RSA®

The Security Division of EMC

White paper

La función de la seguridad en cloud computing de confianza

¿Cuáles son las implicaciones para la seguridad de cloud computing?

El entusiasmo por cloud computing está tan relacionado con el aspecto económico como con la tecnología. El aumento de las aplicaciones y del volumen de datos que deben administrarse ha convertido a los data centers en un elemento importante del gasto corporativo, sin un final previsto. La cloud computing pública parece ser una forma de manejar algunos de estos costos.

El concepto de cloud computing es sencillo: se reemplazan los recursos de TI que demandan mucho capital y deben administrarse de manera interna por capacidad y servicios de TI de "pago por uso" contratados a precios básicos. Estos servicios están diseñados a partir de nuevas tecnologías, como la virtualización y las arquitecturas orientadas al servicio, y aprovechan Internet a fin de reducir el costo de los recursos de hardware y software de TI para servicios informáticos, redes y almacenamiento. Al mismo tiempo, las empresas están usando los mismos conceptos y las mismas tecnologías para crear nubes privadas, a fin de aprovechar los servicios de TI básicos y centralizados que satisfacen sus necesidades de seguridad.

Hoy en día, las implementaciones de nubes públicas y privadas deben comprender un conjunto adecuado de principios de seguridad y, por lo tanto, garantizar a los usuarios y los clientes un ambiente de cloud computing de confianza.

