Asegure la información de la empresa y garantice el cumplimiento

Un enfoque holístico hacia la protección de datos

Puntos importantes

- InfoSphere Discovery de IBM para entender y definir información
- InfoSphere Guardium de IBM para seguridad de base datos, encriptación de datos y redacción de datos
- InfoSphere Optim de IBM para soporte de requerimientos de enmascaramiento de datos.

Los titulares noticiosos que reportan una frecuencia creciente de robos de información e identidad han derivado en una mayor consciencia de las violaciones a la seguridad y privacidad'y sus consecuencias. En respuesta a este problema, se han impuesto nuevas regulaciones en todo el mundo. Si bien los aspectos específicos tengan variaciones de una regulación a otra, la imposibilidad de garantizar el cumplimiento puede dar por resultado penalizaciones financieras significativas e incluso tiempo en prisión. Además, las organizaciones corren el riesgo de perder la lealtad de sus clientes y destruir el valor de su marca.

Considerando que la información es un componente crítico de la operación de negocios diaria, resulta esencial garantizar la privacidad y proteger la información, sin importar dónde resida. Distintos tipos de información tienen distintos requerimientos de protección y privacidad; por lo tanto, las organizaciones deben tomar un enfoque holístico para la salvaguarda de información, al:

- Entender dónde existe información: Las organizaciones no pueden proteger información sensible, a menos que sepan dónde reside y cómo se relaciona a lo largo de toda la empresa
- Salvaguardar información sensible, tanto estructurada como desestructurada: La información estructurada contenida en las bases de datos debe protegerse de acceso no autorizado. La información desestructurada en documentos y formatos requiere políticas de privacidad para redactar (remover) información sensible al tiempo que continúa permitiendo que se comparta información de negocios necesaria.
- Proteger ambientes que no son de producción: La información en ambientes que no son de producción (desarrollo, capacitación y aseguramiento de calidad) debe protegerse, mientras se permite que sea utilizable durante los procesos de desarrollo, prueba y capacitación de aplicaciones.

- Asegurar y monitorear de manera continua el acceso a la información: Las bases de datos de la empresa,almacenes de datos y compartición de archivos requieren análisis en tiempo real, a fin de garantizar que el acceso a la información esté protegido y sea auditado. Se requieren controles basados en políticas para detectar con rapidez actividad no autorizada o sospechosa y alertar al personal clave. Además, las bases de datos y compartición de archivos deben protegersecontra nuevas amenazas y otras actividades maliciosas y continuamente monitorearse para detectar debilidades.
- Demostrar cumplimiento para pasar auditorías: No basta con desarrollar un enfoque holístico hacia la seguridad y privacidad de la información. Las organizaciones también deben demostrar y probar cumplimiento ante auditores de terceros. Las soluciones de IBM® para seguridad de datos y privacidad están diseñadas para soportar este enfoque holístico hacia la protección de datos e incorporar una inteligencia que permita a las organizaciones atender de manera proactiva amenazas de TI y riesgos empresariales, mientras permanecen enfocados en las metas del negocio.

Cómo entender el enfoque creciente en la protección de datos

Según el reporte de Octubre de 2011, 'DATABASES ARE MORE AT RISK THAN EVER÷ (Las bases de datos están en más riesgo que nunca), donde se entrevistó a 355 profesionales de la seguridad de datos, una cuarta parte de los que respondieron sintieron que era muy probable o inevitable que ocurriera una violación a la información durante 2012. Sólo 36% de las organizaciones han iniciado acciones para asegurar que sus aplicaciones no estén sujetas a ataques por inyección de código SQL y más de 70% de ellas tardan más de tres meses en aplicar actualizaciones de parches críticos, lo que da a los atacantes la oportunidad que buscan. La mayoría de los que respondieron no pueden decir si ha habido acceso o cambios no autorizados a su base de datos. En muchos casos, una violación pasa de largo durante meses o más "sólo 40% de las organizaciones auditan sus bases de datos con regularidad. Las estrategias de prevención son casi inexistentes en la mayoría de las compañías. Sólo una cuarta parte de quienes respondieron se dicen capaces de detener el abuso de privilegios por parte de usuarios autorizados de la base de datos, sobre todo de usuarios con alto nivel de privilegios. Sólo el 30% encripta información sensible y personal identificable en todas sus bases de datos, a pesar de las regulaciones sobre privacidad de información a nivel mundial que exigen la encriptación de datos para información en reposo.

Además, la mayoría admiten tener información sensible en ambientes que no son de producción, accesible para desarrolladores, pruebas e incluso para terceros.

