Cinco errores comunes a evitar en la seguridad de datos

Descubra cómo mejorar su seguridad

IBM Security

Contenido

La seguridad de los datos debe ser una máxima prioridad para las empresas, y por un buen motivo.

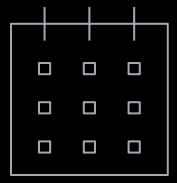
Incluso cuando el entorno TI se vuelve cada vez más descentralizado y complejo, es importante saber que muchas brechas de seguridad son evitables. Aunque los retos y los objetivos de la seguridad puedan ser distintos para cada empresa, a menudo las organizaciones cometen los mismos errores cuando afrontan la seguridad de los datos. Es más, muchos líderes de las empresas muchas veces aceptan estos errores como una práctica normal del negocio.

Existen varios factores internos y externos que pueden llevar a ciberataques exitosos, como, por ejemplo:

- Erosión de los perímetros de red
- Entornos de TI más complejos hacen que aumenten las posibles superficies de ataque
- Incremento de servicios en la nube que aumenta las demandas de seguridad
- Naturaleza cada vez más sofisticada de los ciberdelitos
- Escasez persistente de habilidades en ciberseguridad
- Falta de conciencia de los empleados de los riesgos de la seguridad de datos

8,19 millones de dólares

Coste medio de una brecha de datos en Estados Unidos en 2019[1]



245 días

Tiempo medio para identificar y contener una brecha de datos en Estados Unidos[1]

¿Cómo de relevante e importante es su práctica de seguridad de datos?

Veamos los cinco errores más comunes – y evitables – en la seguridad de datos que hacen que las empresas sean vulnerables a ataques potenciales y cómo puede evitarlos.

Acelerar el cumplimiento

Centralizar la seguridad

Establecer la propiedad

Evaluar las vulnerabilidades

Priorizar actividades

Error 1

Incapacidad para ir más allá del cumplimiento

El cumplimiento no implica necesariamente seguridad. Las organizaciones que centran sus recursos limitados de seguridad en cumplir auditorías o certificaciones pueden volverse complacientes. Muchas grandes brechas de datos se han producido en organizaciones que cumplían todas las normativas sobre el papel. Los siguientes ejemplos muestran cómo limitarse únicamente al cumplimiento puede disminuir la seguridad efectiva:

Cobertura incompleta
A menudo, las empresas intentan resolver fallos de configuración de bases de datos y políticas de acceso desfasadas antes de una auditoría anual. Las evaluaciones de vulnerabilidades y riesgos deben ser actividades que se hagan de una manera continuada.

Mínimo esfuerzo
Muchas empresas adoptan soluciones de seguridad de datos solo para cumplir requisitos legales o de sus colaboradores. Esta mentalidad de "implementemos un estándar mínimo y volvamos al negocio" puede ir en contra de buenas prácticas de seguridad. La seguridad de datos eficaz es una maratón, no un sprint.

Urgencia desvanecida
Las empresas pueden volverse autocomplacientes con la gestión de los controles cuando las normativas, como por ejemplo la ley Sarbanes-Oxley (SOX) y el Reglamento general de protección de datos (GDPR), maduran. Aunque con el tiempo los líderes puedan ser menos considerados acerca de la privacidad, la seguridad y la protección de datos regulados, los riesgos y costes asociados al incumplimiento siguen siendo los mismos.

1,4 al día

1,4 brechas de datos sanitarios al día estimados en 2019, a pesar de la legislación Health Insurance Portability and Accountability Act (HIPAA).[2]

Omisión de datos no regulados
Los activos, como, por ejemplo, la propiedad intelectual, pueden poner en riesgo su organización si se pierde o se comparte con personal no autorizado. Centrarse solamente en el cumplimiento puede llevar a las organizaciones a pasar por alto la seguridad y no proteger datos valiosos.

Solución

Reconocer y aceptar que el cumplimiento es un buen punto de partida, no el objetivo

Los departamentos de seguridad de datos deben establecer programas estratégicos que protejan de forma consistente los datos críticos de sus empresas, en lugar de simplemente responder a los requisitos de cumplimiento.