Contenido

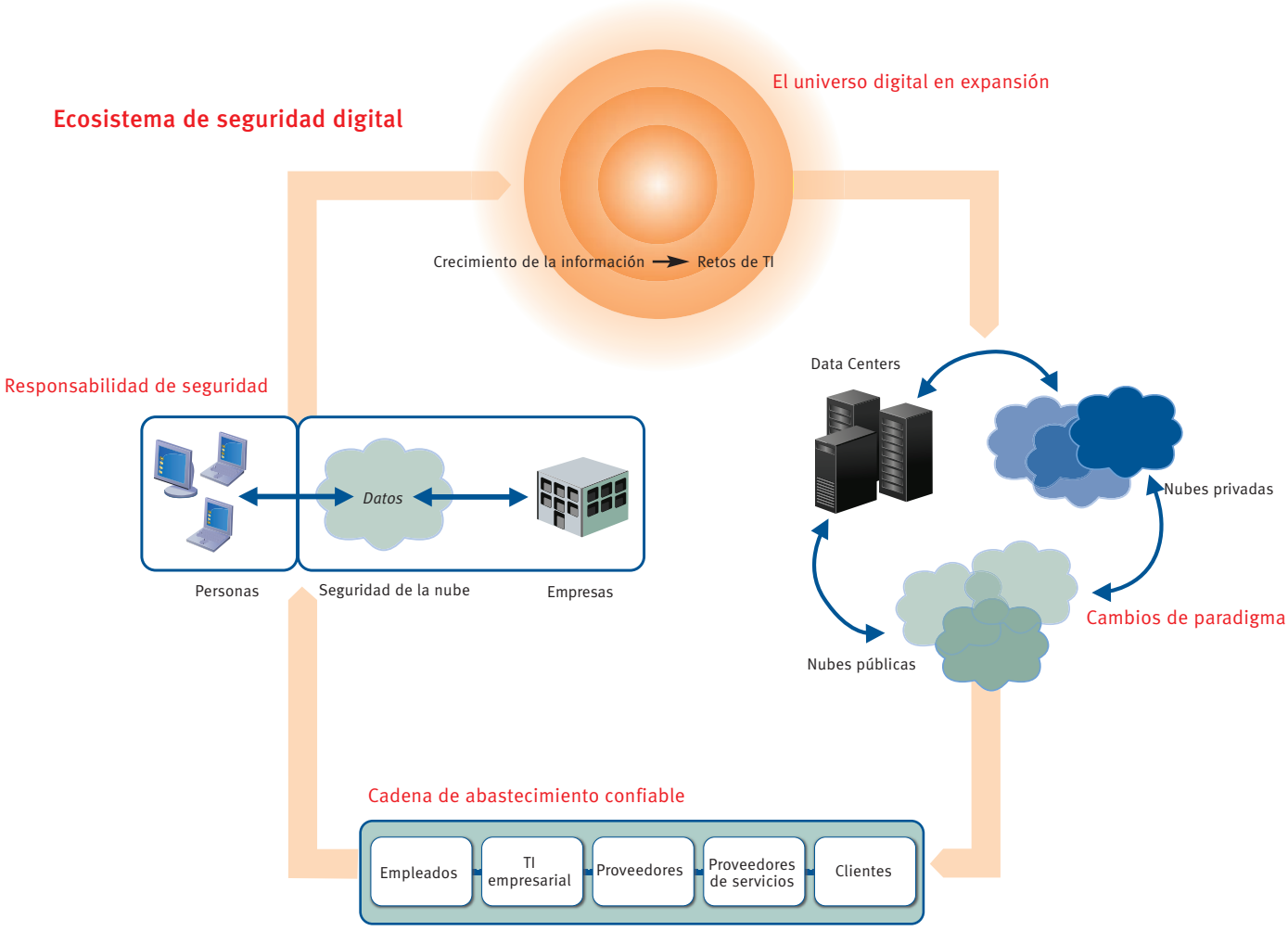
I. Descripción general

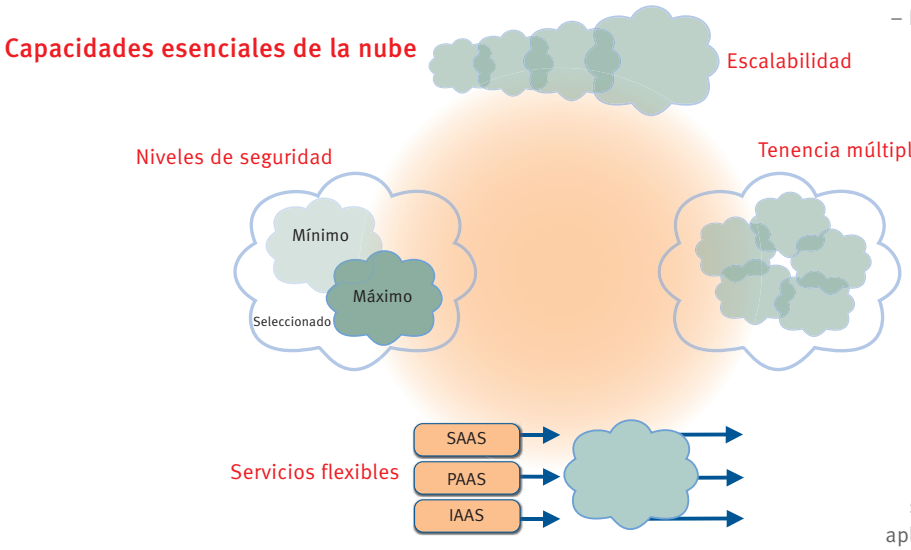
En esta etapa temprana del desarrollo de nubes públicas, las ofertas son una combinación de aplicaciones empresariales convencionales y para el consumidor de activos que administran datos relativamente poco delicados, como el correo electrónico, los servicios de mensajería instantánea y los espacios web compartidos, y aquellas que manejan datos más delicados, como Salesforce.com y Mozy de EMC. No obstante, si cloud computing pretende satisfacer las necesidades de la empresa en relación con la confidencialidad de los datos del Cliente y el cumplimiento de las directivas legales, deberá proporcionar niveles más altos de seguridad para brindar soporte a aplicaciones empresariales más delicadas.

La cloud computing pública también incorpora nuevos interesados en la ecuación de la seguridad (proveedores de servicios de otros fabricantes, proveedores y contratistas de infraestructuras) y reduce el control que TI tiene sobre cada una de estas áreas.

Cloud computing pública incorpora nuevos interesados en la ecuación de seguridad y reduce el control de TI.

Si cloud computing tiene éxito como una alternativa al data center corporativo, los departamentos de TI requerirán relaciones con proveedores de nubes que les permitan confiar en los servicios de nube y verificar los eventos en la nube. Deberá soportar con eficacia un alto nivel de seguridad, similar al de los modelos actuales centrados en controles, y deberá implementarse de modo que permita a las empresas confiar en las partes que se extienden de sus propios data centers hacia una nube pública.





II. Cloud Computing pública: escalabilidad y tenencia múltiple

La cloud computing pública describe una arquitectura informática que amplía el enfoque orientado al servicio (ejemplificado en conceptos, como "utility computing", "arquitecturas orientadas al servicio" y "software como un servicio") en un modelo de mercado. Los proveedores ofrecen servicios que "se ejecutan en la nube", dado que es posible acceder a ellos por medio del Protocolo de Internet y tienen una ubicación independiente, lo que significa que los usuarios no necesitan conocer el lugar en el que se encuentran los recursos de TI subyacentes.

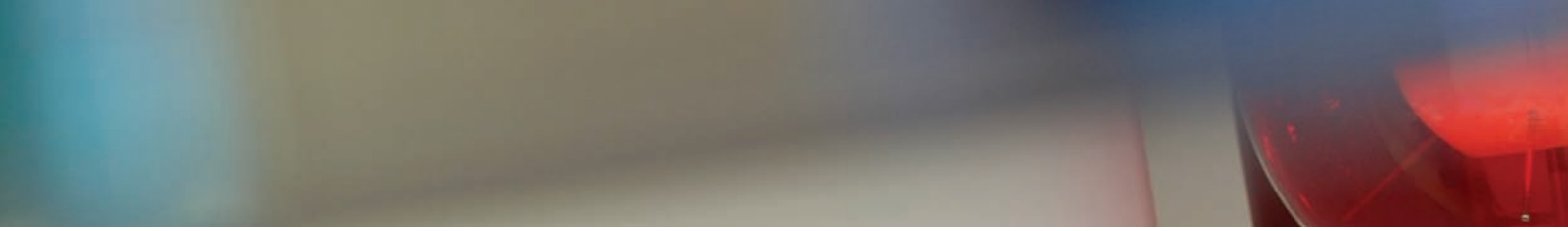
Los servicios de nube tienen dos sellos distintivos: son escalables (los recursos requeridos de almacenamiento y potencia informática pueden aumentarse o disminuirse en función de las necesidades de los clientes) y son de tenencia múltiple (proporcionan almacenamiento simultáneo y seguro de servicios para diversos clientes utilizando los mismos recursos de la infraestructura de nube). La cloud computing actual comprende tres tipos de servicios:

