar las vulnerabilidades

Priorizar las actividades

Error 1

No avanzar más allá de la regulación

El cumplimiento de regulaciones no es necesariamente lo mismo que seguridad. Las organizaciones que enfocan sus limitados recursos de seguridad para cumplir con las auditorías o certificaciones pueden volverse complacientes. Se han dado muchas grandes violaciones de datos en organizaciones que, en el papel, estaban totalmente en normativa. Los siguientes ejemplos muestran cómo solo se enfocan en regulaciones puede reducir efectivamente la seguridad:

Cobertura incompleta:
Las empresas suelen tener problemas para abordar errores de configuración de la base de datos y políticas de acceso obsoletas antes de una auditoría anual. La evaluación de vulnerabilidades y riesgos debería ser una actividad constante.

Esfuerzo mínimo
Muchas organizaciones adoptan soluciones de seguridad de datos apenas para cumplir con requisitos legales o de asociados de negocios. La idea de "implementemos un estándar mínimo y volvamos a los negocios" puede ir en contra de buenas prácticas de seguridad.
Una seguridad de datos efectiva es una maratón, no una carrera corta.

Menor urgencia
Las empresas pueden volverse complacientes con relación a los controles de gestión cuando las reglamentaciones, como la Ley Sarbanes-Oxley (SOX) y el Reglamento general de protección de datos (GDPR), maduran. Mientras, con el tiempo, los líderes pueden volverse menos considerados sobre la privacidad, la seguridad y la protección de datos regulados, los riesgos y los costos asociados a la no regulación permanecen.

1,4 por día

se estima en 1,4 violaciones de datos en cuidados de la salud por día en 2019, a pesar de la Ley de Portabilidad y responsabilidad de seguros de salud (HIPAA).[2]

Omisión de datos no regulados
Activos, como la propiedad intelectual, pueden poner en riesgo su organización si se pierden o se comparten con personal no autorizado. Enfocarse solamente en la regulación puede tener como resultado que las organizaciones de seguridad pasen por alto y no protejan adecuadamente datos valiosos.

Solución

Reconocer y aceptar que la regulación es un punto de partida y no la meta

Las organizaciones de seguridad deben establecer programas estratégicos que protejan de forma consistente los datos críticos de sus negocios, en oposición a simplemente cumplir con los requisitos.

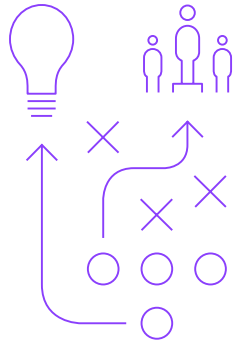
Los programas de seguridad y protección de datos deben incluir estas prácticas centrales:

- **Descubra y clasifique sus datos confidenciales** en almacenes de datos on-premises y en la nube.
- **Evaluar riesgos** con insights y analítica contextual.
- **Proteger datos confidenciales** por medio de políticas de cifrado y de acceso flexible.
- **Supervisar el acceso a los datos y a los patrones de uso** para descubrir rápidamente la actividad sospechosa.
- **Responder a amenazas** en tiempo real.
- **Simplificar la normativa** y sus informes.

El último elemento incluye responsabilidad legal relativa a la normativa regulatoria, las posibles pérdidas que puede sufrir un negocio y los costos potenciales de esas pérdidas más allá de las multas por no regulación.

En última instancia, usted debe pensar holísticamente sobre el riesgo y el valor de los datos que quiere proteger.

Ver la regulación como una oportunidad para innovar y elevar los estándares de seguridad para dar soporte a sus negocios.



Error 2

No reconocer la necesidad de una seguridad de datos centralizada

Sin mandatos más amplios de normativas que cubran la privacidad y seguridad de los datos, los líderes de las organizaciones pueden perder de vista la necesidad de una seguridad de datos constante a nivel de toda la empresa.

Para empresas con entonos de multicloud híbrido que cambian y crecen constantemente, los nuevos tipos de fuentes de datos pueden aparecer diaria o semanalmente y dispersar mucho los datos confidenciales.

