cloud security alliance

Guía para la Seguridad en áreas críticas de atención en Cloud Computing

Resumen ejecutivo
Versión 2 – noviembre 2009

Realizada por los expertos de:

cloud security alliance

Traducción al castellano
coordinada y patrocinada por:

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Índice

Presentación 4

Dominio 1
Marco de la arquitectura de Cloud Computing 6

Dominio 2
Gobierno y gestión de riesgos de las empresas 12

Dominio 3
Cuestiones legales y eDiscovery.....16

Dominio 4
Cumplimiento normativo y auditorías.....18

Dominio 5
Gestión del ciclo de vida de la información.....21

Dominio 6
Portabilidad e interoperabilidad.....27

Dominio 7
Seguridad tradicional, continuidad del negocio y recuperación de catástrofes.....30

Dominio 8
Operaciones del centro de datos 32

Dominio 9
Respuesta ante incidencias, notificación y subsanación.....35

Dominio 10
Seguridad de las aplicaciones 39

Dominio 11
Cifrado y gestión de claves.....42

Dominio 12
Gestión de acceso e identidades.....45

Dominio 13
Virtualización 50

Título:
Guía para la Seguridad en áreas críticas de atención en Cloud Computing de Cloud Security Alliance (CSA)
Resumen ejecutivo. Versión 2.
Noviembre de 2009

Título original:
Security Guidance for Critical Areas of Focus in Cloud Computing V2
Executive Summary. Prepared by the Cloud Security Alliance
November 2009

Traducción al castellano coordinada y patrocinada por ISMS Forum Spain

Coordinación: Joris Vredeling, ISMS Forum Spain.
Traducción: Jaume Bellmunt Montagut.
Revisión técnica: Antonio Ramos, miembro de la Junta Directiva de ISMS Forum Spain.

CLOUD SECURITY ALLIANCE
Cloud Security Alliance en una organización sin ánimo de lucro creada para fomentar el uso de buenas prácticas, reforzar las garantías de seguridad y ofrecer formación en todo lo concerniente a Cloud Computing.

Cloud Security Alliance está formada por expertos en diversos temas de un amplio abanico de disciplinas, que se unen con los siguientes objetivos:

Fomentar un alto nivel de comprensión entre consumidores y proveedores en cloud computing, respecto a todo lo que se refiere a los requisitos y necesidades en materia de seguridad.
Fomentar la investigación independiente de las mejores prácticas en seguridad en cloud computing.
Lanzar campañas de concienciación y programas de formación sobre el uso adecuado de Cloud Computing y soluciones de seguridad en Cloud Computing.
Generar consenso en temas y orientación sobre seguridad en Cloud Computing.

Más información acerca de CSA se puede consultar a través de su página oficial:
http://www.cloudsecurityalliance.org.

Presentación

Es motivo de gran satisfacción para ISMS Forum Spain poder presentar en lengua española este amplio Resumen Ejecutivo de la **Guía para la Seguridad en áreas críticas de atención en Cloud Computing de Cloud Security Alliance (CSA)**. En la línea ya iniciada con otras publicaciones, la Asociación tiene como objetivo acercar a los profesionales de la seguridad de la información herramientas de trabajo útiles y accesibles, sin ninguna barrera idiomática que dificulte su comprensión.

Quisiera agradecer, en nombre de todos los asociados de ISMS Forum Spain, a CSA (Cloud Security Alliance), a su director Jim Reavis y a su cofundador Nils Puhlmann, por habernos autorizado cortésmente a traducir y editar en castellano la presente Obra. Es para nosotros un reconocimiento más a la labor de divulgación y fomento del conocimiento de las herramientas y Sistemas de Gestión de la Seguridad de la Información que nuestra Asociación está llevando a cabo. Seguimos, pues, consolidando la labor informativa que ISMS Forum Spain viene desarrollando desde su fundación en favor de todos sus asociados.

El presente documento es el preludio de la segunda versión de esta Guía. La primera data de abril de 2009, y el volumen de contenidos de la misma se triplicará en la segunda edición, tal es la rápida evolución de la materia que nos ocupa, y que gana terreno por momentos a otras formas de trabajo que están quedando obsoletas frente a ella. Preparada por un amplio conjunto de expertos de CSA, la guía completa está aún en fase de corrección y edición final. Así, los distintos dominios que contiene el presente resumen ejecutivo –desarrollados en profundidad- se irán publicando a lo largo de los próximos meses hasta completar un manual que tendrá más de 350 páginas. Sin embargo, esto no es un mero aperitivo, sino una herramienta de trabajo verdaderamente útil: contiene perfectamente sintetizadas las claves a tener en cuenta para comprender los principios y procesos que rigen el Cloud Computing, los modelos a los que podemos adherirnos, y sobre todo, las áreas críticas que debemos tener en cuenta y las medidas que deberíamos tomar los responsables de seguridad de la información para que nuestras organizaciones puedan trabajar “en la nube” con la máxima garantía y confianza y los mínimos riesgos posibles.

Este resumen ofrece, pues, un claro marco contextual y un conjunto de orientaciones, consejos y buenas prácticas indispensables para aquellos profesionales y empresas que están trabajando o pensando en trabajar en un futuro próximo en la modalidad de Cloud Computing. Basada en los conocimientos y en la experiencia práctica de un amplio equipo de miembros de Cloud Security Alliance, estamos seguros de que esta Guía constituirá un válido soporte para todos los profesionales de nuestro sector.

Una vez más, nos vemos reforzados en nuestro compromiso de seguir siendo un foro plural e independiente donde los profesionales de la Seguridad de la Información pueden compartir ideas y experiencias.

Gianluca D’Antonio
Presidente de ISMS Forum Spain
Noviembre de 2009

Dominio 1: Marco de la arquitectura de Cloud Computing

Este dominio, Marco de la arquitectura de cloud computing, proporciona un marco conceptual para el resto de material informativo relativo a Cloud Security Alliance. Comprender el cloud computing es fundamental para conseguir su buena utilización, y por ello éste es el apartado más extenso del resumen ejecutivo.

Los contenidos de este dominio se centrarán en una descripción de cloud computing que está específicamente concebida desde la perspectiva de los profesionales de redes informáticas y seguridad. Las siguientes áreas clave deben tenerse en cuenta dentro del Marco de la arquitectura de cloud computing:

- Definición básica: ¿Qué es el cloud computing?
- Características esenciales del cloud computing
- Modelos de servicio en la nube
- Modelos de despliegue en la nube
- Multiposesión
- Modelo de referencia de nube
- Implicaciones en la seguridad del cloud computing

¿Qué es el cloud computing?

La nube es un modelo a la carta para la asignación y el consumo de computación. La nube describe el uso de una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento. Estos componentes pueden orquestarse,

abastecerse, implementarse y desmantelarse rápidamente, y escalarse en función de las dimensiones para ofrecer unos servicios de tipo utilidad.

La CSA ha decidido asumir la definición del NIST de cloud computing (versión 15 en el momento de redactar este texto) para aportar coherencia y consenso alrededor de un idioma común que nos permita en última instancia centrarnos más en los casos prácticos que en los matices semánticos.

Características esenciales del cloud computing

Los servicios en la nube se basan en cinco características esenciales que ejemplifican sus similitudes y diferencias con las estrategias de computación tradicionales:

- **Autoservicio a la carta.** Un consumidor puede abastecerse unilateralmente de capacidades de computación, como tiempo de servidor y almacenamiento en red, según sus necesidades, de forma automática sin requerir la interacción humana con cada proveedor de servicios.
- **Amplio acceso a la red.** Las capacidades están disponibles en la red y se accede a ellas a través de mecanismos estándar que fomentan el uso por parte de plataformas de clientes heterogéneas tanto ligeras como pesadas (p.ej., teléfonos móviles, portátil y PDAs).
- **Reservas de recursos en común.** Los recursos computacionales del proveedor se ponen en reservas en común para que puedan ser utilizados por múltiples consumidores que utilicen un modelo de multiposesión, con diferentes recursos físicos y virtuales asignados dinámicamente y reasignados en función de la demanda de los consumidores. Existe un sentido de independencia de la ubicación física en que el cliente generalmente no tiene control o conocimiento sobre la ubicación exacta de los recursos suministrados, aunque se puede especificar una ubicación a un nivel más alto de abstracción (p.ej., país, región, o centro de datos). Algunos ejemplos de recursos son: almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales.
- **Rapidez y elasticidad.** Las capacidades pueden suministrarse de manera rápida y elástica, en algunos casos de manera automática, para poder realizar el redimensionado correspondiente rápidamente. Para el consumidor, las capacidades disponibles para abastecerse a menudo aparecen como ilimitadas y pueden adquirirse en cualquier cantidad y en cualquier momento.
- **Servicio supervisado.** Los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de evaluación en algún nivel de abstracción adecuado para el tipo de servicio (p.ej., almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas). El uso de recursos puede seguirse, controlarse y notificarse, lo que aporta transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Modelos de servicio en la nube

Tres modelos arquetípicos y sus combinaciones derivadas describen la prestación de los servicios en la nube. A menudo se hace referencia a los tres modelos individuales como el “Modelo SPI,” donde “SPI” hace referencia a Software, Plataforma e Infraestructura (as a Service, o como Servicio) respectivamente y se definen del siguiente modo:

- **Cloud Software as a Service (SaaS).** En el Software de nube como servicio, la capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Puede accederse a las aplicaciones desde varios dispositivos del cliente a través de una interfaz de cliente ligero como un navegador de Internet (p.ej., correo web). El consumidor no gestiona ni controla la infraestructura de nube subyacente que incluye la red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicaciones individuales, con la posible excepción de unos parámetros de configuración de la aplicación específicos del usuario limitados.
- **Cloud Platform as a Service (PaaS).** En la Plataforma de nube como servicio, la capacidad proporcionada al consumidor es desplegar en la infraestructura de nube aplicaciones adquiridas o creadas por el consumidor, que fueran creadas utilizando lenguajes y herramientas de programación soportadas por el proveedor. El consumidor no gestiona ni controla la infraestructura de nube subyacente que incluye la red, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones desplegadas y la posibilidad de controlar las configuraciones de entorno del hosting de aplicaciones.
- **Cloud Infrastructure as a Service (IaaS).** En la infraestructura de nube como servicio, la capacidad suministrada al consumidor es abastecerse de procesamiento, almacenamiento, redes y otros recursos computacionales fundamentales de forma que el consumidor pueda desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura de nube subyacente pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y la posibilidad de tener un control limitado de componentes de red seleccionados (p.ej., hospedar firewalls).

Modelos de despliegue en la nube

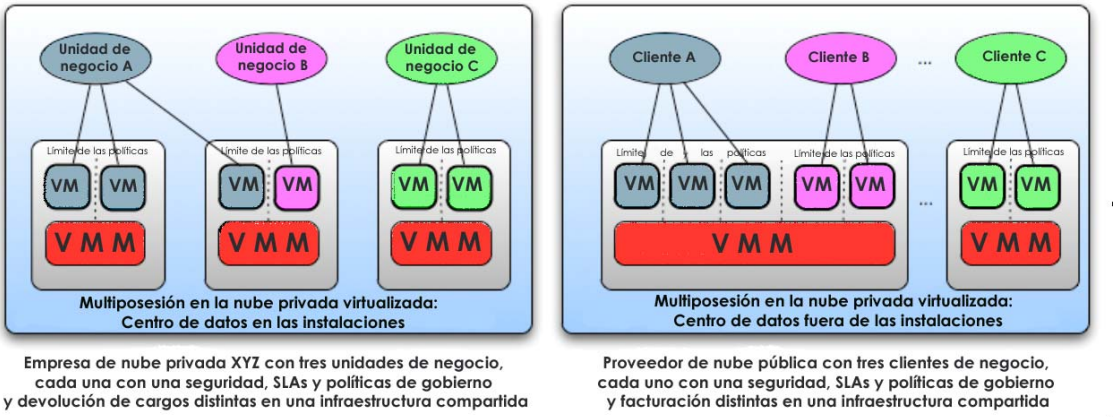
Con independencia del modelo de servicio utilizado (SaaS, PaaS, IaaS,) hay cuatro formas principales en los que se despliegan los servicios en la nube y se caracterizan con modelos de despliegue adicionales que afrontan requisitos específicos:

- **Nube pública.** La infraestructura de nube se pone a disposición del público en general o de un gran grupo industrial y es propiedad de una organización que vende los servicios en la nube.
- **Nube privada.** La infraestructura de nube se gestiona únicamente para una organización. Puede gestionarla la organización o un tercero y puede existir tanto en las instalaciones como fuera de ellas.
- **Nube híbrida.** La infraestructura de nube es una composición de dos o más nubes (privada, comunitaria o pública) que se mantienen como entidades separadas pero que están unidas por tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones (p.ej., procedimientos de escalado para el equilibrio de cargas entre nubes en el caso de picos puntuales).
- **Nube comunitaria.** La infraestructura de nube la comparten diversas organizaciones y soporta una comunidad específica que tiene preocupaciones similares (p.ej., misión, requisitos de seguridad, políticas y consideraciones sobre cumplimiento normativo). Puede ser gestionada por las organizaciones o un tercero y puede existir en las instalaciones y fuera de ellas.