- Software como un servicio (SaaS). Una aplicación se almacena como un servicio proporcionado a los clientes. Entre los ejemplos, se incluyen la aplicación web CRM, de Salesforce.com, y Gmail y Google Docs, de Google.
- Plataforma como un servicio (PaaS). La combinación de servicios de software e infraestructura con herramientas de desarrollo de aplicaciones, de modo que las aplicaciones y los servicios web puedan crearse y almacenarse. Entre los ejemplos, se incluyen Google AppEngine y AppExchange, de Salesforce.com.
- Infraestructura como un servicio (IaaS). Las funcionalidades generalmente proporcionadas de manera local, mediante un equipo de escritorio o un data center, se ofrecen como recursos remotos, de modo que un Cliente pueda definir y administrar tareas informáticas o de almacenamiento. Entre los ejemplos, se incluyen los servicios de almacenamiento basados en políticas Atmos, de EMC, y Elastic Compute Cloud ("EC2"), de Amazon, para servicios informáticos.

No obstante, antes de que cloud computing pueda estar a la altura de lo que promete a las empresas, necesita más refinamiento, especialmente, en el área de seguridad. Hasta la fecha, la mayoría de las aplicaciones orientadas a las nubes públicas han sido aplicaciones centradas en el consumidor creadas en función del almacenamiento de datos básicos y el procesamiento de transacciones. En esta etapa inicial, las aplicaciones y los datos que se procesan en las nubes no son predominantemente delicados, y los servicios de nubes ofrecen seguridad mínima o con disponibilidad general. Las ofertas de nubes en sí son islas informáticas patentadas, con pocos estándares y posibilidades limitadas de interoperabilidad.

Las tendencias en el crecimiento de la información simplemente aumentarán la urgencia del problema para las empresas. En el estudio "The Expanding Digital Universe" (El universo digital en expansión), de IDC, "se analiza el explosivo crecimiento en el volumen de información delicada que se crea; la proporción en la que se crean y se almacenan los datos crecerá seis veces para el año 2010". El estudio destaca que, si bien las personas crearán información mayormente digital, las corporaciones serán responsables de la seguridad, la privacidad, la confiabilidad y el cumplimiento de normas de, al menos, el 85% del universo digital en rápida expansión.

Resulta claro que la cloud computing pública debe ser más segura para que las empresas la acepten más. Con este avance, la confianza y la verificación serán nuevamente los activadores clave de la seguridad. Las empresas necesitarán garantizar la confidencialidad, la integridad y la disponibilidad de los datos cuando terceros en la cadena de servicios de nube los transmitan, los almacenen o los procesen.



Antes de que las empresas puedan usar nubes de manera más innovadora, se deben mejorar las tecnologías de seguridad, los estándares y la interoperabilidad.

III. Los retos de la nube: la seguridad es el gran interrogante

Aprovechar cloud computing significa importantes cambios para las organizaciones de TI de la empresa. El más grande será la disminución del control aun cuando se les asigne la tarea de asumir una mayor responsabilidad por la confidencialidad y el cumplimiento de normas de las prácticas informáticas en la empresa. Esto hace que la seguridad sea un problema importante, dado que los departamentos de TI supervisan los servicios de nube y a los proveedores.

Relaciones cambiantes

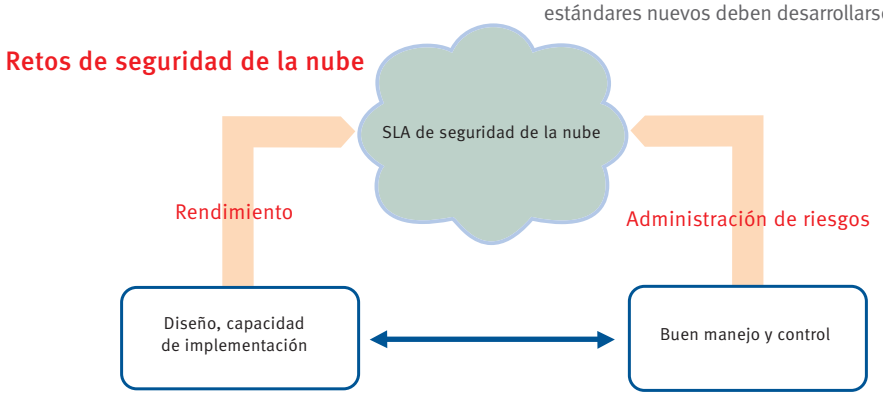
Un problema clave para cloud computing es que los aspectos de la seguridad de infraestructura tradicional van más allá del control de una organización y se desplazan a la nube. Esto dará lugar a cambios fundamentales en la cantidad y en las funciones de los interesados en la seguridad, ya que las empresas entregan el control de la infraestructura y de los procesos de seguridad a contratistas externos. Las relaciones de confianza entre los diversos interesados en la nube (usuarios, corporaciones, redes, proveedores de servicios, etc.) deben considerarse atentamente a medida que la cloud computing pública evoluciona para administrar datos empresariales delicados.