Los líderes de empresas que están aumentando y expandiendo sus infraestructuras de TI pueden dejar de reconocer los riesgos que representan sus superficies de ataque cambiantes. Pueden faltarles una visibilidad y un control adecuados cuando sus datos confidenciales se mueven en un entorno de TI cada vez más complejo y dispar. No adoptar controles de protección, seguridad y privacidad de datos end-to-end, especialmente dentro de entornos complejos, puede representar una omisión muy costosa.

Soluciones operativas de seguridad compartimentadas pueden causar otros problemas. Po ejemplo, organizaciones con un centro de operaciones de seguridad (SOC) y una solución de gestión de información de información y eventos de seguridad (SIEM) pueden desatender la alimentación de esos sistemas con insights obtenidos de su solución de seguridad de datos. Del mismo modo, la falta de interoperabilidad entre el personal, los procesos y las herramientas de seguridad puede dificultar el éxito de cualquier programa de seguridad.

El cifrado, la gestión de la continuidad comercial, la integración de la seguridad en el proceso de desarrollo de software (DevSecOps) y compartir la inteligencia de amenazas pueden ayudar a reducir los costos de violaciones de datos.[1]

Solución

Sepa dónde residen sus datos confidenciales, incluyendo repositorios on-premises y en la nube

La protección de los datos confidenciales debería darse en conjunto con sus esfuerzos más amplios en seguridad. Además de entender dónde están almacenados sus datos confidenciales, usted también necesita saber cuándo y cómo se accede a ellos, aunque esta información cambie rápidamente. Asimismo, usted debe trabajar para integrar la seguridad de datos su programa de seguridad general para permitir una comunicación estrechamente alineada entre tecnologías. Una solución de seguridad de datos que opera entre entornos y plataformas disímiles puede ayudar en este proceso.

Por lo tanto, ¿cuál es el momento adecuado para integrar la seguridad de datos con otros controles de seguridad como parte de una práctica de seguridad más holística? Aquí tenemos algunas señales que sugieren que su organización puede estar lista para dar el paso siguiente:

Riesgo de perder datos valiosos
El valor de los datos personales, sensibles y propietarios de su organización es tan grande que su pérdida causaría un daño significativo a la viabilidad de su negocio.

Implicaciones regulatorias
Su organización recolecta y almacena datos con requisitos legales, tales como números de tarjetas de crédito, otras informaciones de pagos o datos personales.

La protección de los datos confidenciales debería darse en conjunto con sus esfuerzos más amplios en seguridad.

Falta de supervisión de seguridad
Su organización ha crecido a tal punto que es difícil hacer un seguimiento y asegurar todos los terminales de la red, incluyendo instancias en la nube. Por ejemplo, ¿tiene usted una idea clara de dónde, cuándo y como se almacenan, se comparten y se accede a sus datos en todo su almacenamiento de on-premises y en la nube?

Evaluación inadecuada
Su organización ha adoptado un abordaje fragmentado en el que no hay una clara comprensión de lo que se gasta exactamente en todas sus actividades de seguridad. Por ejemplo, ¿posee usted procesos establecidos para medir de forma precisa su rentabilidad (ROI) en términos de recursos destinados a reducir los riesgos de la seguridad de datos?

Si alguna de estas situaciones se aplica a su organización, usted debe considerar adquirir las habilidades y soluciones en seguridad necesarias para integrar la seguridad de datos en su práctica de seguridad más amplia existente.

Error 3

No definir a quién pertenece la responsabilidad de los datos

Incluso siendo conscientes de la necesidad de la seguridad de datos, muchas empresas no cuentan con alguien responsable específicamente de proteger los datos confidenciales. Esta situación suele volverse evidente durante un incidente de seguridad de datos o de auditoría cuando la organización se encuentra bajo presión para descubrir quién es realmente responsable.

Los altos ejecutivos pueden dirigirse hacia el director de información (CIO) quien podría decir "Nuestro trabajo es mantener el sistema en funcionamiento. Vayan a hablar con alguien de mi equipo de TI". Esos empleados de TI pueden ser responsables de muchas bases de datos en las que residen datos confidenciales y aún así no contar con presupuesto para seguridad.

