Supere los desafíos de la protección de los datos en cualquier parte

Manteniendo datos confidenciales protegidos en la era de la computación en la nube

Haga clic en los círculos para avanzar a los diferentes capítulos

Despliegue un entorno en la nube

Las organizaciones están realizando rápidamente una transición a la nube, aprovechando las tecnologías de infraestructura como servicio (IaaS), software como servicio (SaaS) y plataforma como servicio (PaaS) como nuevas maneras de optimizar el negocio, aun cuando estos entornos presentan nuevos riesgos para los datos confidenciales.

Desafíos de seguridad en la nube

Los despliegues en la nube con frecuencia implican mantener datos confidenciales en ubicaciones que usted no puede controlar y que son administrados por terceros que podrían tener acceso irrestricto a los datos.

Desafíos organizacionales

Los desafíos para la protección de los datos en la nube incluyen garantizar el cumplimiento de regulaciones, supervisar los controles de acceso, asegurar la privacidad, mejorar la productividad y responder a las vulnerabilidades, al mismo tiempo que se saca partido de los datos locales y los datos basados en la nube de manera conjunta, para impulsar el negocio.

Enfoque de protección de datos

La seguridad de los datos y las tecnologías de protección deben operar en múltiples entornos (físicos, en la nube e híbridos) al mismo tiempo. Su solución de seguridad de datos debe ser automatizada, dinámica, adaptable, y debe proporcionar capacidades de cifrado coherentes y flexibles.

Conclusión

A medida que la computación en la nube se vuelve generalizada, los fundamentos de la seguridad permanecen iguales: asegurar, proteger los datos y respaldar el cumplimiento de regulaciones.

1.1 Despliegue de un entorno en la nube

Hace pocos años, muchas organizaciones adoptaron los entornos en la nube privados para ayudar a incrementar la flexibilidad y controlar los costos, en gran medida debido a la falta de madurez y de conAtrol de los entornos en la nube pública que se encontraban disponibles. Sin embargo, hoy la decisión de adoptar la nube es menos binaria y más orientada hacia una variedad de opciones, abarcando diferentes modelos de despliegue (público, privado e híbrido) y tipos de servicio, incluyendo IaaS, PaaS y SaaS.

Con más opciones pormenorizadas, el despliegue de la nube se fragmenta, dependiendo de la línea de negocios, en lugar de consistir en una decisión estandarizada de TI. Y si bien la lista de nuevas opciones de nubes es amplia, la mayoría de las empresas adoptará un entorno mixto e híbrido, para aprovechar sus inversiones existentes en mainframes, bases de datos locales, distribuciones de Big Data, sistemas de archivos y mucho más.[1]

Una nube privada es una infraestructura de TI que se opera exclusivamente para una sola organización, ya sea que su gestión sea interna o realizada por un tercero. Con las nubes privadas, las organizaciones controlan toda la pila de software, así como la plataforma subyacente, desde la infraestructura de hardware hasta las herramientas de medición. Los servicios en la nube privada se destinan a su uso por las unidades de negocios de una sola empresa (o a su uso compartido con sus socios).[1] No obstante, cuando las cargas de trabajo se mueven a las nubes privadas, proteger los datos en los entornos virtuales se vuelve aún más importante, en especial debido a que las cargas de trabajo con diferentes niveles de confiabilidad se combinan para ejecutarse en el mismo hardware físico.

Estudios realizados por Gartner demuestran que las inversiones significativas y su utilización continuarán en la computación en la nube privada. Sin embargo, casi todas las empresas encuestadas por Gartner desean aprovechar un modelo de nube híbrida, con elementos tanto en la nube privada como en la nube pública. Las empresas están utilizando opciones de computación en la nube pública “llave en mano” para habilitar servicios más rápidos, aumentar la agilidad empresarial y estimular la innovación. La computación en la nube pública tiene un papel clave para la innovación y, como resultado, se prevé que crezca un 15,2 % durante el año 2019.[1]

En lo que respecta a los entornos en la nube, ya sea en la nube pública o en entornos hospedados de forma privada, los controles de seguridad y protección de datos deben proteger los datos confidenciales y respaldar los requisitos gubernamentales y de conformidad del sector.

1.2 Despliegue de un entorno en la nube

Los tipos de servicios más comunes son IaaS, PaaS y SaaS. La forma más fácil de visualizar las diferencias es considerar su pila de TI. En la parte inferior se encuentra su infraestructura, que incluye el hardware, los servidores y las redes, lo cual representa su base de TI. Sobre esta infraestructura se encuentran sus plataformas de software o middleware, que proporcionan las herramientas que los desarrolladores necesitan para desplegar aplicaciones empresariales. Finalmente, en la parte superior se encuentran las aplicaciones empresariales que interactúan con los empleados internos y los clientes.

IaaS permite que las organizaciones mantengan sus plataformas físicas de software y middleware y sus aplicaciones empresariales existentes, pero que subcontraten la gestión de su infraestructura subyacente. Las compañías hacen esto con el propósito de aprovechar rápidamente la nube, minimizando al mismo tiempo el impacto y aprovechando las inversiones existentes.