Los data centers convencionales cuentan con seguridad basada en estructuras similares a fortalezas que protegen los datos dentro de infraestructuras físicas de hardware y de software seguras: su seguridad depende principalmente del control del acceso de los usuarios y las personas encargadas del mantenimiento de datos e infraestructura. En cloud computing, aún existe un data center en algún lugar, pero ¿quién lo controla? Cloud computing disipa muchos de los límites de seguridad corporativa tradicionales y sustituye las cadenas de custodia transitorias de los datos, lo que conlleva importantes implicancias para la seguridad y la confianza de los datos y las aplicaciones empresariales confidenciales.

El uso compartido del control plantea muchas preguntas sobre la responsabilidad. ¿Cómo sabrá qué empleados de su proveedor de nube tienen acceso a la información y las aplicaciones? Ese acceso debe ser detallado, de modo que solo pocas personas seleccionadas que puedan controlarse tengan acceso amplio.

Estándares

Antes de que los datos delicados y reglamentados se trasladen a la nube pública, se deben enfrentar los problemas de estándares de seguridad y compatibilidad, entre ellos, la autenticación sólida, la autorización delegada, la administración de claves para datos encriptados, la protección contra la pérdida de datos y la creación de informes reglamentarios. ¿Cómo se cumplirán estos requerimientos en las infraestructuras de nube individuales y en varias nubes seleccionadas por el consumidor como mejores prácticas? Los proveedores de servicios de nube actuales pueden convertirse en modelos de facto en función de los cuales pueden emerger la seguridad y la federación de los controles de autorización. O bien, es posible que, del trabajo actualmente realizado por diversos organismos, surjan las respuestas a preguntas, como qué estándares actuales se pueden aplicar a cloud computing, qué brechas existen y qué estándares nuevos deben desarrollarse.



Portabilidad entre nubes públicas

Si bien cloud computing promete una arquitectura abierta y de fácil integración, las ofertas tempranas de nubes tienen tendencia a crear "silos" de seguridad: los usuarios necesitan una cuenta de Amazon para usar el servicio EC2 de Amazon y una cuenta de Google para acceder a las aplicaciones de AppEngine. Las empresas requerirán portabilidad de información y de identidades entre las diferentes nubes, de modo que puedan combinar y ajustar sus servicios en un ambiente abierto basado en estándares que permita la interoperabilidad.

La portabilidad se convertirá en un problema importante a medida que las infraestructuras de múltiples nubes ofrezcan servicios más complejos. Por ejemplo, imagine que desea alquilar un gran volumen de potencia de CPU de Amazon durante algunos días para realizar un análisis profundo de los datos de sus clientes utilizando una herramienta analítica personalizada, pero los datos están en Salesforce.com. Las nubes deberán comunicarse entre sí de manera segura.

Confidencialidad y privacidad

Las unidades de negocios ya están asignando tareas a los departamentos de TI que implican la protección de los datos en las nubes privadas y públicas, con la expectativa de que la información delicada pierda su estado delicado o se implemente con autorización de acceso verificable para proteger su privacidad y su confidencialidad. Las organizaciones de TI históricamente no han desarrollado la capacidad para identificar y clasificar de con eficacia usuarios y datos delicados. Sin esta capacidad, enfrentarán dificultades para extender las funcionalidades de seguridad a los ambientes de nubes.

¿De qué manera su proveedor de nubes garantizará la confidencialidad y la privacidad? Recientemente, un proveedor de telefonía celular se sintió avergonzado, por ejemplo, cuando sus empleados vieron los registros telefónicos antiguos de Barack Obama. ¿Cómo se pueden evitar estos incidentes? ¿De qué manera se protegerá contra amenazas internas, como un empleado del proveedor de nubes que extrae información empresarial delicada? Los proveedores de nubes deberán enfrentar esta responsabilidad fundamental.

Controles de acceso viables

Los requerimientos del buen manejo y control de la información deberán equilibrarse con el deseo de los usuarios de contar con un control de acceso eficiente y sólido al mismo tiempo. Los usuarios y las corporaciones esperarán que el acceso sea transparente y conveniente. En el caso de muchas nubes, como las que ofrecen servicios populares al público general, es posible que los usuarios no toleren un enfoque basado en token.

Otro punto débil importante es la carencia de autorización delegada. Mientras algunos servicios de nube ofrecen una autenticación delegada sólida (por ejemplo, Salesforce.com) que permite el control de acceso basado en la identidad del usuario, pocos (si es que hay alguno), ofrecen autorización delegada para permitir el control de acceso basado en el contenido de la información en sí. Esta capacidad se está convirtiendo en un factor cada vez más importante debido a la incorporación de Web 2.0, donde los privilegios detallados para la administración y el control de autorizaciones serán sumamente esenciales.

Cumplimiento de normas

Muchas unidades de negocios están optando por el uso de servicios de nube en función del aspecto económico atractivo y omiten los departamentos de TI para almacenar las aplicaciones y los datos en la nube directamente. Esto crea varios problemas para las organizaciones de TI con un menor control interno y externo. Las actividades de las unidades de negocios multiplican los retos de cumplimiento de normas del departamento de TI incluso cuando los departamentos legales y de cumplimiento de normas prevén que los departamentos de TI podrán informar y demostrar el control sobre la información delicada. Además, cada Cliente empresarial debe evaluar atentamente el cumplimiento de la norma SAS-70 de un proveedor de nubes para comprobar si la certificación cumple con la política de cumplimiento de normas establecida por su propia empresa.