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 por el negocio como un todo. Pueden ofrecer consejos a los gerentes de diferentes líneas de negocios (LOB) dentro de una empresa, pero en muchas otras, no hay nadie que sea explícitamente responsable de los datos en sí. Para una organización, los datos son uno de sus activos más valiosos. Sn embargo, sin la responsabilidad de la propiedad, asegurar datos confidenciales apropiadamente se convierte en un desafío.

El 74 %

de las organizaciones consultadas dicen que la falta de habilidades en ciberseguridad ha tenido un impacto en su organización.[3]

En 2018, el 67,9 % de las firmas encuestadas informaron tener un director ejecutivo de datos (CDO). Sin embargo, el rol sigue estando mal definido".[4]

Informe NewVantage
Big Data and AI Executive Survey
2019, Executive Summary of Findings

Lea el estudio →

Solución

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

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

Compartidos entre unidades de negocios

Localizados en infraestructuras de multicloud híbrida

Almacenados en dispositivos móviles

Un director de datos (CDO) o un director de protección de datos (DPO) pueden manejar estas obligaciones. De hecho, empresas con sede en Europa o que hacen negocios con sujetos de datos de la Unión Europea enfrentan mandatos de GDPR que les exigen contar con un DPO. Este prerrequisito reconoce que los datos confidenciales, en este caso, información personal, tienen un valor que va más allá del LOB que usa los datos. Asimismo, el requisito hace énfasis en que las empresas tengan un rol específicamente designado para ser responsable de los activos de datos. Considere los siguientes objetivos y responsabilidades para elegir un CDO o un DPO:

Conocimiento técnico y sentido comercial
Evalúe el riesgo y cree un caso comercial práctico que líderes de negocios no técnicos puedan entender, con relación a inversiones adecuadas en seguridad.

Implementación estratégica
Dirija un plan a nivel técnico que aplique detección, respuesta y seguridad de datos para proporcionar protecciones.

Liderazgo en regulación
Entender los requisitos de normativas y saber cómo mapear dichos requisitos para los controles de seguridad de datos, para que su negocio esté en cumplimiento con las normas.

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

Flexibilidad y escala
Saber cuándo y cómo ajustar la estrategia de seguridad de datos, como expandir las políticas de acceso y uso de datos a nuevos entornos, integrando herramientas más avanzadas.

División del trabajo
Establezca expectativas con proveedores de servicios de nube, con relación a acuerdos de nivel de servicio (SLA) y las responsabilidades asociadas a los riesgos de seguridad de datos y remediación.

Plan de respuesta a violación de datos
Finalmente, esté listo para jugar un papel importante para establecer un plan estratégico de respuesta y mitigación de fallas.

En última instancia, el CDO o DPO deberá liderar la promoción de la colaboración en seguridad de datos entre los equipos y en toda la empresa, ya que todos necesitan trabajar juntos para asegurar efectivamente los datos corporativos. Esta colaboración puede ayudar al CDO o DPO a supervisar los programas y las protecciones que su organización necesita para ayudar a proteger sus datos confidenciales.

Error 4

No atender las vulnerabilidades conocidas

Las fallas de alto perfil en las empresas suelen ser el resultado de vulnerabilidades conocidas que no fueron corregidas inclusive después de la publicación de los parches. Dejar de parchar rápidamente vulnerabilidades conocidas pone en riesgo los datos de su organización, porque los cibercriminales buscan activamente estos puntos débiles de entrada.

Sin embargo, para muchos negocios es un desafío implementar los parches rápidamente debido al nivel de coordinación necesario entre TI, seguridad y grupos operativos. Además, los parches suelen requerir pruebas para ver si no interrumpen procesos o si introducen una nueva vulnerabilidad.

En entornos de nube, a veces es difícil saber si un servicio contratado o un componente de aplicación debería ser parchado. Incluso si se encuentra una vulnerabilidad en un servicio, sus usuarios suelen no tener control sobre el proceso de remediación del proveedor del servicio.