Multiposesión

Aunque no es una característica esencial del cloud computing en el modelo del NIST, la CSA lo ha identificado como un elemento importante de la nube.

Desde el punto de vista del consumidor, la definición de multiposesión en los modelos de servicio en la nube implica la necesidad de permitir unos modelos de aplicación, segmentación, aislamiento, gobierno, niveles de servicio y devolución de cargos/facturación para diferentes consumidores constituyentes de servicios. Estos consumidores de servicios podrían utilizar una oferta de servicio de proveedor en la nube pública o ser de hecho de la misma organización como una unidad de negocio y no se requiere que sean entidades organizativas distintas, pero que utilicen infraestructuras compartidas.



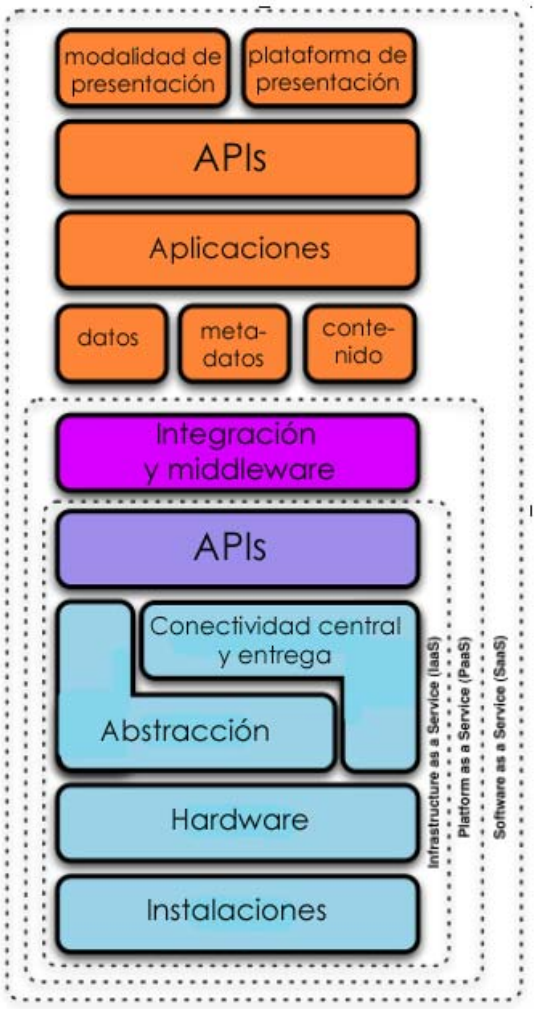
Empresa de nube privada XYZ con tres unidades de negocio, cada una con una seguridad, SLAs y políticas de gobierno y devolución de cargos distintas en una infraestructura compartida

Proveedor de nube pública con tres clientes de negocio, cada uno con una seguridad, SLAs y políticas de gobierno y facturación distintas en una infraestructura compartida

Desde el punto de vista del proveedor, la multiposesión sugiere un acercamiento arquitectónico y de diseño que permita economías de escala, disponibilidad, gestión, segmentación, aislamiento, eficacia operativa y el apalancamiento de la infraestructura compartida, datos, metadatos, servicios y aplicaciones para muchos consumidores constituyentes.

Modelo de referencia de nube

Comprender la relación y las dependencias entre los modelos de cloud computing es crucial para comprender los riesgos de seguridad del cloud computing. La IaaS es la base de todos los servicios en la nube, de modo que la PaaS se basará en la IaaS, y el SaaS, por su lado, se basará en la PaaS tal como se describe en el diagrama del marco. De este modo, a medida que se heredan capacidades, también se heredan cuestiones y riesgos relacionados con la seguridad de la información.



La IaaS incluye toda la capa de recursos de infraestructura desde las instalaciones hasta las plataformas de hardware que hay en ellas. La IaaS incorpora la capacidad de extraer recursos (o no) así como entregar conectividad física y lógica a dichos recursos. En última instancia, la IaaS proporciona un conjunto de APIs que permiten la gestión y otras formas de interacción con la infraestructura por parte del consumidor del servicio.

La PaaS se sitúa por encima de la IaaS y añade un nivel adicional de integración con los marcos de desarrollo de aplicaciones, capacidades de middleware y funciones como base de datos, mensajes y puesta en cola que permite a los desarrolladores crear aplicaciones que se agregan a la plataforma y cuyos lenguajes y herramientas de programación son soportados por la capa.

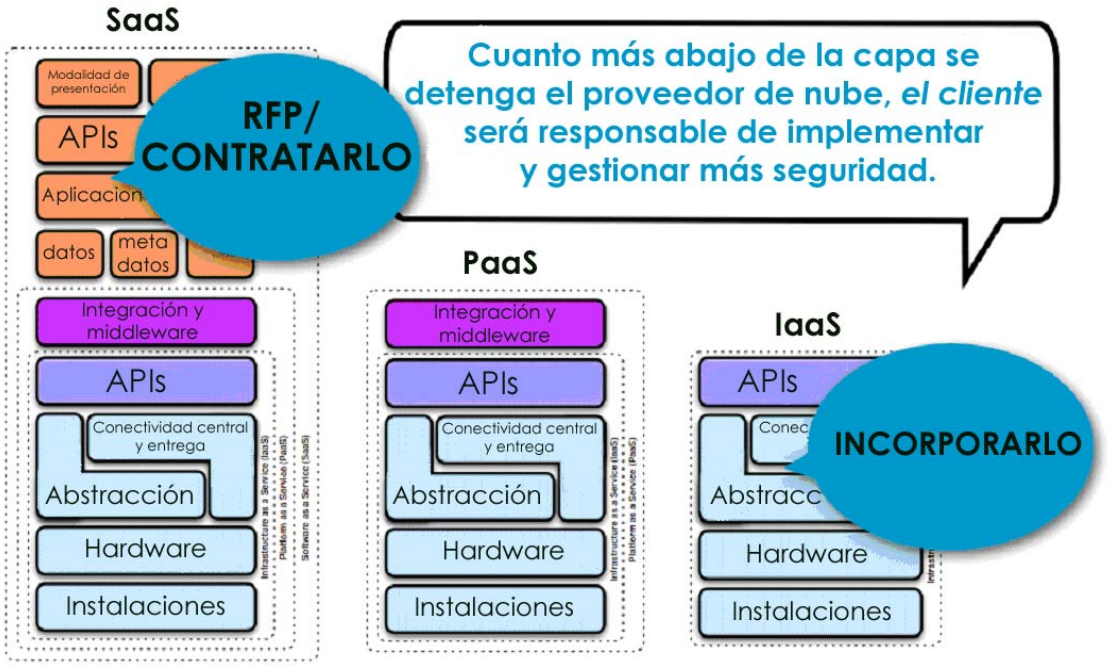
El SaaS, a su vez, se crea a partir de las capas de la IaaS y la PaaS subyacentes y proporciona un entorno operativo completo que se utiliza para proporcionar toda la experiencia del usuario que incluye el contenido, cómo se presenta, las aplicaciones y las capacidades de gestión.

Debería quedar claro, de este modo, que existen importantes elementos de decisión en cada uno de los modelos en cuanto a funciones integradas, abertura (extensibilidad) y seguridad se refiere; algunos de los elementos a tener en cuenta para cada uno los tres modelos de despliegue de nube, son:

- Por lo general, el SaaS proporciona una gran cantidad de funciones integradas incorporadas directamente a la oferta con la menor cantidad posible de extensibilidad dirigida por el consumidor y generalmente un nivel relativamente elevado de seguridad integrada (o por lo menos una responsabilidad de seguridad por parte del proveedor).
- Por otro lado, la PaaS generalmente ofrece unas funciones expuestas al consumidor menos integradas ya que está diseñada para permitir a los desarrolladores crear sus propias aplicaciones encima de la plataforma y, de este modo, es más extensible que el SaaS por naturaleza, pero debido a este equilibrio, compensa en capacidades y funciones de seguridad.
- Finalmente, la IaaS proporciona pocas funciones de tipo aplicación pero aporta una extensibilidad enorme. Esto provoca unas capacidades de seguridad y una funcionalidad generalmente menos integradas además de proteger la propia infraestructura. Este modelo requiere que los sistemas

operativos, las aplicaciones y el contenido los gestione y los obtenga el consumidor.

La idea clave desde la perspectiva de una arquitectura de seguridad al comparar los modelos es que cuanto más abajo de la capa se detenga el proveedor del servicio en la nube, más capacidades de seguridad y gestión deberá implementar y gestionar el consumidor.



Resumen

Las claves para comprender el efecto de la arquitectura de nube sobre la arquitectura de seguridad son un léxico común y conciso, junto con una taxonomía sistemática de ofertas en virtud de las cuales los servicios y la arquitectura de nube pueden deconstruirse, mapearse hasta un modelo que permita compensar seguridad y controles operativos, evaluación de riesgos y marcos de gestión y, a su vez, los estándares de cumplimiento normativo.

Comprender cómo cambian los requisitos de arquitectura, tecnología, procesos y capital humano o permanecen inalterados al desplegar los servicios de cloud computing es clave. Sin una comprensión clara de las implicaciones en la arquitectura de alto nivel de los servicios en la nube, resulta imposible afrontar cuestiones más detalladas de forma racional.

Este resumen general de la arquitectura, junto con las restantes doce áreas de atención crítica proporcionarán al lector una base sólida sobre la cual asesorarse, operar, gestionar y gobernar la seguridad en entornos de cloud computing.

Colaboradores: Glenn Brunette, Phil Cox, Carlo Espiritu, Christofer Hoff, Mike Kavis, Sitaraman Lakshminarayanan, Kathleen Lossau, Erik Peterson, Scott Matsumoto, Vern Williams, Richard Zhou.

Dominio 2: Gobierno y gestión de riesgos de las empresas

El gobierno y la gestión de riesgos efectivos en las empresas en los entornos de cloud computing son consecuencia de unos procesos de gobierno de la seguridad de la información bien desarrollados en el marco de las obligaciones de gobierno corporativo de una organización relacionadas con la atención debida. Unos procesos de seguridad de la información bien desarrollados deberían dar lugar a unos programas de gestión de la seguridad de la información escalables con el negocio, repetibles en toda la organización, mesurables, sostenibles, defendibles, en mejora continua y rentables en todo momento.

Los problemas fundamentales del gobierno y la gestión de riesgos de las empresas en el cloud computing hacen referencia a la identificación e implementación de las estructuras, procesos y controles organizativos adecuados que se requieren para mantener un gobierno de la seguridad y la información, así como una gestión de riesgos y un cumplimiento normativo efectivos. También deberían garantizar una información de seguridad efectiva en toda la cadena de suministro de la información, incluyendo a proveedores y usuarios de servicios de cloud computing y sus distribuidores terceros en cualquier modelo de despliegue de la nube dentro de un entorno de negocio definido.

Recomendaciones para el gobierno

- √ Una parte de los ahorros obtenidos por los servicios de cloud computing deben invertirse en un examen más profundo de las capacidades de seguridad del proveedor, controles de seguridad de la aplicación, y evaluaciones y auditorías detalladas constantes para garantizar que los requisitos se cumplen en todo momento.