La creación de informes será un requerimiento clave para cualquier ambiente de nube en el que haya información de identificación personal (PII) y otros datos delicados o reglamentados. ¿Quién será responsable de garantizar el cumplimiento de normas? ¿Usted o su proveedor de nubes? ¿Tendrá acceso a los datos de log del ambiente de nube en el que se encuentra la información de su empresa para poder correlacionarlos con eventos en otros sistemas? ¿Qué sucede si alguien roba datos de su sistema basado en nubes en un intento de forzar el acceso a los sistemas del data center administrado internamente de su empresa?

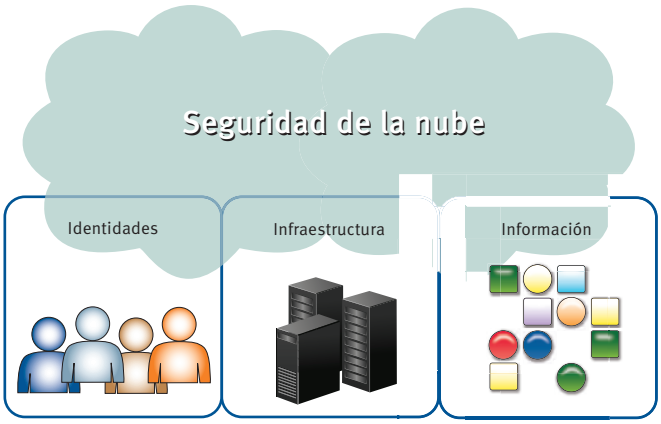
¿Cómo se correlacionan esos eventos? ¿Quién es responsable si se viola alguna PII? ¿Sabrá cuál es la ubicación física de su información? Estas preguntas pueden crear un problema relacionado con el cumplimiento de reglamentaciones internacionales.

Niveles de servicio de seguridad

Dado que todos los tipos de datos terminarán en las nubes, desde los datos de mayor valor a los datos masivos y no delicados, habrá una necesidad cada vez mayor de contar con distintos niveles de servicio de seguridad que se correspondan con la confidencialidad de diferentes tipos de datos. El reto real será el mapeo de niveles de seguridad a procesos de información o de negocios, de modo que puedan transferirse a la nube al menor costo posible, pero al nivel de seguridad más alto necesario.

> Se requerirán distintos niveles de servicio de seguridad para que se ajusten a la confidencialidad de diferentes tipos de datos.

Elementos principales para proteger la nube



IV. Principios para la protección de la nube: seguridad de la identidad, la información y la infraestructura

La cloud computing pública requiere un modelo de seguridad que reconcilie la escalabilidad y la tenencia múltiple con la necesidad de confianza. A medida que las empresas trasladan sus ambientes informáticos con las identidades, la información y la infraestructura a la nube, deben estar dispuestas a renunciar a cierto nivel de control. Para hacerlo, deben confiar en los sistemas y los proveedores de nubes, y verificar los procesos y los eventos de nubes. Entre los componentes básicos importantes de la confianza y de las relaciones de verificación, se incluyen el control de acceso, la seguridad de los datos, el cumplimiento de normas y la administración de eventos; todos ellos son elementos de seguridad bien comprendidos por los departamentos de TI actuales, implementados con productos y tecnologías existentes, y extensibles a la nube.

Seguridad de la identidad

La administración de identidades end-to-end, los servicios de autenticación de otros fabricantes y la identidad federada se convertirán en un elemento clave de la seguridad de la nube. La seguridad de la identidad preserva la integridad y la confidencialidad de los datos y las aplicaciones, a la vez que ofrece acceso de disponibilidad inmediata a los usuarios adecuados. El soporte para estas capacidades de administración de identidades de usuarios y componentes

de la infraestructura será un requerimiento importante para cloud computing, y la identidad deberá administrarse de manera que cree confianza. Se requerirá.