Cómo identificar riesgos asociados con una seguridad y privacidad de datos insuficiente

Las corporaciones y sus funcionarios pueden enfrentar multas entre US$5,000 hasta US$ 1, 000,000 por día y posiblemente tiempo de prisión, si se hace un mal uso de la información. Según el estudio del Ponemon Institute, '2011: Cost of Data Breach Study÷ (2011: Estudio de costos de violaciones de datos) publicado en Marzo de 2012, el costo promedio para la organización de una violación a la información durante 2011 fue de $5.5 millones de dólares. Las violaciones a la información en 2011 costaron a sus empresas un promedio de $194 dólares por registro comprometido. El número de registros violados por incidente en 2011 osciló entre aproximadamente 4,500 registros a más de 98,000. En 2011, el tamaño promedio de los registros violados fue de 28,349. Como en años anteriores, los costos por violaciones a la información parecen ser directamente proporcionales al número de registros violados.

Las severas multas son sólo un ejemplo de la manera en que pueden verse afectadas las empresas. Entre otros impactos negativos se encuentran la erosión en el precio de las acciones por la preocupación de los inversionistas y la publicidad negativa derivada de una violación a la información, además del daño irreparable a la marca cuando se identifica a una empresa como no confiable.

Cómo enfrentar los desafíos a la seguridad y privacidad de la información

¿Qué hace que el enfoque de IBM hacia la protección de datos resulte tan único? La experiencia. La alineación de personas, procesos, tecnología e información separa las soluciones de seguridad y privacidad de información de IBM de las de la competencia. La meta del portafolio de IBM es ayudar a las organizaciones a cumplir con sus obligaciones legales, regulatorias y de negocios, sin añadir gastos indirectos adicionales. Esto ayuda a las organizaciones a soportar iniciativas de cumplimiento, reducir costos, minimizar riesgos y sostener un crecimiento rentable. Además, IBM ha integrado la seguridad de la información dentro de un marco de seguridad más amplio. El marco de seguridad de IBM (véase la figura 1) y las mejores prácticas asociadas, proporcionan los modelos de experiencia, análisis de datos y madurez para dar a los clientes de IBM la oportunidad de abrazar la innovación con confianza.

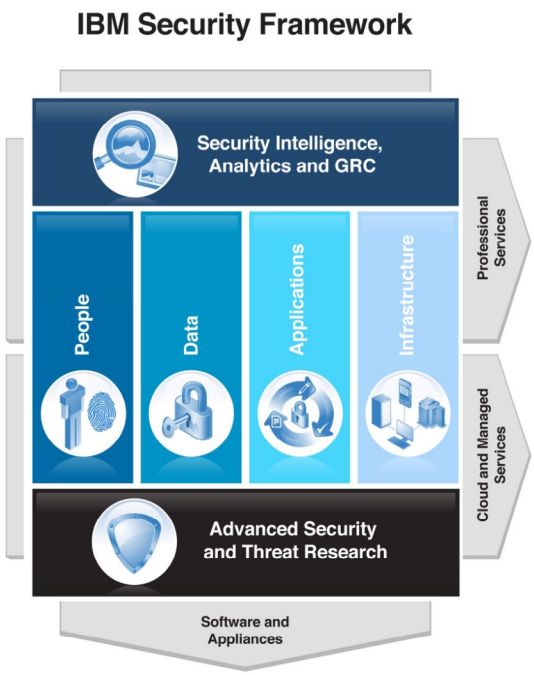

Figura 1: IBM es el único proveedor que proporciona inteligencia de seguridad que abarca personas, datos, aplicaciones e infraestructura.

Tomando un enfoque de tres capas para la protección de información

La plataforma de InfoSphere proporciona un enfoque único en tres capas para asegurar una protección holística de la información: Entender y Definir, Asegurar y Proteger, Monitorear y Auditar.

Entender y Definir

Las organizaciones deben descubrir dónde reside la información sensible, clasificar y definir tipos de datos, determinar métricas y políticas para garantizar protección en el tiempo. La información puede ser distribuida entre múltiples aplicaciones, bases de datos y plataformas con poca documentación. Muchas organizaciones dependen demasiado de expertos en sistemas y aplicaciones para esta información. En ocasiones, esta información se integra en una lógica de la aplicación y es posible aplicar relaciones ocultas tras bambalinas.

IBM InfoSphere Discovery está diseñado para identificar y documentar qué información se tiene, dónde se localiza y cómo se enlaza entre sistemas mediante la captación inteligente de relaciones y la determinación de transformaciones aplicadas y reglas de negocios. Ayuda a automatizar la identificación y definición de relaciones de datos en ambientes complejos y heterogéneos.