PaaS permite que las empresas subcontraten tanto la infraestructura como el middleware o software. Esto elimina una significativa carga impuesta a la compañía, desde una perspectiva de TI, y permite que ésta se centre en el desarrollo de aplicaciones empresariales innovadoras.

SaaS es la opción más extrema, en la que se subcontrata toda la TI, permitiendo que las organizaciones se centren más en sus puntos fuertes esenciales (por ejemplo, cuidado de la saludo o servicios financieros), en lugar de realizar una gran inversión económica y de tiempo en tecnologías que pueden quedar a cargo de expertos en tecnología.

Cada paso desde IaaS a PaaS y a SaaS hace que las organizaciones cedan algún nivel de control de los sistemas que almacenan, gestionan y distribuyen sus datos confidenciales. Este aumento en la confianza depositada en terceros también implica un aumento en el riesgo.

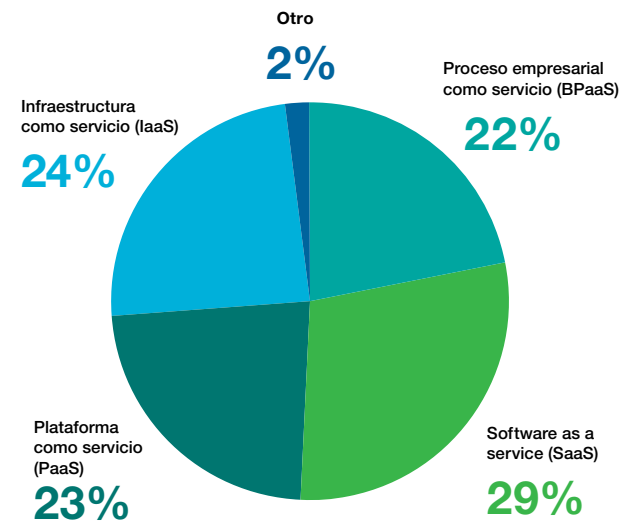


Figura 1: Pregunta de encuesta: "¿Cómo se divide el presupuesto actualmente asignado a los servicios de nube 'pública' entre los siguientes tipos de nube?"

Fuente: Ed Anderson y Sid Nag, "Market Trends: Cloud Adoption Trends Favor Public Cloud With a Hybrid Twist", Gartner, 4 de agosto de 2016. ID: G00294424.

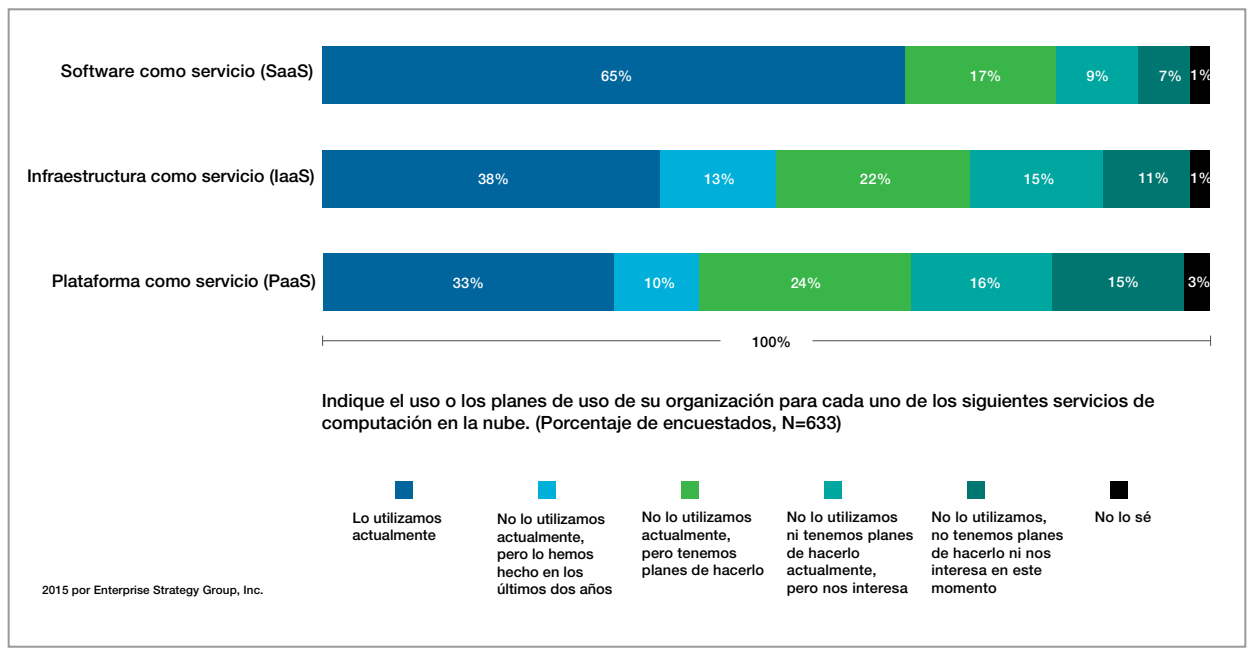
1.3 Despliegue de un entorno en la nube

El “uso de la nube” no es binario. Un estudio de más de 600 tomadores de decisiones empresariales muestra que la mayoría de las empresas encuestadas han adoptado al menos algunas aplicaciones de SaaS; menos del 20 % de los encuestados no tenía planes ni se interesaba por el uso de SaaS.