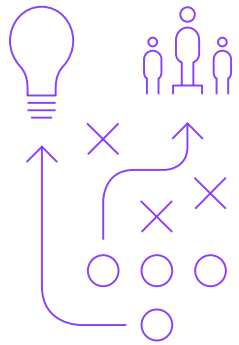
Los programas de protección y seguridad de datos deben incluir las siguientes prácticas básicas:

- **Descubrir y clasificar datos sensibles** almacenados on-premise o en la nube.
- **Evaluar el riesgo** con conocimiento contextual y analítico.
- **Proteger los datos sensibles** mediante el cifrado y políticas de acceso flexibles.
- **Supervisar el acceso a los datos y los patrones de uso** para descubrir rápidamente la actividad sospechosa.
- **Responder a las amenazas** en tiempo real.
- **Hacer más sencillo el cumplimiento** y la elaboración de informes.

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

Finalmente, debe pensar de forma global en el riesgo y el valor de los datos que busca proteger.

Ver el cumplimiento como una oportunidad para innovar y elevar los estándares de seguridad para dar apoyo a su empresa.



Error 2

Incapacidad para reconocer la necesidad de tener una seguridad de datos descentralizada

Sin reglamentos de cumplimiento más amplios que cubran la seguridad y privacidad de datos, los líderes de las organizaciones pueden perder de vista la necesidad de tener una seguridad de datos consistente a nivel de toda la empresa.

Para las empresas con entornos multicloud híbridos, que cambian y crecen constantemente, cada día o cada semana pueden aparecer nuevas fuentes de datos que dispersan los datos sensibles.

Los líderes de compañías que estén ampliando sus infraestructuras de TI pueden no reconocer el riesgo que plantea su superficie de ataque cambiante. Pueden carecer de una visibilidad y control adecuados, mientras sus datos sensibles se mueven por un entorno TI cada vez más complejo y dispar. La incapacidad para adoptar controles de protección, seguridad y privacidad de datos de extremo a extremo – especialmente en entornos complejos – puede llevar a tener que realizar una supervisión muy costosa.

El uso de soluciones de seguridad en silos puede causar problemas adicionales. Por ejemplo, las organizaciones con un centro de operaciones de seguridad (SOC) y una solución de gestión de eventos e información de seguridad (SIEM) pueden desatender la alimentación de dichos sistemas con los conocimientos obtenidos de sus soluciones de seguridad de datos. De modo similar, una falta de interoperabilidad entre personas, procesos y herramientas de seguridad pueden obstaculizar el éxito de cualquier programa de seguridad.

El cifrado, la gestión de la continuidad de negocio, la integración de la seguridad en un proceso de desarrollo de software (DevSecOps) y el uso compartido de información de amenazas puede ayudar a disminuir los costes de las brechas de datos.[1]

Solución

Saber dónde residen los datos sensibles, incluyendo los repositorios on-premise y en la nube

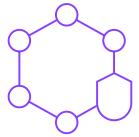
La protección de los datos sensibles debe producirse a la par que un mayor esfuerzo de seguridad. Además de saber dónde se almacenan los datos sensibles, también es necesario saber cuándo y cómo se accede a ellos – aún cuando esta información cambie rápidamente. Adicionalmente, debe integrar las políticas y conocimientos de la protección y seguridad de los datos, con su programa global de seguridad para que exista una comunicación alineada entre las tecnologías. Una solución de seguridad de datos que funcione en plataformas y entornos dispares puede ser útil en este proceso.

Entonces, ¿cuándo es el momento más adecuado para integrar la seguridad de datos con otros controles de seguridad como parte de una práctica más global de seguridad? Estos son algunos de los signos que sugieren que la organización puede estar preparada para dar este siguiente paso:

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

Implicaciones normativas
La organización recopila y almacena datos con requisitos legales, tales como números de tarjeta de crédito, otra información de pago o datos personales.

La protección de los datos sensibles debe producirse conjuntamente con sus esfuerzos más amplios de seguridad.



Falta de supervisión de la seguridad
La organización ha crecido hasta tal punto que es difícil hacer un seguimiento y asegurar todos los endpoints, incluidas las instancias en la nube. Por ejemplo, ¿tiene una idea clara de dónde, cuándo y cómo se almacenan, se comparten y se accede a los datos en sus almacenes de datos on-premise y en la nube?

Evaluación inadecuada
Su empresa ha adoptado un enfoque fragmentado en el que no existe un claro conocimiento de lo que se está gastando exactamente entre todas las actividades de seguridad. Por ejemplo, ¿cuenta con procesos para medir con precisión el retorno de la inversión (ROI) en términos de recursos que se asignan para reducir el riesgo de seguridad de los datos?