- √ Tanto los clientes de servicios de cloud computing como los proveedores deberían desarrollar un sólido gobierno de seguridad de la información, con independencia del modelo de servicio o de despliegue. El gobierno de la seguridad de la información debería considerarse como colaborativo entre los clientes y los proveedores para alcanzar los objetivos de alineación entre la misión del negocio y el programa de seguridad de la información. El modelo de servicio puede ajustar las funciones y responsabilidades definidas en el gobierno de seguridad de la información y la gestión de riesgos (basado en el respectivo alcance de control para usuarios y proveedores), mientras el modelo de despliegue puede definir las responsabilidades y las expectativas (basado en las conclusiones de la evaluación de riesgos).

- √ Las organizaciones de usuarios deberían incluir la revisión de las estructuras y procesos de gobierno de seguridad de la información específicas dentro de su due diligence de las posibles organizaciones proveedoras. Los procesos de los proveedores deberían evaluarse para conocer la madurez de sus capacidades además de su presencia, así como la conformidad con los procesos de gestión de la seguridad de la información del usuario. Los controles de seguridad de la información del Proveedor deberían ser compatibles con estos procesos.

- √ Deberían identificarse como necesarias unas estructuras y procesos de gobierno colaborativo, en el marco del diseño y el desarrollo de la prestación

de servicios, así como unos protocolos de evaluación de riesgos del servicio y de gestión de riesgos, e incorporarlos en los contratos de servicio.

√ Los departamentos de seguridad deberían implicarse durante el establecimiento de los Contratos de Nivel de Servicios y las obligaciones contractuales, para garantizar que los requisitos de seguridad se pueden aplicar contractualmente.

√ Establecer métricas y estándares para medir los resultados y la efectividad de la gestión de la seguridad antes de trasladarse a la nube. Como mínimo, las organizaciones deberían comprender y documentar sus métricas actuales y cómo éstas cambiarán cuando se trasladen las operaciones a la nube cuando un proveedor pueda utilizar unas métricas distintas y potencialmente incompatibles.

√ Siempre que sea posible, los estándares y métricas de seguridad (especialmente las relacionadas con los requisitos legales y de cumplimiento normativo) deberían incluirse en los Contratos de Nivel de Servicio y en los acuerdos. Estos estándares y métricas deberían estar documentados y ser demostrables (auditables).

Recomendaciones de gestión de riesgos de las empresas

Como ocurre con cualquier proceso de negocio, es importante seguir las mejores prácticas para la gestión de riesgos. Las prácticas deberían ser proporcionales a tus usos particulares de los servicios en la nube, que pueden ir desde el procesamiento de datos inocuos y efímeros hasta unos procesos de negocio críticos para la misión que impliquen información muy sensible. Una discusión completa de la gestión de riesgos de las empresas y de la gestión de los riesgos de información queda fuera del alcance de este material orientativo, pero hay algunas recomendaciones específicas de la nube que puedes incorporar en tus procesos de gestión de riesgos actuales.

√ Debido a la falta de control físico sobre la infraestructura en muchos despliegues de cloud computing, los Contratos de Nivel de Servicio, los requisitos contractuales, y la documentación del proveedor desempeñan un papel más importante en la gestión de riesgos que en la infraestructura tradicional propiedad de la empresa.

√ Debido a los aspectos del abastecimiento a la carta y la multiposesión del cloud computing, las formas tradicionales de auditoría y evaluación puede que no estén disponibles, o pueden ser modificadas. Por ejemplo, algunos proveedores restringen las evaluaciones de vulnerabilidad y los testeos de penetración, mientras que otros limitan los registros de auditoría disponibles y el seguimiento de la actividad. En caso de que éstos sean requeridos por tus políticas internas, puede que debas buscar opciones de evaluación alternativas, excepciones contractuales específicas u otro proveedor que se alinee mejor con tus requisitos de gestión de riesgos.

√ La estrategia de gestión de riesgos debería incluir la identificación y valoración de activos, la identificación y el análisis de amenazas y vulnerabilidades y su impacto potencial sobre los activos (escenarios de riesgo e incidencias), análisis de la probabilidad de eventos/escenarios, niveles y criterios de aceptación aprobados por la gestión, y el desarrollo de

planes de tratamiento de riesgos con múltiples opciones (controlar, evitar, transferir, aceptar) para el tratamiento de riesgos. Los resultados de los planes de tratamiento de riesgos deberían incorporarse en los contratos de servicio.

√ Los inventarios de activos deberían incluir activos que acojan servicios en la nube y que estén bajo el control del proveedor. Los planes de valoración y clasificación de activos deberían ser acordes.

√ Las estrategias de evaluación de riesgos entre el proveedor y el usuario deberían ser sistemáticas, con unos criterios de análisis de impactos y unos criterios que definan la probabilidad de ocurrencia. El usuario y el proveedor deberían desarrollar conjuntamente escenarios de riesgo para el servicio en la nube; esto debería ser intrínseco para el diseño de servicio del proveedor para el usuario, y para la evaluación por parte del usuario de los riesgos de servicio en la nube.

√ El servicio, y no solo el distribuidor, debería ser objeto de la evaluación de riesgos. La utilización de servicios en la nube, y los modelos particulares de servicio y despliegue a utilizar deberían ir en concordancia con los objetivos de gestión de riesgos de la organización, así como con los objetivos del negocio.

√ Cuando un proveedor no pueda demostrar unos procesos de gestión de riesgos exhaustivos y eficaces en relación con sus servicios, los usuarios deberían evaluar cuidadosamente el uso del distribuidor y las propias capacidades del usuario para compensar posibles lagunas en la gestión de riesgos.

√ Los usuarios de servicios en la nube deberían preguntarse si su propia administración ha definido tolerancias al riesgo en relación con los servicios en la nube y si han aceptado los posibles riesgos residuales derivados de la utilización de los servicios en la nube.

Recomendaciones para la gestión de terceros

√ Los usuarios deberían considerar los servicios en la nube y la seguridad como cuestiones de seguridad de la cadena de suministro. Esto significa examinar y evaluar la cadena de suministro del proveedor, en la medida de lo posible. Esto también significa examinar la propia gestión de terceros del proveedor.

√ La evaluación de los proveedores de servicios terceros debería centrarse específicamente en la gestión de incidencias de los proveedores, en las políticas, procesos y procedimientos de continuidad del negocio y de recuperación de catástrofes, e incluir la revisión de las instalaciones de co-localización y back-up. Esto debería incluir la revisión de las evaluaciones internas del proveedor de la conformidad con sus propias políticas y procedimientos y la evaluación de las métricas del proveedor para proporcionar información razonable en relación con el rendimiento y la efectividad de sus controles en esas áreas.

- √ El plan de continuidad del negocio del usuario y de recuperación de catástrofes debería incluir escenarios de la pérdida de los servicios del proveedor y de la pérdida por parte del proveedor de servicios de terceros y capacidades dependientes de terceros. El testeo de esta parte del plan debería coordinarse con el proveedor de la nube.

- √ Las estructuras y procesos de gobierno de la seguridad de la información, de gestión de riesgos y cumplimiento normativo del proveedor deberían evaluarse de forma exhaustiva:

  - o Solicitar una documentación clara sobre cómo se evalúan las instalaciones y los servicios en cuanto al riesgo y cómo se auditan las debilidades de control, la frecuencia de las evaluaciones y cómo las debilidades de control se mitigan de forma oportuna.
  - o Requerir la definición de qué considera el proveedor como factores clave de éxito para la seguridad de la información y los servicios, los indicadores clave de rendimiento y cómo éstos se miden en relación con la Gestión de la Seguridad de la Información y los Servicios Informáticos.
  - o Revisar el recabado, evaluación y proceso de comunicación de los requisitos legales, normativos, sectoriales y contractuales del proveedor de forma exhaustiva.
  - o Celebrar una due diligence completa del contrato o términos de uso para determinar funciones y responsabilidades. Garantizar la revisión de la representación legal, incluyendo una evaluación de la aplicabilidad de las disposiciones de contratos locales y leyes en jurisdicciones extranjeras o de otros estados.
  - o Determinar si los requisitos de due diligence incluyen todos los aspectos relevantes de la relación del proveedor de la nube, como la situación financiera del proveedor, su reputación (p.ej., comprobación de las referencias), controles, personal clave, planes y tests de recuperación de catástrofes, seguros, capacidades de comunicaciones y uso de subcontratistas.

Colaboradores: Patrick F. Sullivan, Ph.D., Nadeem Bukhari, Donald Blumenthal, J.D.

Dominio 3: Cuestiones legales y eDiscovery

El cloud computing crea nuevas dinámicas en la relación entre una organización y su información que implican la presencia de un tercero, el proveedor de la nube. Esto crea nuevos retos a la hora de comprender las leyes que se aplican a una amplia variedad de escenarios de gestión de la información.

Un análisis completo de las cuestiones legales relacionadas con el cloud computing requiere la consideración de dimensiones funcionales, jurisdiccionales y contractuales.

- La Dimensión Funcional implica determinar cuáles de las funciones y servicios que se producen en el cloud computing crean implicaciones legales para los participantes y los grupos de interés.
- La Dimensión Jurisdiccional implica la forma en que los gobiernos administran las leyes y las normativas que afectan a los servicios de cloud computing, los grupos de interés y los activos de datos implicados.
- La Dimensión Contractual implica las estructuras, términos y condiciones de contratos y los mecanismos de aplicación a través de los cuales los grupos de interés en los entornos de cloud computing pueden afrontar y gestionar las cuestiones legales y de seguridad.

El cloud computing en general puede distinguirse de la externalización tradicional de tres formas: el momento del servicio (a la carta e intermitente), el anonimato de la identidad de los proveedores de servicio y el anonimato de la localización de los servidores implicados. Al considerar la IaaS y la PaaS específicamente, gran parte de la orquestación, configuración y desarrollo de software la lleva a cabo el cliente y mucha de la responsabilidad no puede transferirse al proveedor en la nube.

El cumplimiento de las recientes promulgaciones legislativas y administrativas en todo el mundo obliga a una mayor colaboración entre abogados y profesionales de la tecnología. Esto es especialmente cierto en el cloud computing debido al potencial de nuevas áreas de riesgos legales que crea la naturaleza distribuida de la nube en comparación con la infraestructura interna o externalizada tradicional.

Una gran cantidad de leyes y normativas de los Estados Unidos y de la Unión Europea bien imputan la responsabilidad a los subcontratistas de la nube o bien requieren a las entidades del negocio que les impongan la responsabilidad a través de un contrato.

Los tribunales actualmente se están dando cuenta de que la gestión de los servicios de la seguridad de la información son críticos a la hora de tomar decisiones en cuanto a si la información puede aceptarse como prueba. Aunque ya suponía un problema en la infraestructura informática tradicional, es una cuestión especialmente acuciante en el cloud computing debido a su falta de historial legal establecido en el caso de la nube.

Recomendaciones

√ Los clientes y proveedores de la nube deben comprender mutuamente las funciones y responsabilidades de cada uno en relación con el eDiscovery (o investigación electrónica), incluyendo actividades como la preservación de

documentos debido a litigio, búsquedas de descubrimiento, quién presta testimonio experto, etc.

- √ Se aconseja a los proveedores de la nube que se aseguren de que sus sistemas de seguridad de la información son sensibles a los requisitos de los clientes para preservar datos como auténticos y fiables, incluyendo tanto información primaria como metadatos, archivos de registro y otra información relacionada.

- √ Los datos que se encuentran bajo la custodia de los proveedores de servicios en la nube deben recibir la misma tutela que si estuvieran en manos del propietario o custodio original.

- √ Planificar la resolución tanto esperada como inesperada de la relación en las negociaciones contractuales, y una devolución metódica o enajenación segura de tus activos.

- √ La due diligence precontractual, la negociación de términos contractuales, el seguimiento postcontractual, y la resolución de contratos y la transición de la custodia de los datos forman parte del deber de diligencia requerido a un cliente de servicios en la nube.

- √ Saber dónde el proveedor de servicios en la nube hospedará los datos es un requisito previo para implementar las medidas necesarias para garantizar el cumplimiento de las leyes locales que restringen el flujo de datos transfronterizo.

- √ En calidad de custodio de los datos personales de sus empleados o clientes, y del resto de activos de propiedad intelectual de la empresa, una empresa que utilice servicios de cloud computing debería asegurarse de que mantiene la propiedad de sus datos en su formato original y autenticable.

- √ Numerosas cuestiones de seguridad, como sospechas de violación relacionada con los datos, deben tratarse en disposiciones específicas del contrato de servicio que clarifiquen los respectivos compromisos del proveedor de servicios en la nube y del cliente.