El despliegue de PaaS, que exige un mayor compromiso con el almacenamiento de datos y la computación fuera del sitio, comprensiblemente se queda atrásde las aplicaciones en la nube más graduales, pero el 67 % de los encuestados utilizan, han utilizado o planean adoptar la tecnología de PaaS.

La adopción de la infraestructura en la nube (IaaS), que transfiere la carga de la instalación y el mantenimiento de la infraestructura física de la empresa a un proveedor dedicado, se encuentra estadísticamente entre las opciones de PaaS y de SaaS. Al momento de la encuesta, el 73 % de los encuestados habían utilizado o tenían planes de utilizar alguna forma de infraestructura en la nube, o ya habían experimentado una infraestructura de este tipo.

Desafíos de la protección de datos en entornos virtuales y en la nube privada



2.1 Desafíos de la seguridad en la nube

La nube es especialmente adecuada para el almacenamiento de datos empresarial a largo plazo, brindando economías de escala tanto en materia de equipos como de administración que pueden hacer que los centros de datos basados en la nube sean un lugar para almacenar la información crítica del negocio más inteligente que una pila de servidores internos. Esto se debe a que, aun cuando los gastos de adquisición de almacenamiento se reducen, los costos del mayor uso empresarial y del personal necesario para la gestión del almacenamiento continúan aumentando. Sin embargo, si bien poner los datos en manos de administradores dedicados puede ayudar a ahorrar tiempo y dinero, también puede dar como resultado importantes desafíos de seguridad y crear nuevos niveles de riesgo.

Es importante darse cuenta de que, independientemente del modelo de despliegue o del tipo de servicio, los principios fundamentales de la seguridad de datos no deberían cambiar. Lo que sí cambia es el hecho de que sus datos confidenciales se almacenarán en muchos lugares, tanto dentro de su compañía como fuera de ésta. Esto significa que los controles de seguridad deberán acompañar sus datos. Al evaluar las tecnologías de seguridad de datos, elija soluciones que operen en múltiples entornos de forma transparente y simultánea. Asegúrese de que la solución de seguridad de datos sea dinámica y adaptable en una amplia variedad de entornos, para que no sea necesario integrar módulos de protección de datos adicionales de manera dispersa.

Mantener los datos a salvo en todas partes y de todos

El más importante de estos desafíos es obvio: los datos confidenciales están ahora en todas partes, tanto dentro como fuera de sus firewalls, y son gestionados de alguna forma por personas de su organización y por terceros. Ya no es posible proteger los datos confidenciales simplemente bloqueando el acceso a la red. De hecho, usted depende de la red para compartir y tener acceso a sus datos. Esto hace que la seguridad esté fundamentalmente en manos de más personas que nunca, muchas de las cuales ya no trabajan directamente para su empresa. En general, en los entornos en la nube, los proveedores de servicios en la nube (CSP) pueden tener acceso a sus datos confidenciales, lo cual hace que sean la “nueva frontera” en lo que respecta a las amenazas internas.

Además, los delincuentes cibernéticos ahora saben que los CSP almacenan grandes volúmenes de datos importantes. Estos dos riesgos hacen que capacidades tales como el cifrado de datos y la supervisión de la actividad de datos sean una parte especialmente valiosa de su estrategia de seguridad.

2.2 Desafíos de la seguridad en la nube

La portabilidad es la gran razón por la que el almacenamiento en la nube es una opción económica para comenzar. Los gastos de infraestructura (que abarcan desde propiedades inmobiliarias hasta costos de energía) varían significativamente según la zona geográfica e incluso el momento del día. Del mismo modo, los costos de almacenamiento y el rendimiento entre los tipos de medios cambian. Las cintas, los discos y el almacenamiento de estado sólido han presentado mejoras en materia de capacidad, velocidad y confiabilidad, y la combinación más económica de tecnologías de almacenamiento para que una empresa dada puede cambiar rápidamente. Por lo tanto, con el almacenamiento en la nube sus datos pueden encontrarse en un lugar diferente mañana, o en un medio diferente del medio en que se encontraban hoy. Lo mismo es cierto para la virtualización. No sólo los datos basados en la nube, sino también los recursos de computación basados en la nube, pueden cambiar de manera transparente y rápida tanto en términos de ubicación como de hardware.