El 51 %

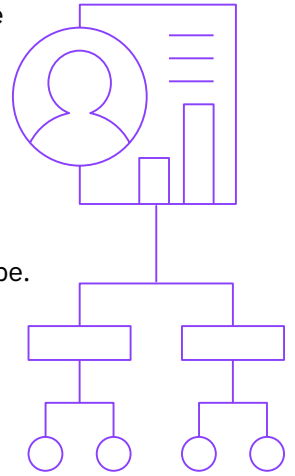
de las fallas registradas en 2019 fueron causadas por ataques maliciosos. Los ataques maliciosos son la causa principal más frecuente y más cara de las fallas.[1]

Solución

Establecer un programa de gestión de vulnerabilidades efectivo con la tecnología apropiada para dar soporte a su crecimiento

La gestión de vulnerabilidades envuelve típicamente algunos de los siguientes niveles de actividad:

- Mantener un inventario y un estado de referencia precisos de sus activos de datos.
- Realizar revisiones y evaluaciones frecuentes en busca de vulnerabilidades en toda su infraestructura, incluso entre los activos en la nube.
- Priorizar la remediación de vulnerabilidades que considere la probabilidad de que una vulnerabilidad sea explotada y el impacto que dicho evento tendría en su negocio.
- Incluir gestión y respuesta a vulnerabilidades como parte del SLA con proveedores de servicios tercerizados.
- Enmascarar datos confidenciales o personales siempre que sea posible. Cifrado, tokenización y redacción son tres opciones para lograr este fin.
- Utilizar una gestión apropiada de claves de cifrado, asegurando que las claves de cifrados estén almacenadas de forma segura y en un ciclo apropiado para mantener protegidos sus datos cifrados.



Incluso dentro de un programa de gestión de vulnerabilidades maduro, ningún sistema es perfecto. Asumiendo que las intrusiones pueden ocurrir incluso en los entornos mejor protegidos, sus datos requieren otro nivel de protección. El conjunto adecuado de técnicas y capacidades de cifrado de datos puede ayudar a proteger sus datos de amenazas nuevas y emergentes.

Error 5

No priorizar y aprovechar la supervisión de la actividad de datos

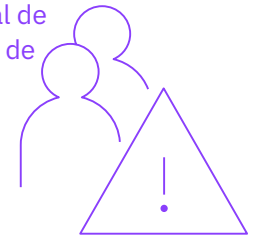
Supervisar el acceso y el uso de datos es parte esencial de cualquier estrategia de seguridad de datos. El líder de una organización debe saber quién, cómo y cuándo se accede a los datos. Esta supervisión debe abarcar si estas personas deben tener acceso, si ese nivel de acceso es correcto y si representa un riesgo elevado para la empresa.

Las identificaciones de usuarios privilegiados son responsables comunes de las amenazas internas.5 Un plan de protección de datos debe incluir supervisión en tiempo real para detectar cuentas de usuarios privilegiados utilizadas para actividades sospechosas o no autorizadas. Para prevenir la posible actividad maliciosa, una solución debe realizar las siguientes tareas:

- Bloquear y poner en cuarentena la actividad sospechosa, con base en violaciones a las políticas.
- Suspender o cerrar sesiones con base en comportamiento anómalo.
- Usar flujos de trabajo específicos para las reglamentaciones en todos los entornos de datos.
- Enviar alertas accionables a los sistemas de seguridad de TI y de operaciones.

El costo promedio global de una amenaza interna es de

US$ 11,45 millones.[6]



Dar cuenta de la información relativa a la seguridad y a la regulación, así como saber cuándo y cómo responder a posibles amenazas puede ser difícil. Con usuarios autorizados accediendo a fuentes múltiples de datos, incluyendo bases de datos, sistemas de archivos, entornos de mainframe y entornos de nube, supervisar y grabar datos de todas estas interacciones puede parecer abrumador. El desafío reside en supervisar, capturar, filtrar, procesar y responder de forma efectiva a enormes volúmenes de actividad de datos. Sin un plan adecuado establecido, su organización puede tener más información de actividades de la que puede procesar razonablemente y, a su vez, reducir el valor de la supervisión de la actividad de datos.

Solución

Desarrollar una estrategia amplia de detección y protección de datos

Para eso, al iniciar un camino de seguridad de datos, usted necesita mensurar y estimar sus esfuerzos de supervisión para abordar de forma adecuada los riesgos y requisitos. Esta actividad suele implicar adoptar un abordaje por etapas que permite mejores prácticas de desarrollo y escala en toda su empresa. Por otra parte, es crítico establecer conversaciones con participantes clave del negocio y de TI al inicio del proceso para entender los objetivos comerciales de corto y de largo plazo.