- √ El proveedor de servicios en la nube y el cliente deberían disponer de un proceso unificado para responder a citaciones, emplazamientos y otras solicitudes legales.

- √ El contrato de servicios en la nube debe permitir al cliente de los servicios en la nube o al tercero designado, realizar el seguimiento del rendimiento de los proveedores de servicio y testar las vulnerabilidades del sistema.

- √ Las partes de un contrato de servicios en la nube deberían asegurarse de que el contrato se anticipa a los problemas relacionados con la recuperación de los datos del cliente una vez finalizada su relación contractual.

Colaboradores: Jean Pawluk, Francoise Gilbert, Jeffrey Ritter, Scott Giordano, Tanya Forsheit, Peter McLaughlin, David Jackson.

Dominio 4: Cumplimiento normativo y auditorías

Con el desarrollo del cloud computing como medio viable y rentable de externalizar sistemas enteros o incluso procesos de negocio enteros, mantener el cumplimiento con tu política de seguridad y los diversos requisitos normativos y legislativos de los cuales tu organización tiene conocimiento puede ser más difícil de lograr e incluso más difícil de demostrar a los auditores y asesores.

Es justo decir que muchas de las normativas relacionadas con la informática que las organizaciones deben cumplir no se redactaron pensando en el cloud computing. Es posible que los auditores y asesores no estén familiarizados con el cloud computing en general y con un servicio en la nube en particular. Así las cosas, corresponde al cliente de la nube comprender:

- La aplicabilidad normativa de un determinado servicio en la nube.
- La división de las responsabilidades de cumplimiento normativo entre el proveedor de la nube y el cliente de la nube.
- Que la capacidad del proveedor de la nube para presentar evidencias es necesaria para el cumplimiento normativo.
- El papel del cliente de la nube a la hora de salvar las distancias entre el proveedor de la nube y el auditor/asesor.

Recomendaciones

√ Implicar a los equipos Legales y Contractuales. Los términos de servicio estándar del proveedor de la nube es posible que no cubran tus necesidades de cumplimiento, y por ello se recomienda que el personal Legal y de Contratos se implique pronto para garantizar que las disposiciones de los contratos de servicios en la nube tratan las obligaciones de cumplimiento normativo y auditoría.

√ Cláusula de derecho a auditoría. Los clientes a menudo necesitarán la capacidad de auditar al proveedor de la nube, habida cuenta de la naturaleza dinámica tanto de la nube como del entorno normativo. La cláusula contractual del derecho a auditar debería obtenerse siempre que sea posible, especialmente cuando se utiliza un proveedor en la nube para un servicio ante el cual el cliente tiene responsabilidades de cumplimiento normativo. A lo largo del tiempo, la necesidad para este derecho debería reducirse y en muchos casos sustituirse por las certificaciones de proveedor en la nube adecuadas, relacionadas con nuestra recomendación para el dimensionado del alcance de la certificación ISO 27001 que se comenta más adelante en este apartado.

√ Analizar el alcance del cumplimiento normativo. Analizar el alcance del cumplimiento normativo significa determinar si las normativas de cumplimiento a las que está sujeta la organización se verán afectadas por la utilización de servicios en la nube, para un conjunto determinado de aplicaciones y datos.

√ Analizar el impacto de las normativas en la seguridad de los datos. Los usuarios finales potenciales de los servicios de cloud computing deberían considerar qué aplicaciones y datos están considerando trasladar a los

servicios en la nube, y la medida en que están sujetas a las normativas de cumplimiento.

√ Revisar los socios y los proveedores de servicios relevantes. Se trata de un consejo general para garantizar que las relaciones con los proveedores de servicios no afectan negativamente al cumplimiento normativo. Evaluar qué proveedores de servicios están procesando datos que están sujetos a normativas de cumplimiento, y a continuación evaluar los controles de seguridad que proporciona el proveedor de servicios es fundamental. Diversas normativas de cumplimiento tienen un lenguaje específico sobre cómo evaluar y gestionar los riesgos de distribuidores terceros. Al igual que con los servicios de negocios e informática que no son de nube, las organizaciones deberán comprender cuáles de sus socios de negocio de nube están procesando datos sujetos a normativas de cumplimiento.

√ Comprender las responsabilidades contractuales de protección de datos y los contratos relacionados. El tipo de servicio en la nube en cierta medida dictará si el cliente o el proveedor de servicios en la nube es responsable de desplegar los controles de seguridad. En un escenario de despliegue de la IaaS, el cliente tiene un mayor grado de control y responsabilidad que en un escenario SaaS. Desde el punto de vista del control de la seguridad, esto significa que los clientes de la IaaS deberán desplegar muchos de los controles de seguridad que exigen los requisitos de cumplimiento normativo. En un escenario con el SaaS, el proveedor de servicios en la nube debe proporcionar los controles necesarios. Desde una perspectiva contractual, es clave comprender los requisitos específicos y garantizar que el contrato de servicios en la nube y los contratos de nivel de servicio lo cubren debidamente.

√ Analizar el impacto de las normativas sobre la infraestructura del proveedor. En el campo de las infraestructuras, trasladarse a los servicios en la nube también requerirá un análisis detenido. Algunos requisitos normativos pueden especificar controles que son difíciles o imposibles de alcanzar en un servicio en la nube, dependiendo del tipo de servicio en la nube.

√ Analizar el impacto de las normativas en las políticas y los procedimientos. Trasladar datos y aplicaciones a los servicios en la nube es probable que tenga consecuencias en las políticas y en los procedimientos. Los clientes deberían evaluar qué políticas y procedimientos relacionados con las normativas deberán cambiar. Algunos ejemplos de las políticas y procedimientos que se ven afectados incluyen los informes de actividad, el registro, la retención de datos, respuesta a incidencias, testeo de controles y políticas de privacidad.

√ Preparar evidencias sobre cómo se cumple cada requisito. Recabar evidencias del cumplimiento entre la gran cantidad de normativas y requisitos de cumplimiento supone un reto importante. Los clientes de los servicios en la nube deberían desarrollar procesos para recabar y almacenar evidencias del cumplimiento normativo, incluyendo los registros de auditoría e informes de actividad, copias de las configuraciones del sistema, informes de gestión de cambios, y otros resultados de los procedimientos de testeo. Dependiendo del tipo de servicio en la nube, el proveedor en la nube puede necesitar proporcionar mucha de esta información.

- √ Calificación y selección de auditores. En muchos casos, la organización no tiene voz en la selección de auditores o asesores de seguridad. Si una organización tiene influencia en la selección, es muy recomendable elegir a un auditor que esté familiarizado con el cloud computing, ya que es posible que muchos no conozcan los retos que presenta la nube y la virtualización. Preguntarles si conocen la nomenclatura IaaS, PaaS, y SaaS es un buen punto de partida.

- √ Proveedores en la nube con la SAS 70 Type II. Los proveedores deberían tener esta certificación de auditoría como mínimo, ya que proporcionará un punto de referencia reconocible para auditores y asesores. Habida cuenta de que la auditoría SAS 70 Type II solo garantiza que los controles se implementan tal como está documentado, es igualmente importante comprender el alcance de la auditoría SAS 70, y si dichos controles cumplen tus requisitos.

- √ Hoja de ruta ISO 27001/27002 de los proveedores en la nube. Los proveedores en la nube que tengan la intención de prestar servicios críticos para la misión deberían contar con el estándar ISO 27002 para los sistemas de gestión de la seguridad de la información. Si el proveedor no ha conseguido la certificación ISO 27001, debería demostrar la conformidad con las prácticas de la ISO 27002 y presentar una hoja de ruta para una posterior certificación.

- √ Dimensionado del alcance de la ISO 27001/27002. Cloud Security Alliance realiza un llamamiento en el sector para desarrollar los alcances recomendados para la certificación ISO 27001 para los tipos de negocio de proveedor en la nube comunes.

Colaboradores: Jim Hietala, Anton Chuvakin, Patrick Sullivan, Peter Gregory, Erick Dahan, Greg Kane.

Dominio 5: Gestión del ciclo de vida de la información

Uno de los objetivos principales de la seguridad de la información es proteger los datos fundamentales que abastecen nuestros sistemas y aplicaciones. En nuestra transición hacia el cloud computing, nuestros métodos tradicionales de obtener datos se ven superados por las arquitecturas basadas en la nube. Elasticidad, multiposesión, nuevas arquitecturas físicas, y unos controles abstraídos requieren nuevas estrategias de seguridad de datos. Con muchos despliegues de nubes también estamos transfiriendo datos a entornos externos, o incluso públicos, que hubiesen sido impensables hace solo unos años.

Gestión del ciclo de vida de la información

El Ciclo de Vida de la Seguridad de los Datos es distinto a la Gestión del Ciclo de Vida de la Información, que refleja las diferentes necesidades de los destinatarios de la seguridad. Consiste en las seis fases que se enumeran a continuación:

1. Crear
2. Almacenar
3. Utilizar
4. Compartir
5. Archivar
6. Destruir

Los retos clave que deben considerarse en relación con la seguridad del ciclo de vida de datos en la nube pueden incluir los siguientes:

Seguridad de los datos. Confidencialidad, Integridad, Disponibilidad, Autenticidad, Autorización, Autenticación y No Repudio.

Geo-localización de los datos. Debe existir una garantía de que los datos solo se almacenan en localizaciones permitidas por contrato, SLAs y/o normativas. Por ejemplo el uso de “almacenamiento que cumple las normativas” según exige la Unión Europea para almacenar registros sanitarios electrónicos puede ser una dificultad añadida para el propietario de los datos y el proveedor de servicios de la nube.

Remanencia o persistencia de datos. Los datos deben ser eliminados de manera efectiva y completa cuando se considere que son “destruidos”. En consecuencia, debe haber disponibles y deben utilizarse técnicas para localizar de forma completa y efectiva los datos en la nube, borrar/destruir datos, y asegurar que los datos han sido completamente eliminados.

Mezcla de datos con otros clientes de la nube. Los datos – especialmente los datos clasificados / sensibles – no pueden mezclarse con los datos de otros clientes durante su uso, almacenamiento o tránsito. La mezcla de los datos será una cuestión a evitar cuando surjan las preocupaciones sobre seguridad de los datos y geo-localización.

Planes de backup y recuperación de datos para la recuperación y restauración. Los datos deben estar disponibles y, de este modo, debe haber

planes efectivos de backup y recuperación de datos para la nube al objeto de evitar la pérdida de datos, la sobreescritura de datos no deseada o su destrucción.

Descubrimiento de datos. Mientras los aspectos legales continúan centrándose en el descubrimiento electrónico, los proveedores de servicios en la nubes y los propietarios de datos deberán centrarse en descubrir los datos y asegurar a las autoridades legales y normativas que todos los datos solicitados han sido recuperados. En un entorno de nube, esta cuestión es extremadamente difícil de resolver y requerirá controles administrativos, técnicos y legales.

Agregación de datos e inferencia. Con los datos en la nube, existen preocupaciones añadidas sobre la agregación e inferencia de datos que podrían provocar la violación de la confidencialidad de información sensible y confidencial. De este modo, debe disponerse de prácticas para garantizar a los propietarios de los datos y los grupos de interés que los datos siguen estando protegidos de las "violaciones" leves cuando los datos se mezclan y/o agregan, revelando de este modo información protegida (p.ej., registros médicos que contienen nombres e información médica mezclada con datos anónimos pero que contengan el mismo "campo de referencia".

Recomendaciones

- √ Comprender cómo se mantiene la integridad y que se detecte y se te transmita el compromiso de integridad en calidad de cliente. La misma recomendación es aplicable a la confidencialidad cuando corresponda.

- √ El proveedor de cloud computing debe garantizar al propietario de los datos que proporciona toda la divulgación (es decir, "transparencia") en relación con las prácticas y procedimientos de seguridad que se incluyen en los Niveles de Servicio.

- √ Garantizar que se conoce la identificación específica de todos los controles que se utilizan durante el ciclo de vida de los datos. Garantizar que hay especificaciones escritas en relación con las cuales la entidad es responsable para cada control entre el propietario de los datos y el proveedor de servicios en la nube.