La naturaleza cambiante de la nube significa que los enfoques de seguridad para el almacenamiento basado en la nube necesitan considerar diferentes tipos de almacenamiento. Su enfoque también debe tener en cuenta las copias, ya sean las copias de seguridad a largo plazo o las copias temporales creadas durante el movimiento de datos. Para responder a estos desafíos, seleccione soluciones que operen en las diferentes plataformas y utilice un cifrado sólido.

Incluso si sus datos no se almacenan principalmente en la nube, tanto la forma en que los datos dejan su empresa y uelven a ésta como las rutas utilizadas por éstos son preocupaciones importantes. Incluso en el caso de los datos que se mantienen principalmente cifrados y protegidos por un firewall a nivel local, si partes de tales datos se exponen al transmitirse a otra ubicación para propósitos de copia de seguridad o para su procesamiento por terceros, los datos confidenciales sólo estarán tan seguros como el eslabón más débil de la cadena de procesamiento de datos.

Una eficaz protección de sus datos en la nube requiere tanto medidas pasivas y preventivas (como el bloqueo del acceso a través de puertos no aprobados) como medidas activas, por ejemplo, la detección continua del acceso sospechoso a los datos. La principal de las medidas que están disponibles es el uso de cifrado para sus datos confidenciales. Aunque la detección de malware y el análisis comportamental diseñado para identificar el acceso sospechoso pueden ayudar a evitar vulneraciones de datos internas o externas (y tienen funciones valiosas por sí mismas), el cifrado ayuda a proteger los datos dondequiera que se encuentren, independientemente de si están en reposo o en movimiento.

2.3 Desafíos de la seguridad en la nube

Implicaciones administrativas y reglamentarias

La realidad del almacenamiento y la computación basados en la nube significa que la protección de los datos confidenciales en los sistemas en la nube y en la nube híbrida casi nunca es tan sencilla como desearían los administradores. Las herramientas de seguridad que ofrecen interfaces unificadas para los diferentes endpoints de la nube (desde las granjas de servidores dedicados fuera del sitio hasta las máquinas virtuales en infraestructuras de nube pública) constituyen un buen comienzo para hacer realidad la promesa de una administración remota eficiente.

También son igual de importantes los requisitos reglamentarios y la soberanía de datos (en otras palabras, las reglas que rigen la seguridad y la protección de datos cuando los datos confidenciales se almacenan físicamente en un lugar específico). El almacenamiento de datos en la nube puede hacer que los datos confidenciales se almacenen en ubicaciones en las que haya leyes más estrictas que las leyes en vigencia en su región original. Por ejemplo, una protección más estricta para los datos personales de los individuos que se encuentran en los países de la Unión Europea (UE) es obligatoria, de conformidad con los términos del Reglamento General de Protección de Datos (GDPR) de la UE. Estos requisitos se aplican incluso a a las empresas ubicadas en otras regiones del mundo que almacenan y tienen acceso a datos personales de los residentes de la UE

Conozca quién ha tenido acceso a sus datos:
IBM® Security Guardium® puede ayudar a proteger su infraestructura en la nube y y en la nube híbrida con herramientas de supervisión y de evaluación que revelan anomalías y vulnerabilidades.

3.1 Desafíos organizacionales

3

Las organizaciones aún tienen grandes dificultades cuando tratan de proteger sus datos confidenciales, y las normas complejas son una de las razones de ello. Forrester señala que, en la actualidad, "la mayoría de los arquitectos empresariales y profesionales de seguridad tienen dificultades para mejorar la seguridad de los datos o cumplir con requisitos de conformidad, debido a los crecientes silos de datos y volúmenes de datos. La aplicación de políticas de control de acceso uniformes en diferentes bases de datos, almacenes de datos, Hadoop, NoSQL y archivos se ha vuelto muy complicada."[2]

La virtualización tiene el potencial de hacer que la aplicación de controles de seguridad y mecanismos de conformidad resulte más fácil, pero sólo en caso de que el entorno virtual o en la nube privada sea capaz de respaldar la protección de datos confidenciales mediante una respuesta uniforme a los requisitos de conformidad, a las necesidades de control de acceso, a los requisitos de privacidad, a los requisitos de vulnerabilidad y a las necesidades de productividad.

Desafíos de la protección de datos en entornos virtuales y en la nube privada

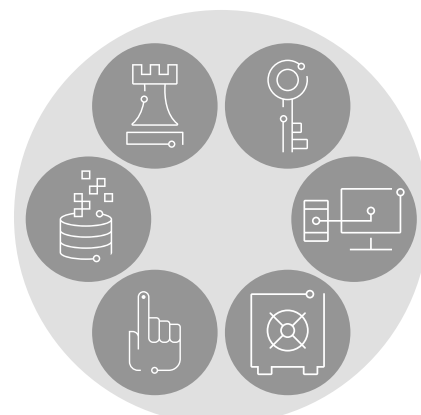


Figura 2: La protección de los datos almacenados en la nube requiere que los administradores presten atención a aspectos de seguridad que abarcan desde la seguridad y privacidad hasta la conformidad normativa en diferentes dominios.