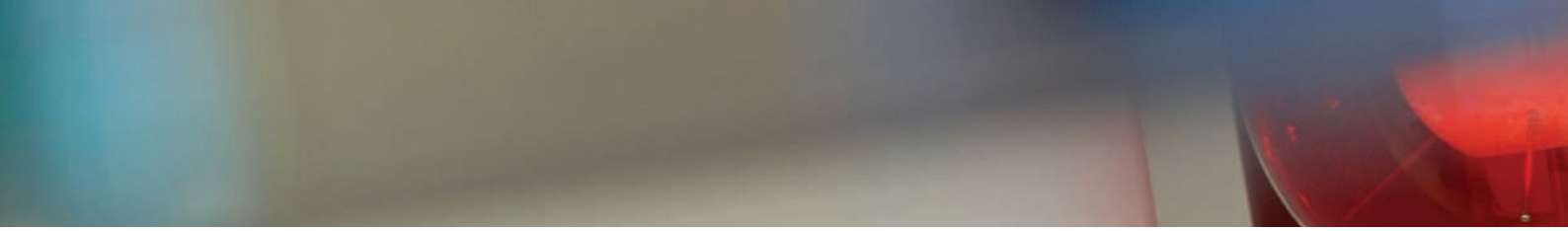
- Autenticación sólida: cloud computing debe ir más allá de la autenticación débil de nombres de usuario y contraseñas si pretende brindar soporte a la empresa. Esto significa adoptar técnicas y tecnologías que ya son estándar en el área de TI empresarial, como la autenticación sólida (autenticación de múltiples factores con tecnología de contraseña de un solo uso), la federación dentro de las empresas y entre estas, y la autenticación basada en riesgos que mide el historial de comportamiento, el contexto actual y otros factores que permiten evaluar el nivel de riesgo de la solicitud de un usuario. Niveles adicionales de autenticación serán fundamentales para cumplir con los acuerdos de nivel de servicio de seguridad; y el uso de un modelo de autenticación basado en riesgos que sea transparente en gran medida para los usuarios reducirá la necesidad de una federación más amplia de controles de acceso.
- Autorización más granular: la autorización puede ser general en una empresa o, incluso, en una nube privada. No obstante, para manejar datos delicados y requerimientos de cumplimiento de normas, las nubes públicas necesitarán capacidades de autorización granular (como controles basados en funciones e IRM) que puedan ser persistentes en toda la infraestructura de nube y el ciclo de vida de los datos.

Los datos delicados en la nube requerirán seguridad granular, que debe mantenerse de manera consistente durante todo el ciclo de vida de los datos.

Seguridad de la información

En el data center tradicional, los controles sobre el acceso físico, el acceso a hardware y software, y los controles de identidad se combinan para la protección de los datos. En la nube, esa barrera de protección que garantiza la seguridad de la infraestructura se disipa. Para compensar, la seguridad deberá estar centrada en la información. Los datos necesitan que su propia seguridad se traslade con ellos y los proteja. Se requerirá.

- **Aislamiento de datos**: en situaciones de tenencia múltiple, será necesario mantener los datos de manera segura para protegerlos cuando varios clientes usen recursos compartidos. La virtualización, la encriptación y el control de acceso serán excelentes herramientas que permitirán distintos grados de separación entre las corporaciones, las comunidades de interés y los usuarios. En el futuro cercano, el aislamiento de datos será más importante y ejecutable para IAAS de lo que quizá será para PAAS y SAAS.
- **Seguridad de datos más granular**: a medida que la confidencialidad de la información aumenta, la granularidad de la implementación de la clasificación de los datos debe aumentar. En los ambientes de data center actuales, la granularidad del control de acceso basado en funciones a nivel de grupos de usuarios o unidades de negocios es aceptable en la mayoría de los casos porque la información permanece dentro del control de la empresa. Para la información en la nube, los datos delicados requerirán seguridad a nivel de archivos, campos o incluso bloques para satisfacer las demandas de seguridad y cumplimiento de normas.
- **Seguridad de datos coherente**: habrá una necesidad evidente de contar con protección de contenido basada en políticas para satisfacer las necesidades propias de la empresa y las directivas de políticas reglamentarias. Para algunas categorías de datos, la seguridad centrada en la información necesitará encriptación en transmisión y en reposo, además de administración en la nube y en todo el ciclo de vida de los datos.



- **Clasificación eficaz de datos**: cloud computing impone un intercambio de recursos entre el alto rendimiento y los requerimientos de mayor seguridad sólida. La clasificación de los datos es una herramienta fundamental para equilibrar esa ecuación. Las empresas necesitarán saber qué datos son importantes y dónde están ubicados como requerimiento previo para tomar decisiones relacionadas con el costo/beneficio del rendimiento, además de garantizar el enfoque en las áreas más críticas para los procedimientos de prevención de pérdida de datos.
- **Administración de derechos de información**: se suele tratar a IRM como un componente de identidad, una forma de establecer controles generales sobre qué usuarios tienen acceso a los datos. No obstante, la seguridad centrada en los datos más granular requiere que las políticas y los mecanismos de control sobre el almacenamiento y el uso de información estén asociados directamente con la información en sí.
- **Buen manejo y control y cumplimiento de normas**: un requerimiento clave del buen manejo y control y el cumplimiento de normas de la información corporativa es la creación de información de administración y validación; se realiza el monitoreo y la auditoría del estado de seguridad de la información con capacidades de registro. Aquí, no solo es importante documentar el acceso y la denegación de acceso a los datos, sino también garantizar que los sistemas de TI estén configurados para cumplir con las especificaciones de seguridad y no se hayan alterado. La expansión de las políticas de retención para el cumplimiento de normas y políticas de datos también se convertirá en una capacidad esencial de la nube. Básicamente, las infraestructuras de cloud computing deben tener la capacidad de verificar que se administren los datos según las reglamentaciones locales e internacionales correspondientes (como PCI y HIPAA) con controles adecuados, recopilación de logs y creación de informes.

Los datos delicados en la nube requerirán seguridad granular, que debe mantenerse de manera consistente durante todo el ciclo de vida de los datos.

La infraestructura base para una nube debe ser inherentemente segura, ya sea una nube privada o pública, o un servicio SAAS, PAAS o IAAS.