- √ Mantener una filosofía fundamental de saber dónde están los datos. Determinar tu capacidad para conocer la localización geográfica del almacenamiento. Estipular esto en tu SLA y en el contrato. Formaliza esta parte de tu contrato con el proveedor de servicios en la nube y asegúrate de que se definen y se aplican los controles adecuados en relación con las restricciones de localización del país.

- √ Comprender las circunstancias en las cuales el almacenamiento puede ser embargado por un tercero o por una entidad gubernamental. Determinar tu SLA con el proveedor de la nube puede incluir una notificación anticipada al propietario de los datos (si es posible) de que la información del propietario de los datos ha sido o será embargada.

- √ En algunos casos, puede presentarse una citación o mandato de e-discovery en contra del proveedor de servicios de cloud computing. En este caso, cuando el proveedor tenga la custodia de datos del cliente, se debería

requerir al proveedor de servicios en la nube e informar al propietario de los datos de que el proveedor de servicios en la nube es obligado a revelar la información del propietario de los datos.

√ En el contrato entre el propietario de los datos y el proveedor de servicios en la nube debería incluirse un sistema de penalizaciones. De forma específica, los datos que estuvieran sujetos a las leyes de violación de datos estatales e internacionales (p.ej., la Ley del Senado de California 1386 o las nuevas normas de violación de datos de la HIPAA) deberían estar protegidas por el proveedor de servicios en la nube.

√ Es responsabilidad del propietario de los datos determinar quién debería tener acceso a los datos, cuáles deben ser sus derechos y privilegios y en qué condiciones se proporcionan estos derechos de acceso. El propietario de los datos debería aplicar una política de "Denegación por defecto" tanto para los empleados del propietario de los datos como para el proveedor de servicios en la nube.

√ Los proveedores de servicios en la nube deberían ofrecer una cláusula contractual que garantice que se niega el acceso a los datos como filosofía fundamental (es decir, "Denegación por defecto"). Esto resulta de aplicación específicamente a los empleados de Servicios en la nube y a sus clientes que no sean empleados del propietario de los datos y personal autorizado.

√ La responsabilidad del propietario de los datos es definir e identificar la clasificación de los datos. Es responsabilidad del proveedor de servicios en la nube aplicar los requisitos de acceso del propietario de los datos en función de la clasificación de los datos. Dichas responsabilidades deberían constar en el contrato y aplicarse y auditarse para el cumplimiento normativo.

√ Cuando se obliga a un cliente a revelar información, no puede producirse la contaminación de los datos. No solo el propietario de los datos debe garantizar que todos los datos solicitados para órdenes de suspensión temporal, citaciones, resoluciones de e-discovery, etc. están intactas y se revelan debidamente; sino que el propietario de los datos debe asegurarse de que no se ven afectados más datos.

√ Cifrar los datos de la nube. Cifrar los datos en estático y cifrar los datos en tránsito (Referencia Dominio 11, Cifrado y gestión de claves.)

√ Identificar los límites de la zona de confianza en toda la arquitectura informática y en todas las capas de abstracción. Garantizar que en los subsistemas solo se superan los límites de la zona de confianza cuando es necesario y con las debidas salvaguardas para evitar la divulgación, alteración o destrucción de datos no autorizada.

√ Comprender qué técnicas de compartimentación utiliza un proveedor para aislar unos clientes de otros. Un proveedor puede utilizar diversos métodos dependiendo del número y tipos de servicios ofrecidos.

√ Comprender las capacidades y limitaciones de búsqueda de datos del proveedor en la nube cuando esté intentando ver "dentro" del conjunto de datos para el descubrimiento de datos.

- √ Comprender cómo se gestiona el cifrado en el almacenamiento multiposesión. ¿Existe una sola clave para todos los propietarios de datos, una clave por propietario de datos, o múltiples claves por propietario de datos? ¿Existe un sistema para evitar que diferentes propietarios de datos tengan las mismas claves de cifrado?

- √ Los propietarios de datos deberían requerir a los proveedores de servicios en la nube garantizar que se realizan copias de seguridad de sus datos y que no se mezclen con otros datos de clientes de servicios en la nube.

- √ Comprender los procesos de retirada del almacenamiento del proveedor de la nube. La destrucción de los datos es extremadamente difícil en un entorno multiposesión y el proveedor de la nube debería utilizar un cifrado fuerte del almacenamiento que haga los datos ilegibles cuando el almacenamiento sea reciclado, enajenado, o accedido por cualquier medio distinto a las solicitudes, procesos o entidades autorizadas.

- √ Los planes de retención y destrucción de datos son responsabilidad del propietario de los datos. Es responsabilidad del proveedor del servicio en la nube destruir los datos cuando se le solicite con énfasis especial en destruir todos los datos en todas las localizaciones incluyendo los márgenes de flexibilidad de las estructuras de datos y de los medios. El propietario de los datos debería aplicar y auditar esta práctica si es posible.

- √ Comprender la segregación lógica de información y los controles protectores implementados.

- √ Comprender las restricciones de privacidad inherentes en los datos confiados a tu sociedad, ya que es posible que no se permita que esta información sea ostentada por un proveedor en la nube sin unas designaciones muy específicas de los socios.

- √ Comprender las políticas y procesos del proveedor en la nube para la retención y destrucción de datos y compararlas con la política organizativa interna. Ser consciente de que la garantía de la retención de datos puede ser más fácil de demostrar para el proveedor de la nube, pero que la destrucción de datos puede ser muy difícil.

- √ Negociar las penalizaciones a pagar por el proveedor de la nube por violaciones de datos para asegurar que se toma en serio. Si resulta práctico, el cliente debería intentar recuperar todos los costes por violaciones en el marco de su contrato del proveedor. Si no resulta práctico, el cliente debería explorar otros vehículos de transferencia de riesgos, como los seguros, para recuperar los costes de las violaciones.

- √ Llevar a cabo tests de backup y recuperación de forma periódica para asegurar que la segregación lógica y los controles son efectivos.

- √ Asegurar que se aplican los controles de personal del proveedor en la nube para proporcionar una segregación lógica de los deberes.

- √ Comprender cómo se gestiona el cifrado en el almacenamiento multiposesión. ¿Hay una sola clave para todos los clientes, una clave por cliente o múltiples claves por cliente?

Recomendaciones sobre seguridad de datos por parte de ILM Phase

Algunas de nuestras recomendaciones generales, así como otros controles específicos se enumeran dentro del contexto de cada fase del ciclo de vida. Hay que tener en cuenta que dependiendo del modelo de prestación de la nube (SaaS, PaaS, IaaS), algunas recomendaciones deberán ser implementadas por el cliente, algunas las deberá pedir el cliente al proveedor de la nube y otras no estarán disponibles.

Crear

- √ Identificar las capacidades de etiquetado y clasificación de datos disponibles
- √ La gestión de derechos digitales de empresa puede ser una opción disponible.
- √ Tagging. El tagging de datos basado en el usuario es cada vez más habitual en los entornos de Web 2.0 y puede aprovecharse para ayudar a clasificar los datos.

Almacenar

- √ Identificar los controles de acceso disponibles dentro del sistema de archivos, DBMS o sistema de gestión de documentos.
- √ Solución de cifrado, como para correo electrónico, transporte de red, base de datos, archivos y sistemas de archivos.
- √ Las herramientas de descubrimiento de contenidos pueden ayudar a identificar y auditar los datos que requieren una aplicación de controles.

Utilizar

- √ Seguimiento y aplicación de la actividad, a través de ficheros de registro y/o herramientas basadas en los agentes.
- √ Lógica de las aplicaciones.
- √ Controles de nivel de objetos dentro de las soluciones DBMS.

Compartir

- √ Seguimiento y aplicación de la actividad, a través de ficheros de registro y/o herramientas basadas en los agentes.
- √ Lógica de las aplicaciones.
- √ Controles de nivel de objetos dentro de las soluciones DBMS.

- √ Identificar los controles de acceso disponibles dentro del sistema de archivos, DBMS, sistema de gestión de documentos.
- √ Cifrado, como para correo electrónico, transporte de red, base de datos, archivos y sistemas de archivos.
- √ Las herramientas de descubrimiento de contenidos pueden ayudar a identificar y auditar los datos que requieren una aplicación de controles.

Archivar

- √ Cifrado, como en el caso de copias de seguridad en cinta y otros medios de almacenamiento a largo plazo.
- √ Gestión de activos y seguimiento.

Destruir

- √ Crypto-Shredding, la destrucción de las claves utilizadas para el cifrado de los datos.
- √ Asegurar el borrado con disk wiping y técnicas relacionadas.
- √ Destrucción física, como el desmagnetizado de soportes físicos.
- √ Descubrimiento de contenidos para confirmar los procesos de destrucción.

Colaboradores: Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna, Rich Mogull, Jeff Reich.

Dominio 6: Portabilidad e interoperabilidad

Las organizaciones deben acercarse a la nube comprendiendo que pueden tener que cambiar de proveedores en el futuro. La portabilidad y la interoperabilidad deben considerarse de entrada como parte de la gestión de riesgos y la garantía de seguridad de cualquier programa de nube.

Los grandes proveedores en la nube pueden ofrecer redundancia geográfica en la nube, y es de esperar que permitan una elevada disponibilidad con un único proveedor. Sin embargo, es aconsejable realizar una planificación básica sobre la continuidad del negocio, para ayudar a minimizar los daños, en caso de que se cumpla la peor de las previsiones. Por ejemplo, algunas empresas de repente pueden empezar a encontrarse con la urgente necesidad de cambiar de proveedores en la nube, por diversos motivos, como por ejemplo:

- Un aumento inaceptable en el coste en el momento de renovación del contrato.
- Que el proveedor cese en su actividad.
- Que el proveedor de repente cierre uno o más de los servicios en la nube que se están utilizando, sin planes de migración.
- Un descenso inaceptable en la calidad del servicio, como la incapacidad para alcanzar los requisitos clave de rendimiento o cumplir los contratos de nivel de servicio (SLAs).
- Una disputa comercial entre el cliente y el proveedor de la nube.

Algunas consideraciones simples sobre la arquitectura pueden ayudar a minimizar los daños en caso de que se produzcan este tipo de situaciones. No obstante, los medios con los que afrontar estas cuestiones dependen del tipo de servicio en la nube.

Con el Software as a Service (SaaS), el cliente de nube, por definición, sustituirá las viejas aplicaciones de software por nuevas. En consecuencia, el centro de atención no está en la portabilidad de las aplicaciones, sino en preservar o mejorar la funcionalidad de la seguridad que proporciona la aplicación heredada y alcanzar una migración de datos exitosa.

Con la Platform as a Service (PaaS), la expectativa es que se necesitará algún grado de modificación de la aplicación para alcanzar la portabilidad. La idea es minimizar la cantidad de reescritura de la aplicación a la vez que se preservan o se mejoran los controles de seguridad, un añadido para alcanzar la migración de datos con éxito.

Con la Infrastructure as a Service (IaaS), lo principal y la expectativa es que tanto las aplicaciones como los datos puedan migrarse a un nuevo proveedor en la nube.

Debido a la ausencia generalizada de estándares de interoperabilidad y a la ausencia de suficiente presión de mercado para dichos estándares, la transición entre proveedores en la nube puede ser un proceso doloroso y manual. Desde al punto de vista de la seguridad, nuestra principal preocupación es mantener unos controles de seguridad sistemáticos durante el cambio de entornos.

Recomendaciones

Para todas las soluciones de nube:

- √ Sustituir los proveedores en la nube, prácticamente en todos los casos, es una transacción comercial negativa para una parte, que puede provocar una reacción negativa inesperada en el proveedor en la nube inicial. Esto debe planificarse en el proceso contractual tal como se describe en el Dominio 3, en tu Programa de Continuidad del Negocio, como se describe en el Dominio 7, y dentro de tu Gobierno general, en el Dominio 2.

- √ Comprender el tamaño de los conjuntos de datos hospedados en un proveedor en la nube. El tamaño de los datos puede provocar una interrupción de servicio durante una transición, o que el periodo de transición sea más largo de lo esperado. Muchos clientes han descubierto que utilizar un mensajero para enviar discos duros es más rápido que la transmisión electrónica.

- √ Documentar la arquitectura y la configuración de seguridad de controles de seguridad de componentes individuales para que puedan utilizarse para apoyar las auditorías internas, además de facilitar la migración a nuevos proveedores.