Asegurar y Proteger

Las soluciones para seguridad de información y privacidad deben cubrir una empresa heterogénea y proteger la información estructurada y la no estructurada en ambientes que pueden ser o no de producción. Las soluciones de InfoSphere ayudan a asegurar valores sensibles en las bases de datos, en aplicaciones ERP/CRM y también en formatos desestructurados como formularios y documentos. Las tecnologías clave incluyen monitoreo de la actividad en la base de datos, enmascaramiento de datos, redacción y encriptación de datos. Un enfoque holístico hacia la protección de datos asegura una cobertura 360° de toda la información organizacional.

IBM InfoSphere Guardium® Database Activity Monitor and Vulnerability Solution proporciona una solución de seguridad de base de datos que abarca toda la seguridad de la base de datos y el ciclo de vida de cumplimiento con una consola web unificada, almacenamiento de datos administrativos y sistema de automatización de flujo de trabajo. Le permite:

- Acceder a las vulnerabilidades y defectos de configuración de la base de datos
- Asegurar que las configuraciones queden fijas una vez implementados los cambios recomendados
- Proporcionar 100 por ciento de visibilidad y granularidad en todas las transacciones de bases de datos ”a lo largo de todas las plataformas y protocolos‘ con un rastro de auditoría seguro, a prueba de manipulación, que soporta la separación de deberes
- Rastrear las actividades de las principales plataformas para compartir archivos, tales como Microsoft SharePoint
- Monitorear y aplicar políticas para acceso a información sensible, acciones de usuarios con privilegios, control de cambios, actividades de los usuarios de aplicaciones y excepciones de seguridad como intentos de conexión fallidos.

- Automatizar el proceso de cumplimiento de auditoría completo‘ incluyendo distribución de reportes a equipos de supervisión, aprobación y escalamiento- con reportes pre-configurados para la Ley Sarbanes-Oxley, PCI DSS y privacidad de datos
- Crear un solo repositorio de auditoría centralizado para reporte de cumplimiento en la totalidad de la empresa, optimización de información, investigaciones y rastros forenses.
- Escalar fácilmente, pasando de salvaguardar una sola base de datos a proteger cientos de bases de datos en centros de datos distribuidos en todo el mundo.

Tradicionalmente, la protección de información no estructurada en formatos, documentos y gráficas se ha realizado manualmente, eliminando contenido electrónico y utilizando un marcador negro para ocultar la información sensible. Pero este proceso manual puede introducir errores, omitir información de manera inadvertida y dejar atrás información oculta dentro de los archivos.

IBM InfoSphere Guardium Data Redaction protege la información sensible enterrada en documentos y formatos no estructurados de divulgación no intencional. Esta solución automatizada presta eficiencia al proceso de redacción, al detectar información sensible y eliminarla automáticamente de la versión de los documentos disponible para usuarios sin privilegios. Con base en las técnicas de redacción de software líderes en la industria, InfoSphere Guardium Data Redaction también ofrece la flexibilidad de la revisión y supervisión humana, si se requiere.

La solución IBM InfoSphere Optim™ Data Masking Solution proporciona un conjunto amplio de técnicas para enmascaramiento de datos que pueden soportar sus requerimientos de cumplimiento de privacidad de datos, incluyendo:

- Capacidades de enmascaramiento conscientes de la aplicación, diseñadas para ayudar a garantizar que la información enmascarada, como nombres y domicilios, tenga la misma apariencia y sensación que la información original
- Rutinas de enmascaramiento pre-empaquetadas conscientes del contexto, que facilitan la identificación de elementos como número de pago de tarjetas, números de seguro social, domicilios y direcciones de correo electrónico
- Capacidades de enmascaramiento persistentes que propagan los valores de reemplazo enmascarados de manera consistente entre aplicaciones, bases de datos, sistemas operativos y plataformas de hardware.

IBM InfoSphere Guardium Data Encryption proporciona una solución única, administrable y escalable para encriptar información de la empresa, sin sacrificar el desempeño de las aplicaciones o crear complejidad en la administración clave. A diferencia de los enfoques invasivos como la encriptación de la base de datos a nivel de columnas, la encriptación de archivos basada en PKI o la encriptación en punto nativo, InfoSphere Guardium Data Encryption ofrece una solución única, transparente que también resulta fácil administrar.