Estas conversaciones también deben abarcar la tecnología que será necesaria para dar soporte a sus iniciativas clave. Por ejemplo, si el negocio está planeando establecer oficinas en un nuevo territorio usando una combinación de repositorios de datos on-premises y alojados en la nube, su estrategia de seguridad de datos debe evaluar de qué forma impactará ese plan en la seguridad de datos y la postura de regulación de normas de la organización. Si, por ejemplo, los datos de propiedad de la empresa ahora estarán sometidos a nuevos requisitos de seguridad de datos y de requisitos de cumplimiento de regulaciones, tales como GDPR, la Ley de Privacidad del consumidor de California (CCPA), la Ley general de protección de datos (LGPD) de Brasil, etc.

Usted 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 son claras y detalladas para estas fuentes antes de extender estas prácticas al resto de su infraestructura.

El costo total promedio de una violación de datos fue un

El 95 % más alto

en organizaciones sin automatización implementada en 2019.[1]

US$ 5,16 millones **sin automatización.**[1]

US$ 2,65 millones **con automatización totalmente implementada.**[1]

Debe buscar una solución de supervisión de actividad de datos o de archivos que cuente con una rica analítica que pueda enfocarse en riesgos clave y comportamientos inusuales de usuarios privilegiados. Aunque es esencial recibir alertas automáticas cuando una solución de supervisión de actividad de datos o de archivos detecta un comportamiento anormal, usted debe también poder reaccionar rápidamente cuando se descubren anormalidades 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 supervisión y protección de la actividad de datos, suele esperarse que considere las siguientes preguntas:

- ¿Cuáles son mis dos fuentes principales de datos confidenciales?
- ¿Cuáles son las cinco a diez fuentes de datos debo priorizar después, con base en su volumen de datos confidenciales?
- ¿Hay algunos terminales o activos en la nube asociados a datos de mayor riesgo?
- ¿Los datos confidenciales se están moviendo libremente entre entornos on-premises, híbridos y de nube?
- ¿Qué usuarios deben tener acceso a las fuentes de datos y en qué condiciones?
- ¿Qué usuarios de alto riesgo o cuentas privilegiadas deben ser desconectados o necesitan un seguimiento más de cerca?
- ¿Mi solución de seguridad de datos soporta capacidades de supervisión de actividad en tiempo real y de protección automática de datos?
- ¿Está instalada la supervisión en tiempo real para seguir datos en archivos que residen en almacenes de datos, tales como bases de datos Structured Query Language (SQL), distribuciones Hadoop, plataformas Not only SQL (NoSQL), etc.?
- ¿Mi solución de supervisión da cuenta de almacenes de datos que abarcan entornos de multicloud híbrida y me permite generar informes personalizados dirigidos a la persona adecuada en el momento adecuado?
- ¿Cuento con las capacidades de analítica de riesgos y de supervisión filtrada necesarias para priorizar de forma efectiva los riesgos, las vulnerabilidades y los esfuerzos de remediación?

Mientras más específico usted pueda ser sobre las prioridades de supervisión y los requisitos de protección, más efectiva será la solución en la aplicación de sus recursos de detección y respuesta disponibles.

¿Y después?

¿Cómo puede evitar estos cinco errores habituales de seguridad, especialmente a medida que más empresas buscan entornos de multicloud híbrida? Todo empieza por reconocer el problema y preparar su organización para un abordaje proactivo y holístico de la seguridad de datos, independientemente de dónde residan.

Si su negocio tiene un entorno de TI complejo e híbrido, no puede darse el lujo de tener un abordaje compartimentado para la seguridad de datos. Usted debe agregar estrategias de seguridad de datos que abarquen toda su infraestructura de datos y soporten todos sus tipos de datos.

Los próximos pasos inmediatos que puede dar para proteger los datos valiosos de su organización incluyen:

- Construir una estrategia de seguridad de datos que dé soporte a los objetivos tecnológicos y comerciales de su organización a corto y a largo plazo.
- Implementar esa estrategia con las personas, los procesos y las herramientas adecuados
- Planificar sus recursos para asegurar que su programa de seguridad de datos y de regulación puede escalar efectivamente a medida que su organización adopta tecnologías modernas

La plataforma de protección de datos IBM® Security Guardium® está diseñada para ayudar a las organizaciones a asumir un enfoque más inteligente y flexible sobre la protección de datos críticos dondequiera que residan. Vea por qué puede ser adecuada para su organización.