Para las soluciones de nube de IaaS:

- √ Comprender cómo las imágenes de la máquina virtual pueden capturarse y portarse al nuevo proveedor en la nube.

- √ Identificar y eliminar (o por lo menos documentar) cualquier extensión específica del proveedor en el entorno de la máquina virtual.

- √ Comprender qué prácticas hay disponibles para asegurarse de que se produce el desabastecimiento adecuado de imágenes de máquina virtual después de que la aplicación se porte desde el proveedor en la nube.

- √ Comprender las prácticas utilizadas para desmantelar los discos y los dispositivos de almacenamiento.

- √ Comprender las dependencias basadas en el hardware/plataforma que deben identificarse antes de la migración de la aplicación/datos.

- √ Solicitar acceso a los registros del sistema, rastros, registros de acceso y facturación del proveedor en la nube inicial.

- √ Identificar las posibilidades de reemprender el servicio con el proveedor en la nube inicial en parte o en su totalidad si se demuestra que el nuevo servicio es inferior.

- √ Determinar si se están utilizando funciones, interfaces o APIs en el nivel de la administración que sean incompatibles o no fueran implementadas por el nuevo proveedor.

Para las soluciones de nube PaaS:

- √ Cuando sea posible, utilizar componentes de plataforma con una sintaxis estándar, APIs abiertas y estándares abiertos.
- √ Comprender qué herramientas hay disponibles para garantizar la transferencia de datos, los backups y la recuperación.
- √ Comprender y documentar los componentes y módulos de la aplicación que son específicos del proveedor de la PaaS y desarrollar una arquitectura de la aplicación con capas de abstracción para minimizar el acceso directo a módulos propietarios.
- √ Comprender cómo los servicios de base como el seguimiento, el logging o las auditorías se transferirán a un nuevo distribuidor.
- √ Comprender las funciones de control proporcionadas por el proveedor en la nube inicial y cómo se traducen al nuevo proveedor.
- √ Al migrar hacia una nueva plataforma, comprender los efectos sobre el rendimiento y la disponibilidad de la aplicación y cómo se medirán estos efectos.
- √ Comprender cómo se llevará a cabo el testeo antes y después de la migración para comprobar que los servicios o aplicaciones funcionan correctamente. Asegurar que las responsabilidades tanto del proveedor como del usuario para el testeo son conocidas y documentadas.

Para las soluciones SaaS:

- √ Llevar a cabo extracciones de datos y copias de seguridad periódicas a un formato que sea utilizable y que no sea propietario para el proveedor de SaaS.
- √ Comprender si los metadatos pueden preservarse y migrarse.
- √ Comprender que cualquier herramienta personalizada que se implemente deberá ser desarrollada de nuevo o que el nuevo distribuidor deberá proporcionar esas herramientas.
- √ Asegurar que la efectividad del control es sistemática entre los antiguos y los nuevos proveedores
- √ Asegurar la posibilidad de migración de las copias de seguridad y otras copias de registros, registros de acceso y otra información pertinente que pueda requerirse para las cuestiones legales y de cumplimiento normativo.
- √ Comprender las interfaces de gestión, seguimiento y emisión de informes y su integración entre entornos.
- √ ¿Existe una provisión para testar y evaluar las aplicaciones antes de la migración, por parte del nuevo distribuidor?

Colaboradores: Warren Axelrod, Aradhna Chetal, Arthur Hedge, Dennis Hurst, Sam Johnston, Scott Morrison, Adam Munter, Michael Sutton, Joe Wallace.

Dominio 7: Seguridad tradicional, continuidad del negocio y recuperación de catástrofes

El corpus de conocimiento acumulado dentro de la seguridad física tradicional, la planificación de continuidad del negocio y la recuperación de catástrofes sigue siendo bastante relevante para el cloud computing. El rápido ritmo de cambio y la falta de transparencia dentro del cloud computing requieren que los profesionales de seguridad tradicional, planificación de continuidad del negocio y recuperación de catástrofes se comprometan continuamente en el examen y el seguimiento de los proveedores en la nube elegidos.

Nuestro reto es colaborar en la identificación de riesgos, reconocer interdependencias, integrar y apalancar recursos de una forma dinámica y enérgica. El cloud computing y su infraestructura subyacente ayudarán en cierto modo a disminuir algunos problemas de seguridad, pero pueden aumentar otros y nunca se eliminará la necesidad de seguridad. Cuando se producen importantes cambios en los negocios y la tecnología, los principios tradicionales de seguridad deberían permanecer inalterados.

Recomendaciones

- √ Un problema importante es que la centralización de datos pueda suponer el riesgo de mal uso de información privilegiada desde dentro del proveedor en la nube.

- √ Los proveedores en la nube deberían considerar adoptar como referencia de seguridad los requisitos más estrictos de cada cliente. En la medida en que estas prácticas de seguridad no afecten negativamente a la experiencia del cliente, unas prácticas de seguridad estrictas deberían mostrarse como rentables a largo plazo al reducir el riesgo y el control dirigido por el cliente a la vez en diversos campos de preocupación.

- √ Los proveedores deberían tener una sólida compartimentación de funciones de los cargos y limitar el conocimiento de los clientes por parte de los empleados a lo que sea absolutamente necesario para desempeñar las funciones de cada cargo.

- √ Los clientes deberían realizar inspecciones de las instalaciones del proveedor en la nube siempre que sea posible.

- √ Los clientes deberían inspeccionar los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube.

- √ Los clientes deberían identificar las interdependencias físicas en la infraestructura del proveedor .

- √ Asegurarse de que hay una taxonomía autorizada incluida en los contratos para definir claramente las obligaciones contractuales relativas a la seguridad, recuperación y acceso a los datos.

- √ Los clientes deberían solicitar documentación de los controles de seguridad internos y externos del proveedor, y la adherencia a los estándares del sector.

- √ Asegurarse de que los Objetivos de Tiempo de Recuperación (RTOs, en sus siglas inglesas) del cliente se comprenden plenamente y se definen en las relaciones contractuales y se tienen en cuenta en los procesos de planificación tecnológica. Asegurarse de que la hoja de ruta tecnológica, las políticas y las capacidades operativas pueden satisfacer estos requisitos.

- √ El cliente deberá confirmar que el proveedor cuenta con una Política de Plan de Continuidad del Negocio aprobada por el Consejo de Administración del proveedor.

- √ El cliente debería buscar evidencias de un apoyo activo de la administración y la revisión periódica del Programa de Continuidad del Negocio. Su objetivo es asegurarse de que el Programa de Continuidad del Negocio está vigente.

- √ El cliente debería comprobar si el Programa de Continuidad del Negocio está certificado/mapeado para estándares internacionalmente reconocidos como el BS 25999

- √ El cliente debería determinar si el proveedor tiene recursos en línea dedicados a la seguridad y al Programa de Continuidad del Negocio en los que el resumen de los programas y las fichas descriptivas estén disponibles para su consulta.

- √ Asegurarse de que los proveedores en la nube son examinados a través del Proceso de Seguridad del Distribuidor (VSP) de la empresa para asegurar que se comprende claramente qué datos deben compartirse y qué controles deben utilizarse. El VSP debería determinar si el proceso de decisión para la evaluación de riesgos es aceptable para el negocio

- √ La naturaleza dinámica del cloud computing y su relativa juventud justifican unos ciclos más frecuentes de todas las anteriores actividades para descubrir cambios no comunicados al cliente.

Colaboradores: David, Tyson, Luis Morales, Jeff Spivey, Randolph Barr.

Dominio 8: Operaciones del centro de datos

El número de proveedores de cloud computing ha aumentado a medida que los servicios informáticas de empresas y consumidores se han traspasado a la nube. Se ha producido un crecimiento similar en los centros de datos necesarios para alimentar las ofertas de servicios de cloud computing. Proveedores de la nube de todo tipo y tamaño, incluyendo los más conocidos líderes tecnológicos y las miles de empresas de nueva creación y con crecimiento emergente, están realizando importantes inversiones en este prometedor nuevo acercamiento a la prestación de servicios informáticos.

Compartir recursos informáticos para crear eficiencias y economías de escala no es un concepto nuevo. Sin embargo, el modelo de negocio de la nube funciona mejor si las tradicionalmente enormes inversiones en las operaciones de centro de datos se extienden sobre un grupo más grande de consumidores. Históricamente, las arquitecturas de los centros de datos han tenido un tamaño deliberadamente más grande de lo necesario para acoger periódicamente cargas de trabajo más grandes, lo que significa que en los periodos con una demanda normal o baja, los recursos de los centros de datos a menudo están parados o desaprovechados durante largos periodos de tiempo. Los proveedores de servicios en la nube, por otro lado, buscan optimizar el uso de recursos, tanto humanos como tecnológicos, para obtener ventajas competitivas y maximizar los márgenes de beneficio operativo.

El reto para el consumidor de servicios en la nube es cómo evaluar mejor las capacidades del proveedor para prestar unos servicios apropiados y rentables, a la vez que se protegen los datos e intereses del cliente. No debe darse por sentado que el proveedor necesariamente tiene los mejores intereses de sus clientes como máxima prioridad. Con el modelo de portador habitual en la prestación de servicios, del que el cloud computing es una forma, el proveedor de servicios normalmente tiene muy poco o ningún acceso o control sobre los datos o sistemas de los clientes más allá del nivel contratado de gestión. Sin duda, éste es el acercamiento correcto, pero algunas de las arquitecturas de nube podrían tomarse algunas libertades con la integridad y la seguridad de los datos de los clientes con las que el cliente podría no sentirse cómodo si las conociera. Los consumidores deben informarse bien sobre los servicios que estén considerando, haciendo las preguntas adecuadas y familiarizándose con las arquitecturas básicas y las áreas potenciales para las vulnerabilidades de seguridad.

Al tomar una decisión para trasladar parte o la totalidad de las operaciones informáticas a la nube, en primer lugar, ayuda comprender cómo el proveedor de la nube ha implementado las “Cinco principales características del cloud computing” del Dominio 1, y cómo esa arquitectura e infraestructura tecnológicas afectan a su capacidad para cumplir los contratos de nivel de servicio y cualquier cuestión relacionada con la seguridad. La arquitectura tecnológica específica del proveedor podría ser una combinación de productos informáticos y otros servicios en la nube, como aprovechar los servicios de almacenamiento de la IaaS de otro proveedor.

Mientras la arquitectura tecnológica y la infraestructura de los proveedores en la nube pueden ser diferentes, para cumplir los requisitos de seguridad, todas deben poder demostrar una amplia compartimentación de sistemas, datos, redes, gestión, aprovisionamiento y personal. Los controles que separan cada capa de la infraestructura deben integrarse debidamente, de modo que no interfieran

mutuamente. Por ejemplo, debe comprobarse si la compartimentación del almacenamiento puede superarse con las herramientas de gestión o debido a una mala gestión de las claves.

En último lugar, debe comprenderse cómo el proveedor de la nube gestiona la democratización de recursos y el dinamismo para poder predecir los niveles adecuados de disponibilidad del sistema y el rendimiento con las fluctuaciones normales del negocio. Debe recordarse que la teoría del cloud computing todavía supera en cierto modo su práctica, por lo que muchos clientes realizan asunciones incorrectas acerca del nivel de automatización con que en realidad cuentan los sistemas. A medida que se agota la capacidad de recursos suministrada, el proveedor es responsable de asegurar que se entregan al cliente los recursos adicionales necesarios.

Recomendaciones

Es imperativo que una organización que esté considerando adquirir servicios en la nube de cualquier tipo, sea totalmente consciente de qué servicios se están contratando exactamente y qué no se incluye en el servicio. A continuación se incluye un resumen de la información que debe revisarse dentro del proceso de selección del distribuidor y las preguntas adicionales que ayuden a calificar a los proveedores y ajustar mejor sus servicios a los requisitos organizativos.

Las Políticas de Gestión del Proveedor deberían permitir a una organización hacer frente a las siguientes preocupaciones:

- √ Una clara comprensión de los contratos, acuerdos, términos y condiciones del proveedor.
- √ Comprender los contratos secundarios o predecesores (upstream) del proveedor que puedan afectar a la relación.
- √ Tiempos de entrega de sistemas y servicios y Acuerdos de Nivel de Servicios (SLAs).
- √ Cualquier SLA para los componentes o servicios de proveedores de la nube predecesores.
- √ Procesos operativos alrededor de la adquisición de sistemas y servicios.
- √ Informes sobre el rendimiento del proveedor y análisis.
- √ Métodos para contactar con el personal adecuado en las organizaciones de los proveedores.