3.2 Desafíos organizacionales

Conformidad

Piense en dónde residen los datos confidenciales en el entorno en la nube. Es importante identificar y clasificar los tipos de datos confidenciales, y establecer políticas para su uso, ya sea en la nube pública o en un entorno de nube privada. Si los datos se encuentran en una nube pública, usted necesitará comprender cómo el proveedor de infraestructura en la nube planea proteger sus datos confidenciales.

En ambos casos, comprender dónde residen los datos, qué dominios de información existen y cómo éstos se relacionan en toda la empresa ayudará a las organizaciones a definir las políticas adecuadas para proteger y cifrar dichos datos, y para demostrar la conformidad con regulaciones tales como Sarbanes-Oxley (SOX), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), el Protocolo de Automatización de Contenido de Seguridad (SCAP), la Ley Federal de Gestión de la Seguridad de la información (FISMA), la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA) y la Ley de Tecnología de Información en Salud para la Salud Económica y Clínica (HITECH). Las regulaciones continúan surgiendo, y las organizaciones permanecen responsables incluso cuando los datos se transfieren a la nube.

Privacidad

Otro desafío para los administradores del acceso a los datos es garantizar que sólo las personas con una razón empresarial válida tengan acceso a la información personal. Por ejemplo, un médico necesitará consultar información confidencial, como los datos de los síntomas y pronósticos de un paciente, mientras que un empleado de facturación sólo necesitará el número de seguro y la dirección de facturación de dicho paciente.

3.3 Desafíos organizacionales

Controles de acceso

Los delincuentes cibernéticos son inescrupulosos y tienen intenciones perjudiciales. Podrían ser científicos de la computación deshonestos con el propósito de alardear de lo que son capaces de hacer o de hacer una declaración política, o podrían ser intrusos organizados y hábiles. Estados extranjeros han patrocinado a hackers para que recopilen inteligencia de órganos gubernamentales. Es posible que los delincuentes sean incluso empleados descontentos. Las vulneraciones también pueden ser accidentales, como las que se producen cuando se establecen autorizaciones de manera incorrecta en una tabla de base de datos, o cuando las credenciales de un empleado se ven comprometidas. Las mejores prácticas recomiendan que se autorice tanto a los usuarios con privilegios como a los usuarios finales comunes con el “menor privilegio posible”, para minimizar el riesgo de abuso de privilegios o de errores.

Las organizaciones deben proteger los datos de los ataques internos y externos en entornos físicos, virtuales y en la nube privada. Las protecciones del perímetro también son importantes, pero es igual de importante proteger los datos confidenciales en sí. Si se vulnera el perímetro, los datos confidenciales necesitarán encontrarse seguros (e inutilizables por un delincuente), para minimizar el impacto de las vulneraciones y garantizar que el hacker no tenga vía libre. Las defensas deben incluir una solución de seguridad de datos por niveles, para que los administradores puedan entender qué ocurre dentro de la nube privada, por ejemplo, al comprender los patrones de acceso a los datos y los comportamientos de los usuarios con privilegios.

El desafío consiste en brindar las protecciones de acceso y de datos adecuadas, cumpliendo con las necesidades empresariales y garantizando que los datos se gestionen únicamente cuando sea estrictamente necesario, dondequiera que se encuentren.

Productividad

Las políticas de seguridad y de privacidad deben impulsar y mejorar las operaciones empresariales, pero no interferir en éstas. Además, deben incorporarse a las operaciones cotidianas y funcionar sin problemas en todos los entornos, ya sean entornos de nube privada, entornos de nube pública, entornos locales o entornos híbridos, sin afectar la productividad del usuario. Por ejemplo, cuando se despliegue nubes privadas para facilitar la realización de pruebas de aplicaciones, considere el uso de cifrado o de tokenización para mitigar el riesgo de exposición de los datos confidenciales.

3.4 Desafíos organizacionales

Vulnerabilidad

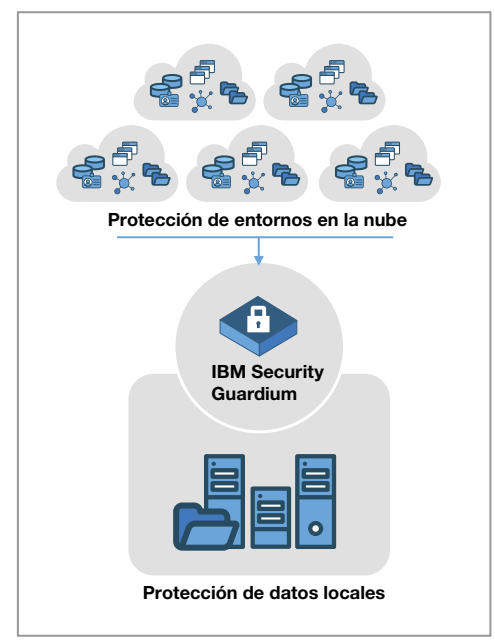
Hoy, las organizaciones cuentan con diferentes tecnologías de seguridad para proteger los datos empresariales y respaldar la conformidad. Sin embargo, el número de vulnerabilidades del repositorio de datos es alto, y los delincuentes pueden aprovechar incluso oportunidades pequeñísimas. Es importante comprender que las vulnerabilidades desde todas las perspectivas y desarrollar un enfoque para solucionarlas. Entre las vulnerabilidades se encuentran la pérdida de revisiones, las microconfiguraciones y la configuración predeterminada de los sistemas. Esta complejidad se vuelve cada vez más difícil de controlar y gestionar a medida que los repositorios de datos se virtualizan.

