Informatica

White paper

Reducir el riesgo de privacidad de datos para la gestión de datos maestros

Acerca de Informatica

La transformación digital modifica las expectativas: mejor servicio, entrega más rápida, menores costes. Los negocios deben transformarse para seguir siendo relevantes, y los datos tienen la respuesta.

Como líder mundial en gestión de datos de cloud empresariales, le brindamos ayuda para que encabece la marcha de forma inteligente, en cualquier sector, categoría o nicho. Informatica le aporta perspectiva para que aumente su agilidad, concrete nuevas oportunidades de crecimiento o incluso invente cosas nuevas. Al estar completamente centrados en todo lo relacionado con los datos, ofrecemos la versatilidad necesaria para alcanzar el éxito.

Le invitamos a explorar todo lo que puede ofrecerle Informatica y a desatar el poder de los datos para impulsar su próxima disrupción inteligente.

Contenidos

Resumen ejecutivo

Con el fin de obtener una visión fidedigna y fiable del cliente, el producto, el servicio, la información operacional y otra información empresarial crítica para el negocio, las organizaciones invierten en iniciativas de gestión de datos maestros (MDM). Estas estrategias de MDM combinan elementos de datos fundamentales de la empresa en registros consolidados con el fin de crear datos fiables que puedan compartirse con el personal y las aplicaciones que los necesiten. Esta práctica es de un valor inmenso para cualquier negocio que desee desarrollar ofertas más centradas en el cliente, mejorar el servicio de atención al cliente y los programas de fidelidad, generar eficiencias en las soluciones y la gestión de productos, migrar a la nube de manera segura, etc.

Los datos fiables se han convertido en la joya de la corona de las iniciativas de productos y clientes de las organizaciones, y proporcionan una ventaja competitiva. Sin embargo, la consolidación de los datos sensibles también supone un blanco atractivo para los ataques externos que generan brechas en la seguridad de los datos y aumentan el posible abuso interno. Por lo tanto, está sujeta a normativas de privacidad como el Reglamento General de Protección de Datos (RGPD), la Ley de Privacidad del Consumidor de California (CCPA) y otras normativas.

Es natural, por lo tanto, que surjan diferentes preguntas relacionadas con la protección de los datos y el cumplimiento en estos entornos:

- ¿Dónde se encuentran todos los datos y cómo proliferan?
- ¿Qué alimenta el repositorio? ¿Quién accede a los datos y con qué aplicaciones?
- ¿Se ajustan el acceso y el uso actuales a las normativas y políticas aprobadas de uso de los datos?
- ¿Es apropiada la protección de los datos? ¿Se mantiene el riesgo de los datos dentro de unos niveles aceptables? ¿Existen condiciones de riesgo inapropiadas que deban solucionarse?

Los resultados de la detección y la clasificación de datos sensibles son la base para tomar decisiones relacionadas con el riesgo de los datos, la protección y el cumplimiento de las normativas de datos controlados.

En este white paper se proporcionan una serie de consideraciones y estrategias para reducir el riesgo con una solución centrada en los datos que:

- aplica análisis, inteligencia basada en metadatos, automatización e inteligencia artificial para identificar y proteger datos maestros sensibles;
- cumple con las nuevas normativas de privacidad y gobierno de datos;
- proporciona preparación para auditorías a fin de demostrar la implantación de controles; y
- avisa a los usuarios en caso de que se produzca un comportamiento anómalo que requiera investigación.

Introducción

Según la empresa de investigación IDC, se prevé que el mundo generará 175 zettabytes de datos en 2025, una cantidad mucho mayor que los 33 zettabytes generados en 2018[1]. Organizaciones de todos los sectores confían en la precisión, la disponibilidad y la protección de sus datos para generar ingresos, atender a los clientes, aumentar la productividad, optimizar las operaciones y dirigir otros procesos empresariales de misión crítica.

El continuo crecimiento exponencial del volumen de datos y su uso también incluye datos maestros sensibles en varios silos, tanto en entornos locales como en el cloud, y en diversos formatos. Estas condiciones han hecho que los métodos tradicionales de protección de los datos pasen a estar obsoletos[2], lo que exige un nuevo enfoque para la seguridad de los datos maestros en toda la organización.

Sin embargo, la mayoría de las compañías no son capaces de identificar con exactitud la ubicación de todos sus datos maestros sensibles ni desde dónde se accede a ellos, sobre todo si se encuentran en formatos no estructurados. Esta falta de visibilidad aumenta los riesgos para la organización y, por estas razones, una filtración en la seguridad de los datos constituye el principal riesgo para la seguridad de IT[3].