Si alguna de estas situaciones se produce en su organización, debe considerar la adquisición de soluciones y habilidad en seguridad necesarias para integrar la seguridad de datos en la práctica más amplia de seguridad existente.

Error 3

Incapacidad para definir de quién es la responsabilidad de los datos

Aunque sean conscientes de la necesidad de la seguridad de datos, muchas compañías no tienen ninguna persona específicamente responsable de la protección de datos sensibles. Esta situación se hace muchas veces patente durante una incidencia de seguridad de datos o una auditoría, cuando la organización está bajo la presión para encontrar quién es responsable.

Los altos ejecutivos pueden acudir al director de tecnologías de la información (CIO), que podría decir, “Nuestro trabajo es mantener los sistemas clave en funcionamiento. Habla con alguien de mi personal TI”. Esos empleados de TI pueden ser responsables de varias bases de datos en las cuales residen datos confidenciales y aún así carecen de un presupuesto para la seguridad.

Habitualmente, el equipo del director de seguridad de la información (CISO) no es directamente responsable de los datos que fluyen por toda la empresa. Pueden aconsejar a los diferentes directores de línea de negocio (LOB) de una empresa, pero, en muchas compañías, nadie es explícitamente responsable de los datos en sí. Para una organización, los datos son uno de los activos más valiosos. Aún así, sin una responsabilidad de la propiedad, la protección adecuada de los datos sensibles se convierte en un desafío.

74%

de las organizaciones encuestadas afirman que la escasez de habilidades en ciberseguridad ha impactado su organización.[3]

En 2018, el 67,9 % de las empresas encuestadas afirmaron tener un director de datos (CDO). Sin embargo, la función sigue estando poco definida”.[4]

NewVantage Report
Big Data and AI Executive Survey 2019,
Resumen ejecutivo de conclusiones

Lea el estudio →

Solución

Contratar a un CDO o DPO dedicado al bienestar y seguridad de los datos sensibles y críticos

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

Compartidos entre varias unidades de negocio

Ubicados en infraestructuras multicloud híbridas

Almacenados en dispositivos móviles

Un director de datos (CDO) o delegado de protección de datos (DPO) puede encargarse de estas tareas. De hecho, las compañías con sede en Europa o que tratan con sujetos de datos europeos se enfrentan al reglamento del GDPR, que las obligan a tener un DPO. Este requisito previo reconoce que los datos sensibles – en este caso información personal – tienen un valor que va más allá del LOB que utiliza dichos datos. Adicionalmente, el requisito enfatiza que las empresas tienen un papel diseñado específicamente para ser responsable de los datos. Considere los siguientes objetivos y responsabilidades a la hora de elegir un CDO o DPO:

Conocimiento técnico y sentido comercial
Evaluar el riesgo y crear un business case práctico en relación con las inversiones en seguridad, que los líderes de negocio no técnicos puedan entender.

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

Liderazgo en cumplimiento
Comprender los requisitos de cumplimiento y saber cómo correlacionar dichos requisitos con os controles de seguridad de datos para que la empresa cumpla la normativa.

Supervisión y evaluación
Supervisar el entorno de las amenazas y medir la eficacia del programa de seguridad de datos.

Flexibilidad y escalado
Saber cuándo y cómo ajustar la estrategia de seguridad de datos, como la ampliación del acceso a datos y las políticas de uso en los nuevos entornos, mediante la integración de herramientas más avanzadas.

División del trabajo
Definir las expectativas con los proveedores de servicios en la nube en relación a los acuerdos de nivel de servicio (SLA) y las responsabilidades asociadas al riesgo y corrección de la seguridad de los datos.

Plan de respuesta a brechas de datos
Finalmente, estar preparados para jugar un papel clave en el diseño de un plan estratégico de respuesta y corrección de infracciones.

Por último, el CDO o DPO debe liderar el fomento de la colaboración en la seguridad de los datos, entre los distintos equipos y en toda la empresa, ya que todo el mundo debe colaborar para proteger eficazmente los datos corporativos. Esta colaboración puede ayudar al CDO o DPO a supervisar los programas y protecciones que necesita su empresa para proteger los datos sensibles.

Error 4

Incapacidad para resolver vulnerabilidades conocidas

Las brechas de perfil alto en las empresas son a menudo el resultado de vulnerabilidades conocidas en las que no se han aplicado las revisiones incluso después de haberse publicado dichas revisiones. La incapacidad para revisar rápidamente las vulnerabilidades conocidas pone en riesgo los datos de su organización, ya que los ciberdelincuentes buscan activamente estos puntos de entrada fáciles.