A medida que las organizaciones adoptan nubes públicas y privadas, por ejemplo, estas soluciones no siempre ofrecen escalamiento. Además, algunos enfoques de cifrado están vinculados a un hardware o un recurso de red específicos. En un entorno en la nube, los administradores no pueden depender del acceso a la infraestructura de hardware de bajo nivel.

Hay otro problema que suele surgir cuando una nube privada se utiliza para desarrollar aplicaciones o realizar pruebas de aplicaciones. Nuevas bases de datos se crean y se dan de baja regularmente. Los datos necesitan protección, ya que estas bases de datos se crean de manera dinámica para respaldar las pruebas y el desarrollo. Un enfoque de seguridad de datos escalable para un entorno en la nube privada de este tipo significa que, a medida que tales bases de datos se crean, también se detectan automáticamente, y los datos que residen allí se clasifican, monitorean y protegen automáticamente.

Finalmente, piense en el uso de las herramientas desarrolladas internamente y disponibles hoy para la seguridad de datos, por ejemplo, las rutinas de enmascaramiento de datos o los scripts de supervisión de la actividad de la base de datos. ¿Se requieren cambios de codificación para hacer que funcionen en una base de datos virtual? Es probable que se requieran inversiones significativas para actualizar estas soluciones desarrolladas internamente; incluso así, se enfrentarán desafíos importantes. Lo ideal es que, a medida que se agreguen nuevas bases de datos u otros orígenes de datos, los procesos y procedimientos de seguridad se lleven a cabo sin intervenciones manuales. En resumen, las estrategias de seguridad deben incorporarse a la estructura de todos los entornos en la nube.

Enfoque de protección de datos



4.1 Enfoque de protección de datos

Las organizaciones deben tratar de centralizar los controles de seguridad y de protección de datos de los entornos en la nube pública y en la nube privada, así como también en el resto de la empresa, y garantizar que las funciones se segreguen, para que los administradores de datos no se conviertan también en administradores o auditores de seguridad. Entre los elementos clave de una estrategia de nube segura, se encuentran los siguientes:

- Entender dónde hay datos confidenciales y quiénes tienen acceso a éstos. Las organizaciones sólo podrán proteger los datos confidenciales con cifrado o aplicar controles de acceso sólidos si saben dónde residen dichos datos y cómo se relacionan eb toda la empresa.
- Proteger los datos confidenciales estructurados y sin estructurar, en línea y fuera de línea, con tecnologías adecuadas, y establecimiento de los requisitos de acceso correctos.
- Proteger los datos más allá de la producción, incluyendo los entornos de desarrollo, pruebas y calidad.
- Supervisar continuamente y de manera segura el acceso a los datos confidenciales, dondequiera que se encuentren.
- Demostrar que se cumple la normativa para que sea posible superar las auditorías utilizando informes pregenerados para auditores, con un flujo automatizado, y se puedan enviar los informes correctos a las personas adecuadas en el momento oportuno, para su aprobación.

Estrategias de protección completas para todos los entornos en la nube y en la nube híbrida para permitir el envío de alertas sobre comportamientos sospechosos a los administradores de seguridad. Además, las organizaciones deben considerar soluciones de seguridad de datos que admitan una conformidad automatizada para agilizar el proceso.

Los procesos de seguridad de datos para los entornos en la nube deben realizar un seguimiento continuo de los datos y proporcionar percepciones sobre quiénes tienen acceso a los datos en las aplicaciones, bases de datos, almacenes de datos, recursos compartidos de archivos, entornos de Big Data y más. Este enfoque puede ayudar a garantizar una protección completa para los datos organizacionales confidenciales, independientemente de dónde se encuentren.