Con un panorama en el que las brechas en la seguridad de los datos son cada vez más frecuentes y ante la proliferación de datos maestros sensibles utilizados de manera inapropiada, las organizaciones deben desarrollar una estrategia de reducción de riesgos que incluya una solución de privacidad centrada en los datos con estas características clave:

- Visibilidad de todas las fuentes de datos para detectar y clasificar datos maestros sensibles localizados en toda la organización.
- Capacidad para implementar los mecanismos de protección de los datos maestros sensibles para mitigar las filtraciones en la seguridad de los datos.
- Cumplimiento de las normativas vigentes en materia de privacidad, así como el uso de inteligencia basada en metadatos, la automatización y la inteligencia artificial para supervisar el comportamiento de los usuarios y avisar de anomalías prácticamente en tiempo real.
- Exhaustivas herramientas de visualización de análisis para la evaluación de riesgos y la gestión de datos sensibles.
- Capacidades de generación de informes transparentes y completos para demostrar los controles con preparación para auditorías.

Gartner prevé que los productos de protección integrados sustituyan a las diversas herramientas de seguridad de datos en silos en un 40 % de las grandes empresas, una cantidad que ha aumentado desde menos del 5 % que había antes[4]. Estas soluciones de protección centradas en los datos ofrecen una vista centralizada de los datos en riesgo, para que todos los usuarios clave de una organización global puedan controlar el movimiento de los datos sensibles y aplicar mecanismos de protección según lo estipulado en los reglamentos y políticas de gobierno.

Estrategia de cuatro puntos para reducir el riesgo de privacidad de los datos sensibles

El riesgo de privacidad de datos sensibles es el resultado de perder datos sensibles con una exposición inadecuada, y la causa más común es una filtración de datos o un uso indebido interno. Existe la creencia equivocada de que este riesgo se mitiga solamente determinando la ubicación de los datos maestros sensibles. Sin embargo, la localización y la clasificación de estos datos es solo el primer paso de una exhaustiva estrategia para mitigar el riesgo.

[1] "The Digitization of the World – From Edge to Core", white paper de IDC, noviembre de 2018.
[2] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 de marzo de 2017.
[3] "Data Breaches and Sensitive Data Risk", Ponemon Institute LLC, febrero de 2016.
[4] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 de marzo de 2017.

Los siguientes pasos requieren la evaluación de las prioridades de riesgo de la organización que se deben abordar, en función de los resultados de los análisis de localización y clasificación. Debe establecer una estrategia para reducir los principales riesgos que incluya controles automatizados que apliquen políticas de gobierno de datos y que involucre a todos los usuarios clave y no solo al departamento de IT. La estrategia debe incluir también la implementación de una solución de protección y privacidad fiable y centrada en los datos que proporcione capacidades para el cumplimiento de las normativas, incluida la visualización completa de análisis de datos sensibles para cuadros de mando de visibilidad de riesgos y generación de informes de auditoría de controles de cumplimiento, así como protección para todo tipo de datos sensibles controlados en la organización.

1. Detección y clasificación

Un enfoque ad hoc habitual para la detección consiste en revisar las fuentes existentes y enviar cuestionarios. Sin embargo, el enfoque manual es poco adecuado, ya que consume tiempo y recursos valiosos, suele resultar impreciso y volverse obsoleto con rapidez, pues se basa en informes propios en lugar de supervisar el flujo de datos y el comportamiento real de los usuarios en tiempo real.

Las organizaciones deben plantearse estas cuestiones:

- ¿Qué datos almacenamos? ¿Quién tiene acceso a los datos? ¿Con qué objetivo acceden a ellos?
- ¿Cómo podemos gestionar los privilegios de usuario y suministrar los derechos sobre los datos?
- ¿Cómo vamos a proteger los datos controlados sensibles y garantizar la aplicación de unos controles apropiados?

Otras consideraciones relacionadas con el cumplimiento de la detección y la clasificación son:

- Definir y comprender el panorama de los datos, incluidas las bases de datos y los datos no estructurados.
- Determinar los sistemas que contienen datos controlados sensibles y asignar datos a identidades.
- Adquirir una solución que puede determinar el movimiento de los datos por el ecosistema, al tiempo que se mantiene una vista casi en tiempo real con análisis y herramientas de elaboración de informes.

2. Cumplimiento

Las organizaciones se esfuerzan por identificar, supervisar y mitigar los riesgos relacionados con las normativas de privacidad de datos. Además, deben supervisar, analizar y avisar sobre el acceso o el movimiento de los datos que puedan poner en peligro el cumplimiento.

El Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2018, se adoptó con el objetivo de reforzar y unificar la protección de los datos de todos los habitantes de la Unión Europea. De esta forma, se pretendía simplificar el entorno normativo para el panorama empresarial internacional. Del mismo modo, la CCPA, vigente desde el 1 de enero de 2020, sube el listón y aumenta la privacidad al incluir los datos de unidades familiares.

Muchas empresas no se han preparado del todo para ninguno de estas normativas y no las cumplen de manera eficaz. No obstante, su incumplimiento podría acarrear importantes sanciones y el desprestigio de la entidad. Por otro lado, el cumplimiento puede marcar la diferencia en la privacidad de los datos controlados, lo cual puede suponer una ventaja competitiva al mejorar la fidelidad de los clientes e impulsar los resultados de la transformación digital. Además, las empresas que demuestran diligencia en la protección de los datos tienen 5 veces más acceso a la información personal de sus clientes, ya que confían en que la manejarán de manera responsable[5].