Sin embargo, muchas compañías tienen dificultades para implementar rápidamente las revisiones debido al nivel de coordinación necesario entre los grupos de TI, seguridad y operativo. Es más, muchas veces las revisiones deben probarse para ver si no interrumpen un proceso o introducen una nueva vulnerabilidad.

En entornos cloud, a veces es difícil saber si un servicio contratado o un componente de aplicación debe corregirse. Incluso si se encuentra una vulnerabilidad en un servicio, muchas veces sus usuarios no tienen el control del proceso de remediación del proveedor de servicios.

51%

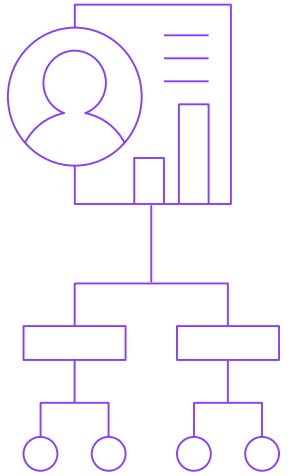
de las brechas registradas en 2019 fueron causadas por ataques malintencionados. Los ataques malintencionados son la causa más habitual y costosa de las brechas.[1]

Solución

Establecer un programa de gestión de vulnerabilidades eficaz con la tecnología adecuada para apoyar su crecimiento

Normalmente, la gestión de vulnerabilidades implica tener alguno de los siguientes niveles de actividad:

- Mantener un inventario preciso y un estado de referencia de los activos de datos.
- Realizar exploraciones frecuentes y evaluaciones de vulnerabilidades en toda la infraestructura, incluidos los activos en la nube.
- Priorizar la remediación de vulnerabilidades que considere la probabilidad de que se explote la vulnerabilidad y el impacto que dicha situación tendría en la empresa.
- Incluir la gestión de vulnerabilidades y la reacción ante ellas en el SLA con proveedores de servicio de terceros.
- Enmascarar los datos sensibles o personales siempre que sea posible. El cifrado, la tokenización y la redacción son tres opciones para lograr este fin.
- Emplear una gestión adecuada de claves de cifrado, asegurándose de que las claves se almacenan de forma segura y que se cambian periódicamente para mantener la seguridad de los datos cifrados.



Ningún sistema es perfecto, ni siquiera los programas de gestión de vulnerabilidades más maduros. Asumiendo que pueden producirse intrusiones incluso en los entornos mejor protegidos, los datos necesitan otro nivel de protección. El conjunto adecuado de técnicas y capacidades de cifrado de datos puede ayudar a proteger sus datos de las amenazas nuevas y emergentes.

Error 5

Incapacidad para priorizar y aprovechar la monitorización de la actividad de datos

La supervisión de uso y del acceso a los datos es una parte esencial de toda estrategia de seguridad de datos. Un responsable de la organización debe saber quién, cómo y cuándo las personas acceden a los datos. Esta monitorización debe englobar si esas personas deben tener acceso, si dicho nivel de acceso es correcto y si representa un elevado riesgo para la empresa.

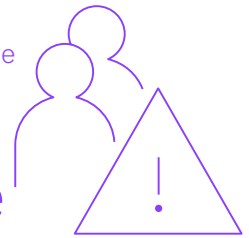
Las identificaciones de usuarios privilegiados son responsables habituales en las amenazas.[5] Un plan de protección de datos debe incluir supervisión en tiempo real para detectar las cuentas de usuarios privilegiados que se utilizan para actividades sospechosas o no autorizadas. Para impedir la posible actividad malintencionada, la solución debe realizar las siguientes tareas:

- Bloquear y poner en cuarentena la actividad sospechosa, en base a las violaciones de políticas.
- Suspender o cerrar las sesiones, en base a un comportamiento anómalo.
- Utilizar flujos de trabajo predefinidos y específicos según la normativa en todos los entornos de datos.
- Enviar alertas activas a los sistemas de seguridad de TI y operaciones.