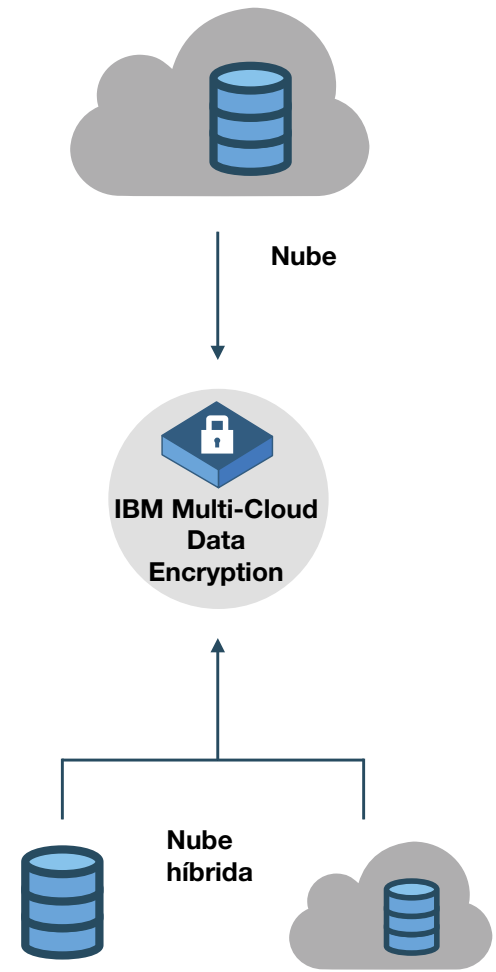
4.2 Enfoque de protección de datos

Las cargas reglamentarias a las que se ven sometidos los poseedores de datos (así como también los riesgos de vulneración) pueden hacer que las empresas que están considerando obtener un almacenamiento basado en la nube nuevo o ampliado actúen con prudencia. Un cifrado sólido es la respuesta más obvia al desafío de proteger los datos confidenciales, ya sea en la infraestructura local o fuera del sitio, pero el cifrado plantea problemas complicados de portabilidad y garantía de acceso. Los datos son tan sólidos como la seguridad y confiabilidad de las claves que los protegen. ¿Cómo se hacen copias de seguridad de las claves? ¿Cómo los datos pueden moverse de manera transparente entre proveedores de nube, o compartirse entre el almacenamiento basado en la nube y el almacenamiento local?

IBM Multi-Cloud Data Encryption protege los datos en la nube (y en la nube híbrida), teniendo en cuenta los requisitos de portabilidad y conformidad. Para mantener las claves de cifrado accesibles y fácilmente disponibles, éstas pueden integrarse con un administrador de claves avanzado.

Además, IBM Security Key Lifecycle Manager puede ayudar a los clientes que necesitan una protección de datos más estricta, empleando un almacenamiento cifrado basado en hardware, para simplificar y centralizar la gestión de las claves de cifrado sin temor a la exposición de los datos en los entornos en la nube virtual.

La gestión de claves es la base de un entorno de cifrado seguro.



5.1 Conclusión

Para garantizar que los datos estén protegidos en los entornos virtuales y en la nube, las organizaciones necesitan comprender qué datos se introducen en estos entornos, cómo se puede supervisar el acceso a tales datos, qué tipos de vulnerabilidades existen y cómo se puede demostrar la conformidad. Se deben incorporar protecciones a los entornos en la nube desde el comienzo, con el objetivo inicial de ayudar a las organizaciones a demostrar la conformidad.

Al momento de seleccionar soluciones de seguridad y protección de datos, elija las soluciones que sean escalables y extensibles en todas las infraestructuras de TI, protegiendo los entornos físicos, virtuales y en la nube de ataques externos malintencionados, del fraude, del acceso no autorizado y de las vulneraciones internas. Estas soluciones deben funcionar en un entorno en la nube sin necesidad de ajustes especiales, configuraciones o gastos adicionales. Este enfoque proporcionará una plataforma eficiente para la entrega de seguridad y privacidad de datos, ayudará a controlar los costos al reducir los recursos de seguridad de datos y brindará una mayor agilidad y flexibilidad, con opciones de autoservicio para seguridad y privacidad.

Guardium puede ayudar a respaldar su estrategia de computación en la nube con:

- Supervisión de datos y actividad de archivos, evaluaciones de vulnerabilidad, redacción y cifrado de datos, bloqueo dinámico, cuarentena y alertas
- Clasificación y descubrimiento automáticos de los datos confidenciales nube
- Enmascaramiento de datos estático y dinámico, para garantizar un modelo de acceso menos privilegiado para los recursos en la nube
- Informes de auditoría y conformidad predefinidos, personalizados para diferentes normas, con el fin de demostrar la conformidad y automatizar el flujo de trabajo de conformidad, en entornos locales y en la nube

5.2 Conclusión

El software Guardium proporciona una solución completa para las infraestructuras físicas, virtuales y en la nube por medio de controles de seguridad centralizados y automatizados en entornos heterogéneos. Guardium ayuda a agilizar la conformidad y a reducir el riesgo, y ofrece imágenes listas para instalar para despliegues de IaaS en las principales plataformas en la nube, como IBM SoftLayer®, Microsoft Azure y Amazon Web Services, además de operar entre los entornos de Microsoft Windows, UNIX y Linux.

La arquitectura flexible de Guardium admite varios modelos de despliegue distintos. Usted puede elegir la arquitectura de sistema más adecuada para su empresa: todos los componentes de Guardium pueden desplegarse en la nube, o usted puede optar por mantener algunos de estos componentes, como el gerente central, en la infraestructura local.