Seguridad de la infraestructura

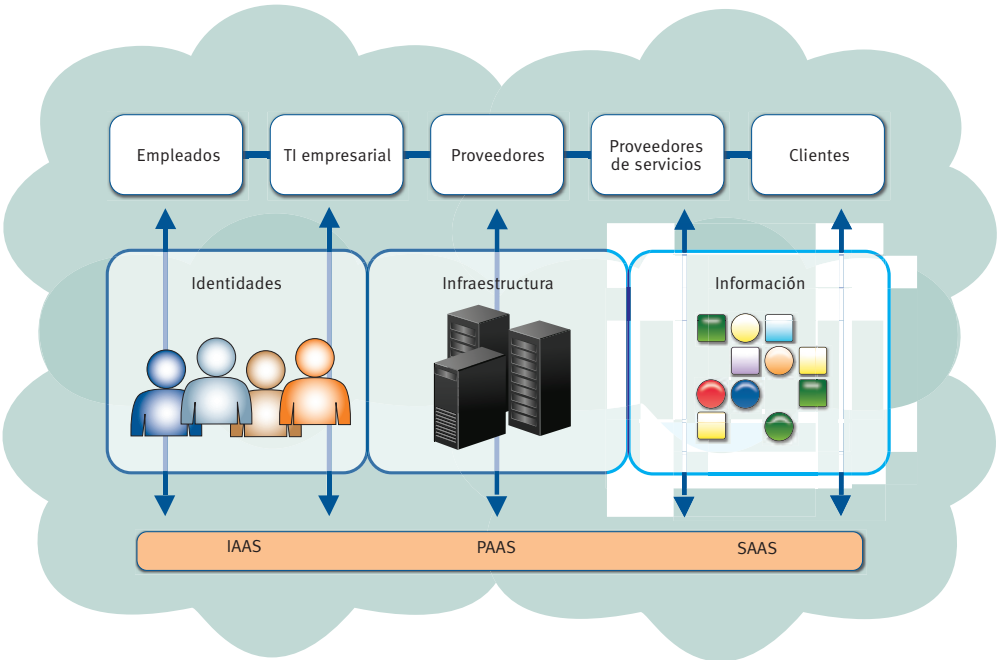
La infraestructura base para una nube debe ser inherentemente segura, ya sea una nube privada o pública, o un servicio SAAS, PAAS o IAAS. Se requerirá.

- Seguridad inherente de componentes: la nube debe estar diseñada para ser segura, creada con componentes inherentemente seguros, implementada y aprovisionada de manera segura con interfaces sólidas a otros componentes y, finalmente, soportada de manera segura con procesos de evaluación de vulnerabilidades y administración de cambios que producen información de administración y seguridades de nivel de servicio que crean confianza. Para estos componentes implementados de manera flexible, la identificación mediante la huella digital del dispositivo para garantizar la seguridad de la configuración y el estado también será un elemento de seguridad importante, al igual que lo es para los datos y las identidades en sí.
- Seguridad de interfaz más granular: los puntos en el sistema en los que se presentan intervenciones (usuario a red, servidor a aplicación) requieren políticas y controles de seguridad granulares que garanticen consistencia y responsabilidad. Aquí, el sistema end-to-end debe ser patentado, un estándar de facto o una federación de proveedores que ofrezca políticas de seguridad implementadas de manera consistente.
- Administración del ciclo de vida de los recursos: el aspecto económico de cloud computing está basado en la tenencia múltiple y en el uso compartido de recursos. A medida que las necesidades y los requerimientos de un Cliente se modifican, un proveedor de servicios debe ofrecer y desactivar esos recursos (ancho de banda, servidores, almacenamiento y seguridad) según corresponda. Este proceso del ciclo de vida debe administrarse en relación con la responsabilidad para crear confianza.

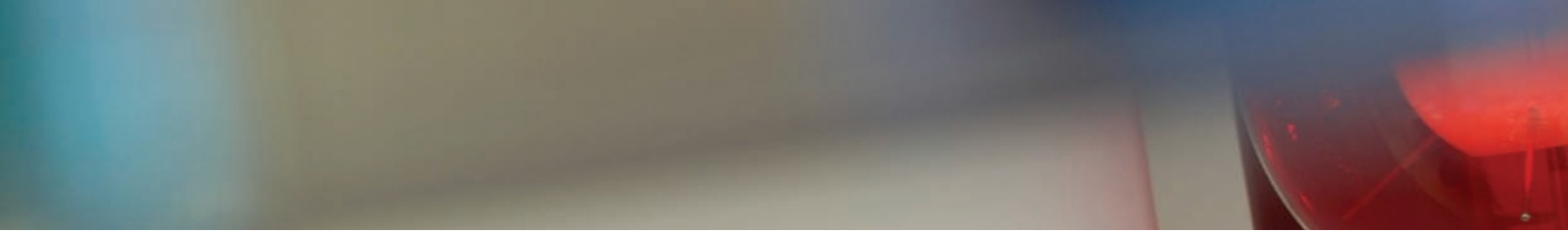
V. Conclusión

Cloud computing promete modificar la economía del data center; pero, antes de trasladar los datos delicados y reglamentados a la nube pública, se deben enfrentar los problemas de estándares de seguridad y compatibilidad, entre ellos, la autenticación sólida, la autorización delegada, la administración de claves para datos encriptados, la protección contra la pérdida de datos y la creación de informes reglamentarios. Todos estos elementos forman parte de un modelo de identidad, información e infraestructura seguro, y pueden aplicarse a nubes privadas y públicas, además de a servicios IAAS, PAAS y SAAS.