Puede ser difícil responsabilizarse de la seguridad de los datos y la información relacionada con el cumplimiento, así como saber cuándo y cómo responder a las amenazas potenciales. Con el acceso de los usuarios autorizados a muchas fuentes de datos, incluyendo bases de datos, sistemas de archivos, entornos de mainframe y entornos de nube, la supervisión y guardado de datos de todas estas interacciones puede parecer abrumador. El reto reside en la supervisión, captura, filtrado, procesamiento y respuesta eficaces a un gran volumen de actividad de datos. Sin la existencia de un plan, su organización puede tener más información que la que pueda procesar razonablemente y, a su vez, disminuir el valor de la supervisión de la actividad de datos.

El coste medio global de una amenaza interna es de

11,45 millones de dólares.[6]



Solución

Desarrollar una estrategia de detección y protección de datos completa

Para ello, al iniciar un viaje a la seguridad de datos, deberá dimensionar y definir el alcance de las acciones de supervisión para dar una respuesta adecuada a los requisitos y a los riesgos. Muchas veces, esta actividad implica la adopción de un enfoque por fases, que permita el desarrollo y escalado de las mejores prácticas. Es más, es crítico mantener una conversación con las partes interesadas de negocio y de TI en las primeras fases del proceso para entender los objetivos de negocio a corto y largo plazo.

Esta conversación también deberá definir la tecnología que dará soporte a sus iniciativas clave. Por ejemplo, si la empresa planea crear oficinas en una nueva geografía que utilice una combinación de repositorios de datos on-premise y en la nube, la estrategia de seguridad de datos deberá evaluar cómo impactará dicho plan en la postura de cumplimiento y seguridad de datos de la organización. Si, por ejemplo, los datos propiedad de la empresa estarán sujetos a nuevos requisitos de cumplimiento y seguridad de datos, tales como el GDPR, la ley California Consumer Privacy (CCPA), laBrazil's Lei Geral de Proteção de Dados (LGPD), etc.

También deberá priorizar y centrarse en una o dos fuentes que probablemente tengan los datos más sensibles. Asegúrese de que las políticas de seguridad de datos sean claras y detalladas para dichas fuentes, antes de extender dichas prácticas al resto de la infraestructura.

El coste medio total de una brecha de datos fue un

95% más alto

en organizaciones sin automatización de la seguridad desplegada, en 2019.[1]

5,16 millones de dólares **sin automatización.**[1]

2,65 millones de dólares **con automatización totalmente desplegada.**[1]

Deberá buscar una solución automatizada de supervisión de actividad de datos o archivos con herramientas de análisis, que pueda centrarse en los riesgos clave y los comportamientos inusuales de usuarios privilegiados. Aunque sea esencial recibir alertas automatizadas cuando una solución de supervisión de actividad de datos o archivos detecte un comportamiento anómalo, también debe permitir la acción rápida cuando se descubran anomalías o desviaciones de las políticas de acceso a datos. Las acciones de protección deben incluir el bloqueo o enmascaramiento dinámico de datos.

Cuando desarrolle sus planes de protección y supervisión de la actividad de datos, suele ser útil considerar las siguientes preguntas:

- ¿Cuáles son mis dos fuentes de datos más sensibles?
- ¿Qué fuentes de datos, de cinco a diez, debo priorizar después, en función de su volumen de datos sensibles?
- ¿Existen ciertos endpoints o activos de nube asociados con datos con un riesgo más elevado?
- ¿Se mueven datos sensibles libremente entre entornos locales, híbridos y en la nube?
- ¿Qué usuarios deben tener acceso a la fuente de datos y bajo qué condiciones?
- ¿Qué usuarios o cuentas privilegiados con un alto riesgo deben desactivarse o requieren un mayor escrutinio?
- ¿Soporta mi solución de seguridad de datos capacidades de protección de datos automatizadas y supervisión de la actividad?
- ¿Existe una supervisión en tiempo real para realizar el seguimiento de datos de los archivos que residen en los almacenes de datos, tales como bases de datos de lenguaje de consulta estructurado (SQL), distribuciones de Hadoop, plataformas Not only SQL (NoSQL), etc.?
- ¿Tiene en cuenta mi solución de supervisión los almacenes de datos que abarcan entornos multicloud híbridos y me permiten generar informes personalizados que van a las personas adecuadas en el momento oportuno?
- ¿Cuento con las capacidades de supervisión filtrada y análisis de riesgos necesarias para priorizar eficazmente las acciones de riesgo, vulnerabilidades y remediación?

Cuanto más específico sea sobre la supervisión de prioridades y requisitos de protección, más eficaz será la solución para poder aplicar sus recursos disponibles de detección y respuesta.