Más información en ibm.com/guardium.

> 4 semanas

La mayoría de las organizaciones reconoce el valor de Guardium en menos de un mes.[7]

¿Por qué IBM Security?

IBM Security ofrece uno de los portafolios de productos y servicios de seguridad empresarial más avanzados e integrados. El portafolio, con el soporte de la mundialmente conocida IBM X-Force® de investigación y desarrollo, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger a sus personas, infraestructuras, datos y aplicaciones de forma holística. Ofrece soluciones para la gestión de identidades y de acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de terminales, seguridad de red y más. Estas soluciones permiten a las organizaciones gestionar riegos efectivamente e implementar seguridad integrada para móviles, nubes, redes sociales y otras arquitecturas comerciales empresariales.

IBM opera una de las mayores organizaciones de investigación, desarrollo y entrega de seguridad, supervisando más de

60 mil millones de

eventos de seguridad por día en más de 130 países.

IBM posee más de 3.700 patentes de seguridad

Para obtener más información sobre IBM Security, visite nuestro sitio web.

Dé el próximo paso

Entre en contacto con nuestro especialista que le ayudará a superar los desafíos de ciberseguridad.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América,
abril de 2020

Este documento se actualizó por última vez en la fecha de su 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. Los ejemplos de cliente y datos de rendimiento mencionados fueron presentados solamente para propósitos ilustrativos. Los resultados reales de rendimiento pueden variar dependiendo de configuraciones específicas y condiciones de operación. Es responsabilidad del usuario evaluar y verificar la operación de cualquier otro producto o programa con productos o programas de IBM. LA INFORMACIÓN DE ESTE DOCUMENTO ES SUMINISTRADA "COMO ESTÁ" SIN NINGUNA GARANTÍA, EXPRESA O IMPLÍCITA, LO QUE INCLUYE NINGUNA GARANTÍA DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO ESPECÍFICO Y NINGUNA GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. Los productos de IBM están garantizados de conformidad con los términos y condiciones de los contratos en virtud de los cuales se suministran.

El cliente es responsable de garantizar la conformidad con las leyes y los reglamentos aplicables. IBM no proporciona asesoría legal, ni manifiesta ni garantiza que sus servicios o productos garanticen que el cliente cumple con cualquier ley o regulación.

Declaración de buenas prácticas de seguridad: La seguridad de los sistemas de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta al acceso indebido dentro y fuera de su empresa. El acceso inadecuado puede dar lugar a la modificación, destrucción, apropiación o utilización indebidas de la información, así como también a daños a sus sistemas o a la utilización indebida de éstos, incluyendo su uso para atacar a otros. Ningún producto o sistema de TI deberá considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente eficaz en la prevención de la utilización o el acceso indebidos. Los productos, sistemas y servicios de IBM están diseñados para ser parte de un enfoque de seguridad legal y amplio que necesariamente involucrará procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para ser más efectivos IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O HAGA A SU EMPRESA INMUNE, A LA CONDUCTA MALINTENCIONADA O ILEGAL DE CUALQUIER TERCERO.

1 "Cost of a Data Rreach report 2019." *IBM Security*. databreachcalculator.mybluemix.net/executive-summary

2 "Healthcare Data Breach Statistics." *HIPAA Journal*. www.hipaajournal.com/healthcare-data-breach-statistics

3 Jon Oltsik. "The Life and Times of Cybersecurity Professionals 2018." *Enterprise Strategy Group and Information Systems Security Association International*, April 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, "Big Data and AI Executive Survey 2019 Executive Summary of Findings." *NewVantage Partners*, 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. "Why Privileged Account Management Is Key to Preventing Insider Threats." *Security Intelligence*, June 20, 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 "Cost of Insider Threats: Global Report 2020." *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 "Ponemon Report: Client Insights on Data Protection with Guardium." *Ponemon Institute*, August 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

SEL03144-USEN-02