En el desarrollo de nubes públicas y privadas, las empresas y los proveedores de servicios deberán usar estos principios que sirven como guía para adoptar y ampliar de manera selectiva las herramientas de seguridad y garantizar la seguridad de los productos a fin de crear y ofrecer cloud computing y servicios confiables end-to-end. Por suerte, muchas de estas soluciones de seguridad están ampliamente disponibles hoy en día y se están desarrollando en detalle para llevar a cabo funcionalidades de nube cada vez más transparentes.



Creación de una nube confiable



EMC, RSA y cloud computing segura

Seguridad de identidades, información e infraestructuras

Para administrar las identidades en la nube, RSA aprovecha sus capacidades de autenticación sólida, la autenticación de múltiples factores, las contraseñas de un solo uso, la administración de identidades federada y las soluciones de autenticación basada en riesgos, como Authentication Manager, Federated Identity Manager, Access Manager y Adaptive Authentication. El sistema Transaction Monitoring de RSA trasciende la protección de la identidad de los usuarios que se registran mediante la autenticación de las transacciones que ejecutan para incrementar la seguridad en línea, reducir el fraude y moderar los riesgos de amenazas avanzadas. Este proceso se realiza, en gran medida, en función del servicio RSA eFraudNetwork™, una red interoganizacional de colaboración para combatir fraudes en línea dedicada a compartir y difundir información sobre actividades fraudulentas. Para administrar la autorización que toma en cuenta el contexto con privilegios detallados y la administración de autorizaciones basada en la administración central e inteligente de políticas, RSA® Entitlements Policy Manager protege los recursos aún más allá de las aplicaciones web.

Para obtener información sobre la seguridad en la nube, EMC Information Rights Manager ofrece autorización que toma en cuenta el contenido para documentos, mientras que RSA® Data Loss Prevention Suite ofrece detección que toma en cuenta el contenido, clasificación y soluciones de prevención de pérdida de datos. Juntos, estos productos brindan a las nubes públicas y privadas la posibilidad de implementar políticas de seguridad coherentes que toman en cuenta el contenido para el buen manejo y control de los datos, el control y el cumplimiento de normas. Además, RSA® Key Manager cuenta con capacidades de encriptación en la nube para la protección y el control de datos.

Finalmente, para la seguridad de la infraestructura, el amplio portafolio de productos de EMC no solo ofrece bases seguras para la virtualización, la separación de datos y las capacidades de protección y disponibilidad de datos, sino que, además, los productos de EMC se crean, se implementan y se soportan de manera segura para ofrecer mayor seguridad a las infraestructuras de nube. Los productos de administración de recursos de infraestructura de EMC combinados con el producto de análisis y administración de logs RSA enVision® permiten la administración y el control eficaces de los componentes de la infraestructura mediante la evaluación del estado, la administración de la configuración, y las funcionalidades de administración y control de eventos. Todos estos elementos son importantes para optimizar las operaciones de la nube y cumplir los requerimientos del cumplimiento de normas.

EMC y RSA están trabajando cada vez más a fin de desarrollar soluciones para la seguridad de nubes que estén diseñadas desde una perspectiva de arquitectura orientada a servicios, de modo que soporten los niveles de seguridad flexibles que los modelos de nubes emergentes requieren.

PaaS, IaaS y Saas seguros

EMC y RSA también ofrecen productos y servicios al mercado de cloud computing. Los siguientes son algunos ejemplos:

El modelo Seguridad como un servicio (SaaS) de RSA para federar los controles de seguridad en ambientes SaaS y PaaS con servicios de control de acceso y autenticación que han estado disponibles desde 2002.

RSA® Key Manager puede encargarse de la administración de los controles de seguridad de datos (claves de encriptación) de los administradores de SaaS/PaaS y mantener el control con los propietarios de datos o las corporaciones de clientes.

Atmos de EMC es un proveedor de Almacenamiento como un servicio para el modelo IaaS con políticas sobre el rendimiento y la seguridad de la distribución del almacenamiento de información.

Autor y colaboradores

Satchit Dokras, Bret Hartman, Tim Mathers, Brian Fitzgerald, Sam Curry, Magnus Nystrom, Eric Baize, Nirav Mehta

Acerca de RSA

RSA, la División de Seguridad de EMC, cuenta con expertos en seguridad centrada en la información, lo que permite proteger la información durante todo su ciclo de vida. RSA permite a los clientes asegurar de manera rentable los recursos de información importantes y las identidades en línea (en el lugar y en la etapa en que se encuentren), y administrar la información y los eventos de seguridad para aliviar la carga que impone el cumplimiento de normas.

RSA ofrece soluciones líderes en la industria de verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas y la información de seguridad, y protección contra fraudes. Estas soluciones brindan confianza respecto a millones de identidades de usuarios, a las transacciones que ejecutan y a los datos que se generan. Para obtener más información, consulte www.EMC.com (visite el sitio web de su país correspondiente) y latinamerica.rsa.com.

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

CLOUD WP 0209