[5] Fragmento de "Bridging the Trust Gap in Personal Data", de Boston Consulting Group

Las organizaciones deben desarrollar políticas inteligentes que identifiquen los almacenes de datos que contengan dominios de datos relevantes para el RGPD, la CCPA y otras normativas en materia de privacidad similares. Estas políticas atienden a varios factores y su lógica de inteligencia de datos determina las combinaciones que suponen una amenaza para la exposición a riesgos de privacidad.

3. Protección

En el tercer trimestre de 2019 se produjeron más de 5000 filtraciones de datos, con casi 8000 millones de registros expuestos[6]. Es evidente que, a pesar de las grandes inversiones en seguridad y privacidad, los datos personales críticos siguen siendo vulnerables. Las organizaciones necesitan proteger constantemente los datos de alto riesgo, identificar los comportamientos sospechosos y el uso o el movimiento no autorizado, además de automatizar y organizar las correcciones.

Las organizaciones deben priorizar los riesgos de datos más críticos y corregirlos mediante controles centrados en los datos que respalden su movilidad, en lugar de confiar únicamente en los controles históricos de acceso al servidor, firewalls y herramientas similares de ciberseguridad centradas en el sistema. Por ejemplo, los controles centrados en los datos incluyen el enmascaramiento, controles basados en la identidad y cifrado.

Además de los controles de privacidad de datos, las organizaciones deben supervisar el acceso a los datos y el comportamiento basado en la identidad. Un acceso excesivo o un comportamiento atípico pueden indicar que los usuarios no están respetando las políticas de privacidad o que las credenciales de usuario están en peligro.

4. Preparación para una auditoría y respuesta

Ahora, las empresas se someten a muchas más auditorías y evaluaciones de datos sensibles que antes. Se afanan por demostrar a los auditores de que tienen visibilidad sobre los datos críticos y que los protegen.

Las organizaciones deben ser capaces de responder de forma inmediata a los auditores y de demostrar que saben dónde se encuentran los datos, los riesgos a los que están expuestos, cómo se protegen y cómo se están utilizando. Deben considerar que los auditores pueden requerir informes y vistas resumidas de departamentos o ubicaciones y que permitan examinar dominios de datos específicos.

Conclusión

La potencia de MDM puede ayudar a las organizaciones a transformar sus operaciones y sus servicios. El poder de estos datos es evidente, pero también suponen un tentador objetivo que los actores internos o externos pueden utilizar de forma indebida. A esto se le suma la constante arremetida de las filtraciones de datos y el aumento de los requisitos de cumplimiento, los cuales obligan a las organizaciones a volver a elaborar las herramientas y los procesos para identificar, analizar y proteger datos sensibles.

Ante el panorama actual en el que existe un mayor riesgo para la privacidad y donde las filtraciones de datos son frecuentes, las empresas deben desarrollar una estrategia digital sólida para supervisar, analizar y corregir constantemente el riesgo al que se exponen los datos maestros sensibles. Deben supervisar los datos casi en tiempo real para detectar indicios de uso indebido o filtración de seguridad de datos, un comportamiento o acceso atípico o transferencias internacionales inadecuadas. Con esta diligencia, las organizaciones pueden aprovechar la MDM para mejorar su postura ante los riesgos con el fin de mitigar el impacto de las filtraciones de datos o del uso indebido interno, así como para satisfacer los requisitos cada vez más exigentes de los reglamentos industriales y regionales.

[6] Q3 2019 Data Breach QuickView Report de Risk Based Security

Recomendaciones

1. Realice una evaluación de los riesgos de la privacidad de datos para conocer exactamente dónde se encuentran los datos controlados sensibles, hasta dónde proliferan en su ecosistema de datos y qué conjuntos de datos sensibles son más vulnerables para remediar esta situación.
2. Atendiendo a los resultados de la evaluación, otorgue prioridad a las principales fuentes de la organización con los datos controlados más sensibles, determine una estrategia y un plazo para protegerlos, e implemente la estrategia como una solución piloto para su enfoque de protección y seguridad de los datos.
3. Defina, documente y distribuya las políticas de cumplimiento de la privacidad de la organización y los usuarios clave responsables del cumplimiento de las normativas de privacidad. Elabore un plan estratégico para este año y de cara al futuro.

Investigación adicional

Para obtener más información acerca de los riesgos de seguridad de los datos sensibles y las consideraciones acerca de la protección, consulte los siguientes vídeos y publicaciones:

Informatica Data Privacy Management

Master Data Management de Informatica–Customer 360

White paper: Privacidad de datos inteligente

Bloor Research: Detectar datos sensibles

Informatica

Sede central mundial José Echegaray 8, Parque Alvia - Edif. 3, PB 3, 28232 Las Rozas de Madrid Tel: +34 91 787 61 40
Número gratuito en Estados Unidos: 1.800.653.3871

IN09_0520_03409