IBM Tivoli® Key Lifecycle Manager ayuda a las organizaciones de TI a administrar mejor el ciclo de vida de las claves de encriptación, al permitirles centralizar y reforzar procesos de gestión de claves. Puede administrar claves de encriptación para dispositivos de almacenamiento de auto encriptación de IBM, al igual que soluciones de encriptación que no sean para IBM, las cuales utilicen el Protocolo de Interoperabilidad de Gestión de Claves (KMIP, por sus siglas en inglés). IBM Tivoli Key Lifecycle Manager proporciona los siguientes beneficios para la seguridad de la información:

- Centralizar y automatizar el proceso de gestión de claves de encriptación
- Reforzar la seguridad de la información mientras se reduce dramáticamente el número de claves de seguridad por administrar
- Simplificar la gestión de claves de encriptación con una interfaz intuitiva para el usuario para configuración y gestión
- Minimizar el riesgo de pérdida o violación de información sensible
- Extender capacidades de gestión de claves para productos que sean o no de IBM
- Apalancar estándares abiertos para ayudar a habilitar la flexibilidad y facilitar la interoperabilidad con proveedores

Monitorear y Auditar

Una vez localizada y asegurada la información, las organizaciones deben comprobar el cumplimiento, estar preparadas para responder ante nuevos riesgos internos y externos y monitorear sus sistemas de manera continua. Monitorear la actividad de usuarios, creación de objetos y configuración de bases de datos y derechos ayuda a los profesionales de TI

y a los auditores a rastrear usuarios entre aplicaciones y bases de datos. Estos equipos pueden establecer políticas detalladas para comportamientos apropiados y recibir alertas cuando se violen estas políticas.

Las organizaciones también deben ser capaces de demostrar cumplimiento con rapidez y dar poder a los auditores para verificar el estatus de cumplimiento. Los reportes de auditoría y autorizaciones deben ayudar a facilitar el proceso de cumplimiento, al tiempo que mantienen los costos bajos y minimizan las interrupciones técnicas y de negocios. Las organizaciones deben crear rastros de auditoría continuos, detallados, de todas las actividades en la base de datos incluyendo el ’quién, qué, cuándo, dónde y cómo÷ de cada transacción.

IBM InfoSphere Guardium Database Activity Monitor proporciona un sistema de gestión de base de datos (DBMS) detallado ”auditoría independiente con un impacto mínimo en el desempeño. InfoSphere Guardium también está diseñado para ayudar a las organizaciones a reducir los costos de operación vía automatización, políticas trans- DBMS centralizadas y repositorios de auditoría, filtración y compresión.

Construir protección con software IBM escalabe y modular

Proteger la seguridad y privacidad de datos es una responsabilidad continua, que debe ser parte de las mejores prácticas de todos los días. IBM proporciona seguridad y privacidad de datos integradas mediante una estrategia en tres capas: Entender y Definir, Asegurar y Proteger y Monitorear y Auditar. Para proteger la información se requiere una visión holística de 360 grados. Con la experiencia amplia y profunda en seguridad y espacio de privacidad, IBM puede ayudar a su organización a definir e implementar dicho enfoque.

Sobre IBM InfoSphere

El software IBM InfoSphere parte de la plataforma integrada para definir, integrar, proteger y administrar información de confianza en sus sistemas. Proporciona todos los bloques de construcciones fundamentales para la información de confianza, incluyendo integración de datos, almacenamiento de datos, gestión de información maestra y gobernabilidad de la información, todo ello integrado con un núcleo de metadatos y modelos compartidos. El portafolios es modular, por lo que se puede empezar desde cualquier punto y mezclar y compaginar los pilares de construcción del software InfoSphere con componentes de otros proveedores, o elegir desplegar múltiples bloques de construcción juntos para una mayor aceleración y valor. La plataforma InfoSphere entrega una base de clase empresarial para proyectos con uso intensivo de información, que proporciona el desempeño, escalabilidad, confiabilidad y aceleración necesarios para simplificar los retos difíciles y entregar información de confianza a su negocio con mayor rapidez.

Sobre la seguridad de IBM

El portafolio de seguridad de IBM proporciona la inteligencia de seguridad para ayudar a las organizaciones a brindar una protección holística a su personal, infraestructura, información y aplicaciones. IBM ofrece soluciones para gestión de identidad y acceso, seguridad de base de datos, desarrollo de aplicaciones, gestión de riesgo, gestión de punto final, seguridad de redes y más. IBM opera con la mayor organización de investigación y desarrollo de seguridad y organización de entrega. Esto comprende nueve centros de operaciones de seguridad, nueve centros de investigación IBM, 11 laboratorios de desarrollo de seguridad para software y un instituto para Seguridad Avanzada con representación en Estados Unidos, Europa y Asia Pacífico. IBM monitorea 13 mil millones de eventos de seguridad por día en más de 130 países y tiene más de 3,000 patentes de seguridad.

Para mayor información

Si desea saber más sobre las soluciones IBM InfoSphere para proteger la seguridad y privacidad de la información, contacte a su representante de ventas local de IBM o visite:
ibm.com/guardium

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Producido en Los Estados Unidos de América
Mayo, 2012

Please Recycle

IMS14383-USEN-01