Siguientes pasos

¿Cómo puede evitar estos errores habituales en la seguridad de datos, especialmente ahora que son muchas las compañías que adoptan entornos multicloud híbridos? Empieza con el reconocimiento del problema y la preparación de la organización para que adopte un enfoque proactivo y global en la protección de los datos, con independencia de donde residan.

Si su empresa tiene un entorno TI híbrido y complejo, no puede permitirse un enfoque compartimentado en la seguridad de los datos. Necesita añadir estrategias de protección de datos que cubran toda la infraestructura de datos y den soporte a todos sus tipos de datos.

Los pasos inmediatos que puede dar para proteger los datos valiosos de su organización son los siguientes:

- Desarrollo de una estrategia de seguridad de datos que soporte los objetivos tecnológicos y de negocio a corto y largo plazo de la organización
- Implementación de dicha estrategia con las personas, procesos y herramientas adecuadas
- Planificación de los recursos para asegurarse de que el programa de seguridad y de cumplimiento normativo puede escalarse eficazmente cuando la organización incorpore nuevas tecnologías

La plataforma de protección de datos de IBM Security Guardium ayuda a las organizaciones a adoptar un enfoque más inteligente y adaptable en la protección de datos críticos, dondequiera que residan. Vea por qué puede ser una buena opción para su organización.

Más información en ibm.com/guardium.

>4 semanas

Muchas organizaciones reconocen el valor de Guardium en menos de un mes.[7]

¿Por qué IBM Security?

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad para la empresa. La cartera, respaldada por la investigación y desarrollo de IBM X-Force® de fama mundial, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger globalmente sus personas, infraestructuras, datos y aplicaciones. Ofrece soluciones para la gestión de identidad y acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión del riesgo, gestión de puntos finales, seguridad de red, etc. Estas soluciones permiten a las organizaciones gestionar eficazmente el riesgo e implementar seguridad integrada para móviles, nubes, redes sociales y otras arquitecturas de negocio empresariales.

IBM opera una de las organizaciones de investigación de seguridad, desarrollo y entrega más amplia del mundo, supervisando más de

60 mil millones

de eventos de seguridad cada día, en más de 130 países.

IBM ostenta más de 3700 patentes de seguridad

IBM España, S.A
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

La página de inicio de IBM se encuentra en:
ibm.com

Este documento es válido en la fecha inicial de publicación y puede estar sujeto a cambios por parte de IBM en cualquier instante. No todas las ofertas están disponibles en todos los países en los que IBM opera.

Los datos de rendimiento y los ejemplos de clientes citados se presentan solamente a efectos ilustrativos. Los resultados reales de rendimiento pueden variar en función de configuraciones específicas y condiciones de operación. Es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto o programa con los productos y programas de IBM. LA INFORMACIÓN DE ESTE DOCUMENTO SE PROPORCIONA "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE, A LAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO DETERMINADO Y A LAS GARANTÍAS O CONDICIONES DE NO INFRACCIÓN. Los productos de IBM se garantizan de acuerdo con los términos y condiciones de los acuerdos bajo los que se proporcionan.

El cliente es responsable de asegurar su propio cumplimiento de los requisitos legales vigentes. IBM no proporciona asesoramiento legal ni representa o garantiza que sus servicios o productos aseguren el cumplimiento de la legislación vigente por parte del cliente.

Declaración de buenas prácticas de seguridad: la seguridad de sistemas TI implica la protección de sistemas e información a través de la prevención, detección y respuesta al acceso inadecuado desde el interior y exterior de la empresa. Un acceso inadecuado puede causar la alteración, destrucción, uso indebido o mal uso de la información o pueda causar daños o mal uso de sus sistemas, incluido el uso en ataques dirigidos a otros. Ningún sistema o producto TI debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente eficaz en la prevención de un uso o acceso inadecuados. Los sistemas, productos y servicios de IBM se han diseñado para formar parte de un enfoque de seguridad legal y completo, que necesariamente implicará procedimientos operativos adicionales y que pueden requerir que otros sistemas, productos o servicios sean lo máximo de eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HARÁN QUE SU EMPRESA SEA INMUNE, A LA CONDUCTA MALINTENCIONADA O ILEGAL DE TODAS LAS PARTES.

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*, abril de 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 Informe de NewVantage, "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,* 20 de junio de 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,* Agosto de 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-ESES-00