Conciencia y formación

Resultará difícil valorar el programa formativo de un proveedor, especialmente en lo que respecta a la conciencia sobre la seguridad. Como mínimo, el proveedor debería atestiguar que:

- √ Lleva a cabo formación sobre conciencia de seguridad para todos los empleados por lo menos una vez al año.
- √ Lleva a cabo formación sobre conciencia para el personal de Operaciones (los encargados de mantener el entorno) por lo menos una vez al trimestre.
- √ Todos los nuevos empleados reciben formación sobre conciencia de seguridad durante su proceso de integración, y antes de que se les dé acceso a los entornos operativos.

Comprender la implementación de las características de la nube según el NIST

- √ ¿Cómo se implementa la abstracción de la infraestructura (NIST: puesta en común de recursos)?
- √ ¿Cómo se implementa la democratización de recursos (NIST: servicio supervisado)?
- √ ¿Cómo se implementan las arquitecturas orientadas al servicio (NIST: amplio acceso a la red)?
- √ ¿Cómo se implementa la elasticidad/dinamismo de recursos (NIST: rapidez y elasticidad)?
- √ ¿Cómo se implementa el modelo de consumo y la asignación de utilidades (NIST: autoservicio a la carta)?

Certificación y acreditación

- √ ¿Qué certificaciones o acreditaciones posee en la actualidad y cuándo fueron obtenidas? ¿Hay documentación acreditativa disponible para la revisión de dichas certificaciones?
- √ ¿Cada cuánto se realizan auditorías (internas) antes de las recertificaciones requeridas?
- √ ¿Pueden los clientes o sus equipos independientes designados auditar las operaciones del centro de datos?

Conocer las prácticas y estrategias de gestión de disponibilidad y capacidad.

Comprender cómo los SLAs con proveedores predecesores o sucesores (upstream/downstream) afectan a los SLAs con los clientes, como las responsabilidades de exclusiones y transferencias.

Gestión de la configuración/cambios

- √ Aprender los procedimientos de gestión de cambios y configuración.
- √ Identificar los controles disponibles para identificar elementos anómalos de configuración, o cambios no autorizados.
- √ Comprender el proceso de gestión de parches.
- √ Comprender el proceso de mantenimiento programado.
- √ Comprender el ciclo de vida y la estrategia de desarrollo del software (muy relevante para el SaaS).

Colaboradores: Jeff Reich, Wing Ko, John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Hadass Harel, Beau Monday, Lee Newcombe, Tajeshwar Singh, Alexander Windel, Richard Zhao, David Lingenfelter.

Dominio 9: Respuesta ante incidencias, notificación y subsanación

A los efectos de la discusión de la respuesta ante incidencias, su notificación y subsanación, el cloud computing se puede definir como un conjunto de aplicaciones y servicios que gestionan datos que son propiedad de un cliente y que hospeda un proveedor de servicios. Este cambio del modelo tradicional, en el que una organización asume toda la responsabilidad, a un modelo compartido, hace que sea mucho más difícil determinar con quién debe contactarse en caso de que se produzca una incidencia de seguridad, una violación de los datos o cualquier otro evento que requiera una investigación y posteriores medidas. Los mecanismos de respuesta a las incidencias de seguridad estándar pueden utilizarse con modificaciones para acoger los cambios que exigen unas responsabilidades de notificación compartidas. Este dominio proporcionará orientación sobre cómo gestionar mejor estas incidencias.

El problema para el cliente de la nube es que las aplicaciones desplegadas en los tejidos de nube no siempre están diseñadas pensando en la integridad de los datos y en la seguridad. Esto puede provocar que se desplieguen aplicaciones vulnerables en los entornos de nube y dar lugar a incidencias de seguridad. Asimismo, cualquier fleco en la arquitectura de la infraestructura, errores cometidos durante los procesos de refuerzo de la seguridad, y simples descuidos presentan riesgos importantes para una operación de nube. Por supuesto, unas vulnerabilidades de este tipo también ponen en peligro las operaciones de los centros de datos tradicionales.

Evidentemente, para la gestión de las incidencias se requieren conocimientos técnicos, pero los expertos en privacidad y legales tienen mucho que aportar a la seguridad de la nube. También desempeñan un papel importante en las respuestas a incidencias en relación con la notificación, subsanación y las posibles medidas legales posteriores. Una organización que esté considerando el uso de servicios en la nube debe revisar qué mecanismos se han implementado para hacer frente a cuestiones sobre acceso de datos por parte de los empleados que no estén regidas por contratos de usuario y políticas de privacidad. Los datos de la aplicación no gestionados por la propia aplicación de un proveedor en la nube, tal como ocurre en las arquitecturas de IaaS o PaaS, por lo general tendrán diferentes controles que los datos gestionados por una aplicación de proveedor de SaaS.

Las complejidades derivadas de que grandes proveedores de la nube proporcionen capacidades de SaaS, PaaS y IaaS crean importantes problemas de respuesta a las incidencias que un cliente potencial debe conocer para alcanzar unos niveles de servicio aceptables. A la hora de evaluar a los proveedores es importante ser consciente de que el proveedor puede estar hospedando cientos de miles de aplicaciones distintas. Desde una perspectiva del seguimiento de incidencias, cualquier aplicación externa amplía la responsabilidad de la funcionalidad del Centro de Operaciones de Seguridad (SOC, en sus siglas inglesas). Normalmente, un SOC controla las alertas y otros indicadores de incidencias, como los que generan los sistemas de detección de intrusiones y los firewalls, pero el número de fuentes que deben controlarse y el volumen de notificaciones puede aumentar de manera exponencial en el entorno de nube abierta, puesto que el SOC puede necesitar controlar actividad entre clientes, así como incidencias externas.

Una organización deberá comprender la estrategia de respuesta a las incidencias del proveedor de la nube que elija. Esta estrategia deberá tratar las cuestiones de la identificación y la notificación, y las opciones para la subsanación de acceso no autorizado a los datos de las aplicaciones. Para complicar aún más las cosas, la gestión y acceso a los datos de aplicaciones tienen diferentes significados y requisitos normativos en función de la ubicación de los datos. Por ejemplo, puede generarse una incidencia relacionada con datos en Alemania, de forma tal que si los datos se hubiesen almacenado en los EE UU, podrían no haberse considerado como un problema. Esta complicación hace que la identificación de incidencias suponga un reto especialmente grande.

Recomendaciones

Miembros y composición del CSIRT

Con independencia de si el cliente pudiese o se le permitiera apoyar las actividades de respuesta a las incidencias, el CSIRT (Equipo de Respuesta a Incidencias sobre Seguridad Informática) mixto debería contar con un personal que disponga de las siguientes habilidades y los siguientes cargos:

- √ Un líder de respuesta a las incidencias que comprenda todos los aspectos de las actividades de respuesta a las incidencias.
- √ Uno o más expertos en la materia (SMEs, en sus siglas inglesas) que puedan analizar, compilar datos y hablar con autoridad sobre los elementos de red, como conmutadores de red, routers, firewalls, y sistemas de detección de intrusión de redes.
- √ Uno o más SMEs que puedan analizar, reunir datos y hablar con autoridad de los elementos del host o del servidor.
- √ Uno o más SMEs que puedan analizar, reunir datos y hablar con autoridad de los controles de seguridad desplegados.
- √ Uno o más SMEs forenses.
- √ Un representante del equipo legal.
- √ Un representante del equipo de marketing y/o relaciones públicas.

Autoridad del CSIRT en un paradigma de nube

De forma ideal, el equipo de respuesta a las incidencias del cliente debería tener la autoridad necesaria en cuanto a todos sus recursos contratados para:

- √ Cerrar una aplicación individual, incluso si ello provoca la degradación de un servicio o un corte dentro de su propio entorno.
- √ Retirar hosts individuales de la red, incluso si ello provoca la degradación del servicio o un corte dentro de su propio entorno, reconociendo que los hosts a menudo serán virtualizados.
- √ Aislar partes de la red, incluso si ello provoca la degradación del servicio o un corte dentro del propio entorno. La red también puede ser virtualizada.
- √ Realizar cambios en los controles de seguridad, como las bases de las normas de firewalls e IDS/IPS dentro de su propio entorno.
- √ Solicitar y recibir todos los registros pertinentes y otros datos forenses disponibles.
- √ Tener plena autoridad para acelerar los cambios en el entorno, como parches para sistemas operativos u otras mitigaciones, en lugar de tener una junta de revisión de cambios de emergencia (a menudo los miembros de un CSIRT también forman parte de la junta de revisión de cambios, y obtener dicha aprobación es un requisito).

- √ Comunicar el estado a las unidades de negocio internas.
- √ Identificar y comunicar el estado a los clientes afectados, si los hubiere.

Trabajar con el CSIRT del Proveedor

De forma ideal, el equipo de respuesta a las incidencias de clientes debería tener la autoridad necesaria con todos sus recursos contratados para:

- √ Cerrar una aplicación individual, incluso si ello provoca la degradación de un servicio o un corte dentro de su propio entorno.
- √ Retirar hosts individuales de la red, incluso si ello provoca la degradación del servicio o un corte dentro de su propio entorno.
- √ Aislar partes de la red, incluso si ello provoca la degradación del servicio o un corte dentro del propio entorno. La red también puede ser virtualizada.
- √ Realizar cambios en los controles de seguridad, como las bases de las normas de firewalls e IDS/IPS dentro de su propio entorno.
- √ Solicitar y recibir todos los registros pertinentes y otros datos forenses disponibles.
- √ Tener plena autoridad para acelerar los cambios en el entorno, como parches para sistemas operativos u otras mitigaciones, en lugar de tener una junta de revisión de cambios de emergencia (a menudo los miembros de un CSIRT también forman parte de la junta de revisión de cambios, y obtener dicha aprobación es un requisito).
- √ Comunicar el estado a las unidades de negocio internas.
- √ Identificar y comunicar el estado a los clientes afectados, si los hubiere.

Contención, erradicación y recuperación de incidencias

- √ Cualquier organización que esté considerando una opción de nube debe asegurarse de que el proveedor en la nube puede albergar almacenamiento de archivo a largo plazo y está dispuesto a testar su recuperación por lo menos una vez al año. También deberían asegurarse de que los contratos de servicio incluyen o facilitan la capacidad para el cliente de declarar que se requiere una subsanación.
- √ Debe tenerse en cuenta que los servicios de subsanación del proveedor que no sean legalmente obligatorios pueden suponer un coste adicional para el consumidor de la nube.
- √ Debe disponerse de un proceso post incidencias bien definido para las “lecciones aprendidas”.

Arquitectura para minimizar incidencias amplias

- √ Cualquier dato clasificado como privado a los efectos de las normativas de violación de datos siempre debería ser cifrado para reducir las consecuencias de una incidencia relacionada con dichas violaciones. El cliente debería estipular por contrato unos requisitos de cifrado (algoritmos, longitud de la clave y gestión de claves, como mínimo).

- √ Los proveedores de la nube necesitan unos marcos de registro de las capas de las aplicaciones para proporcionar la reducción granular de incidencias a un cliente específico.

- √ Los proveedores de la nube deberían crear un registro de propietarios de aplicaciones por interfaz de aplicaciones (URL, servicio SOA, etc.)

- √ Los firewalls de nivel de aplicaciones, proxies y otras herramientas de registro de aplicaciones son capacidades clave que se encuentran disponibles en la actualidad para ayudar a responder a incidencias en entornos multiposesión.

Colaboradores: Jeff Reich, Wing Ko, John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Hadass Harel, Beau Monday, Lee Newcombe, Tajeshwar Singh, Alexander Windel, Richard Zhao, David Lingenfelter.

Dominio 10: Seguridad de las aplicaciones

Los entornos de nube, debido a su flexibilidad abertura y a menudo su disponibilidad pública, suponen un reto para muchas asunciones fundamentales sobre la seguridad de las aplicaciones. Algunas de estas asunciones se sobreentienden; sin embargo, en muchos otros casos no es así. Este apartado tiene por objetivo documentar cómo el cloud computing influye en la seguridad a lo largo de la vida útil de una aplicación (desde el diseño, pasando por las operaciones hasta el desmantelamiento). Esta información es para todos los grupos de interés, que incluyen diseñadores de aplicaciones, profesionales de seguridad, personal de operaciones y gestión técnica sobre cómo mitigar mejor los riesgos y gestionar las garantías dentro de las aplicaciones de cloud computing.