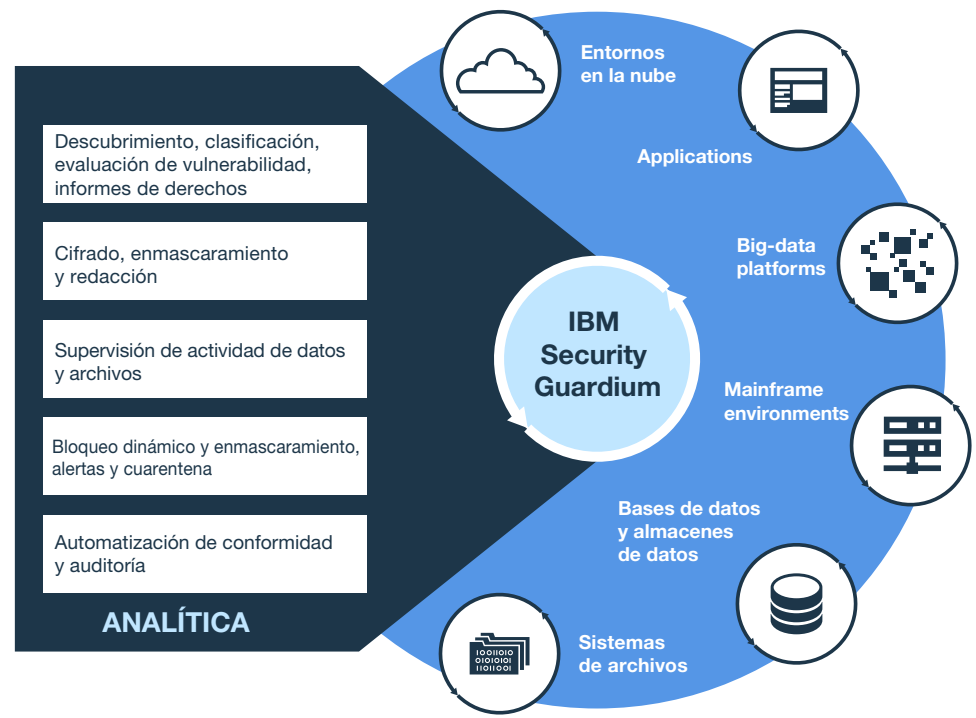


Figura 3: Guardium proporciona una protección de datos integral en una amplia gama de entornos y plataformas de tecnología.

5.3 Conclusión

Esta flexibilidad permite que los clientes existentes amplíen su estrategia de protección de datos a la nube con facilidad, sin afectar los despliegues existentes.

Los recopiladores de supervisión de entrada desplegados en la nube pueden suministrar fácilmente sus datos al gestor central, garantizando una vista única y consolidada de las amenazas a la protección de sus datos, dondequiera que se encuentren.

Los controles de seguridad, que pueden mantener a los delincuentes cibernéticos lejos del almacén de datos o detectar rápidamente una vulneración exitosa, son herramientas importantes. Sin embargo, en la era de los datos portátiles, de la transferencia de cargas de trabajo y de la virtualización, mantener los datos a salvo con cifrado es igualmente importante.

Las soluciones de seguridad de datos de IBM ayudan a proteger los datos confidenciales, para que las organizaciones puedan estar seguras de que sus datos estarán protegidos en los complejos entornos virtualizados y en la nube.

5.4 Recursos Adicionales

Acerca de las soluciones de IBM Security

IBM Security ofrece uno de los portafolios de productos y servicios de seguridad empresarial más avanzados e integrados. Este portafolio, que cuenta con el respaldo de la mundialmente reconocida investigación y desarrollo de IBM X-Force®, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger holísticamente a su personal, sus infraestructuras, sus datos y sus aplicaciones, ofreciendo soluciones para la gestión de la identidad y del acceso, la seguridad de las bases de datos, el desarrollo de aplicaciones, la gestión del riesgo, la gestión de endpoints,la seguridad de la red y mucho más.

Estas soluciones permiten que las organizaciones gestionen el riesgo de manera efectiva e implementen una seguridad integrada para dispositivos móviles, nubes, redes sociales y otras arquitecturas de negocios empresariales. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, supervisa 15 mil millones de eventos de seguridad diarios en más de 130 países y posee más de 3000 patentes de seguridad.

Para obtener más información sobre la seguridad de datos, la conformidad y la nube, visite **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, EE. UU.

Producido en los Estados Unidos de América
Mayo de 2017

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.

1. Thomas J. Bittman, "Internal Private Cloud Is Not for Most Mainstream Enterprises," *Gartner*, 22 de mayo de 2015.

2. Noel Yuhanna, "Enterprise Data Virtualization, T1 2015," *The Forrester Wave*, 11 de marzo de 2015.

Se ruega reciclar

WGM12362-USEN-00