El cloud computing es un reto especial para las aplicaciones en todas las capas del Software como servicio (SaaS), de la Plataforma como servicio (PaaS) y de la Infraestructura como servicio (IaaS). Las aplicaciones basadas en el software de nube requieren un rigor en el diseño similar a las aplicaciones que residen en una Zona de Gestión de Datos (DMZ, en sus siglas inglesas) clásica. Esto incluye un análisis inicial en profundidad que cubra todos los aspectos tradicionales de gestionar la confidencialidad de la información, la integridad y la disponibilidad.

Las aplicaciones en los entornos de nube afectarán y a la vez se verán afectadas por las siguientes grandes categorías:

- **Arquitectura de seguridad de la aplicación** – Debe tenerse en cuenta que la realidad de la mayoría de aplicaciones tiene dependencias en diversos otros sistemas. Con el cloud computing, las dependencias de las aplicaciones pueden ser muy dinámicas, incluso hasta el punto en el que cada dependencia represente un proveedor de servicios tercero individual. Las características de la nube hacen que la gestión de la configuración y el suministro continuado sean sensiblemente más complejas que con el despliegue de aplicaciones tradicional. Este entorno genera la necesidad de realizar modificaciones en la arquitectura para garantizar la seguridad de la aplicación.

- **Ciclo de vida del desarrollo de software (SDLC, en sus siglas inglesas)** – la nube afecta a todos los aspectos del SDLC, desde la arquitectura de la aplicación, su diseño, desarrollo, garantía de calidad, documentación, despliegue, gestión, mantenimiento y desmantelamiento.

- **Cumplimiento normativo** – El cumplimiento normativo afecta claramente a los datos, pero también influye a las aplicaciones (por ejemplo, regulando cómo una programa implementa funciones criptográficas particulares), plataformas (por ejemplo, prescribiendo controles y parámetros de los sistemas operativos) y procesos (como los requisitos de generación de informes para las incidencias de seguridad).

- **Herramientas y servicios** – La nube introduce una serie de nuevos retos alrededor de las herramientas y servicios que deben crearse y mantenerse al ejecutar aplicaciones. Entre éstas están las herramientas de desarrollo y de prueba, las utilidades de gestión de aplicaciones, la conexión con servicios externos, y las dependencias en servicios de sistemas operativos y

bibliotecas, que puedan originarse desde los proveedores de la nube. Comprender las repercusiones de quién proporciona, posee, opera, y asume la responsabilidad para cada una de éstas es una cuestión fundamental.

- **Vulnerabilidades** – Éstas incluyen no solo las vulnerabilidades bien documentadas (y en constante evolución) asociadas a las aplicaciones web, sino también las vulnerabilidades asociadas a las aplicaciones máquina a máquina de las Arquitecturas Orientadas al Servicio (SOA, en sus siglas inglesas), que cada vez registran un mayor despliegue en la nube.

Recomendaciones

- La seguridad del Ciclo de Vida del Desarrollo del Software (SDLC, en sus siglas inglesas) es importante, y en los niveles altos del desarrollo basado en la nube debería afrontar las siguientes tres áreas principales de diferenciación: 1) Modelos actualizados de amenazas y confianza, 2) Herramientas de evaluación de aplicaciones actualizadas para los entornos de nube y, 3) Procesos de SDLC y controles de calidad que den cuenta de los cambios en la arquitectura de seguridad de la aplicación.

- La IaaS, la PaaS y el SaaS crean unos límites de confianza distintos para el ciclo de vida del software, que debe tenerse en cuenta durante el desarrollo, prueba y despliegue de producción de las aplicaciones.

- Para la IaaS, el factor clave de éxito es la presencia de unas imágenes de la máquina virtual fiables. La mejor alternativa es la capacidad de proporcionar la propia imagen de máquina virtual de conformidad con las políticas internas.

- Las mejores prácticas disponibles para reforzar la seguridad de los sistemas host dentro de la DMZ deberían aplicarse a máquinas virtuales. Resulta adecuado limitar los servicios disponibles solo a los necesarios para soportar la capa de la aplicación.

- Asegurar las comunicaciones inter-host tiene que ser la norma, aunque no puede haber ninguna asunción con respecto a un canal seguro entre hosts, ya sea presente en un centro de datos común o incluso en la misma plataforma de hardware.

- Gestionar y proteger las “claves secretas” de la aplicación es esencial.

- Debería tenerse especial cuidado en la gestión de archivos utilizados para el registro y la depuración de aplicaciones, ya que la ubicación de estos archivos puede ser remota o desconocida y la información podría ser sensible.

- Hay que tener en cuenta la Administración Externa y la Multiposesión en el modelo de amenazas de la Aplicación.

- Asegurar los mensajes en el Bus de Servicios Empresariales (ESB, en sus siglas inglesas) con un protocolo como el WS-Security se convierte en responsabilidad de la aplicación, puesto que la capacidad para segmentar los ESBs no está disponible en entornos PaaS.

- Las métricas deberían aplicarse para evaluar la efectividad de los programas de seguridad de las aplicaciones. Entre las métricas específicas de seguridad de aplicaciones directas disponibles están el scoring de vulnerabilidad y la cobertura con parches. Estas métricas pueden indicar la calidad de la codificación de las aplicaciones. Las métricas de gestión de datos indirectos, como el porcentaje de datos cifrados, puede indicar que las decisiones responsables se están tomando desde una perspectiva de arquitectura de aplicaciones.

- Los proveedores de la nube deben disponer de la capacidad para herramientas de análisis dinámico de seguridad para aplicaciones web a utilizar con aplicaciones hospedadas en su entorno.

- Debería prestarse atención a considerar cómo los actores malintencionados reaccionarán ante nuevas arquitecturas de aplicaciones de nube que oculten los componentes de las aplicaciones a su escrutinio. Es probable que los hackers ataquen el código visible, incluyendo, de forma no exhaustiva, el código que se ejecute en el contexto del usuario. También es probable que ataquen la infraestructura y realicen exhaustivas pruebas de las cajas negras.

- Los usuarios deberían obtener un permiso por contrato para llevar a cabo evaluaciones de vulnerabilidad remotas, incluyendo evaluaciones tradicionales (red/host), y evaluaciones de vulnerabilidad de aplicaciones. Muchos proveedores limitan sus evaluaciones de vulnerabilidad debido a la incapacidad del proveedor de distinguir estas pruebas de ataques reales.

Colaboradores: Scott Matsumoto, Dennis Hurst, Michael Sutton, Warren Axelrod, Joe Stein, Aradhna Chetal, Scott Morrison, James Tiller, Georg Hess, Colin Watson, Joe Wallace, Jesus Luna Garcia, Arthur J.Hedge III, John Arnold, Anish Mohammed, Alexander Meisel.

Dominio 11: Cifrado y gestión de claves

Los clientes y proveedores de la nube deben tomar medidas para evitar la pérdida y el robo de datos. Actualmente, se recomienda encarecidamente el cifrado de datos personales y de empresas y, en algunos casos, es obligado por diversas leyes y normativas en todo el mundo. A los clientes de la nube les conviene que sus proveedores cifren sus datos para asegurarse de que están protegidos con independencia de dónde se ubican físicamente los datos. Del mismo modo, el proveedor de la nube debe proteger los datos sensibles de sus clientes por motivos análogos.

Un cifrado fuerte con gestión de claves es uno de los mecanismos centrales que los sistemas de cloud computing deberían utilizar para proteger los datos. Aunque el cifrado por si solo no evita necesariamente la pérdida de datos, las disposiciones de puerto seguro de las leyes y normativas no consideran los datos cifrados perdidos como perdidos en modo alguno. El cifrado proporciona protección de recursos mientras que la gestión de claves permite el acceso a estos recursos.

Cifrado para la confidencialidad y la integridad

Los entornos de nube se comparten con muchos poseedores y los proveedores de servicios han privilegiado el acceso a los datos en esos entornos. De este modo, los datos confidenciales hospedados en una nube deben protegerse utilizando una combinación de control de acceso (ver Dominio 12), responsabilidad contractual (ver Dominios 2, 3 y 4), y cifrado, que describimos en este apartado. Entre éstas opciones, el cifrado tiene la ventaja de que proporciona una dependencia mínima con el proveedor de servicios de la nube y no depende de detectar fallos operativos.

Cifrado de datos en tránsito por las redes. Existe la imperiosa necesidad de cifrar las credenciales multiuso, como los números de tarjeta de crédito, contraseñas y claves privadas, que se encuentran en tránsito por Internet. Aunque las redes del proveedor de la nube pueden ser más seguras que la Internet abierta, por su propia arquitectura, están hechas de muchos componentes diferentes y hay muchas organizaciones distintas que comparten la nube. En consecuencia, es importante proteger esta información sensible y regulada cuando los datos se encuentren en tránsito incluso dentro de la red del proveedor de la nube. Normalmente, esto puede implementarse con la misma facilidad en los entornos SaaS, PaaS e IaaS.

Cifrado de datos estáticos. Cifrar los datos en un disco o en una base de datos con producción activa tiene su valor, ya que puede proteger contra un proveedor de servicios en la nube malintencionado o un coposeedor malintencionado así como contra algunos tipos de abuso de aplicaciones si el cliente ha utilizado el cifrado para proteger los datos. Para un archivo a largo plazo, algunos clientes pueden cifrar sus propios datos y enviarlos en forma de texto cifrado a un distribuidor de almacenamiento de datos de nube. El cliente, entones, controla y mantiene las claves criptográficas y descifra de nuevo los datos en sus propias instalaciones. El cifrado de datos estáticos suele ser un proceso habitual dentro de los entornos IaaS utilizando una serie de herramientas del proveedor o de un tercero. Cifrar datos estáticos dentro de entornos PaaS suele ser más complicado, ya que requiere la instrumentación de ofertas del proveedor o personalizaciones especiales. Cifrar datos estáticos dentro de los entornos SaaS es una característica que los clientes de la nube no pueden implementar y deberán solicitarlo a su proveedor.

Cifrado de datos en soportes de backup. Esto puede proteger contra el mal uso de soportes perdidos o robados. De forma ideal, el proveedor del servicio en la nube lo implementa de forma transparente. Sin embargo, como cliente y proveedor de datos es tu responsabilidad comprobar que se produce dicho cifrado. Una de las consideraciones de la infraestructura de cifrado incluye tratar con la longevidad de los datos.

Más allá de estos usos habituales del cifrado, la posibilidad de ataques exóticos contra los proveedores de la nube también garantizan una mayor exploración de medios para cifrar datos dinámicos, incluyendo datos que se encuentren en la memoria.

Gestión de claves

Los proveedores de servicios en la nube existentes pueden proporcionar planes básicos de claves cifradas para asegurar el desarrollo y los servicios de las aplicaciones basadas en la nube, o pueden dejar todas estas medidas protectoras a discreción de sus clientes. A medida que los proveedores de servicios en la nube progresan hacia poder acoger unos planes de gestión de claves más fuertes, más trabajo debe realizarse para superar los potenciales obstáculos a su adopción. Los estándares emergentes deberían solventar este problema en un futuro cercano, pero todavía se trata de trabajos en curso. Dentro del cloud computing hay diversas problemáticas y retos relacionados con la gestión de claves:

Almacenes de claves seguros. Los propios almacenes de claves deben estar protegidos, al igual que cualquier otro dato sensible. Deben estar protegidos durante su almacenamiento, en tránsito, y en backup. Un mal almacenamiento de claves podría provocar que se pusieran en peligro todos los datos de las bases de datos cifradas.

Acceso a los almacenes de claves. El acceso a los almacenes de claves debe limitarse a las entidades que necesiten específicamente las claves en cuestión. También debería haber políticas que gobiernen los almacenes de claves que utilizan la separación de funciones para ayudar a controlar el acceso; una entidad que utiliza una clave determinada no debería ser la entidad que conserva la clave.

Backup y recuperabilidad de claves. La pérdida de claves supone inevitablemente la pérdida de los datos que protegen dichas claves. Aunque se trata de un modo eficaz de destruir datos, la pérdida accidental de claves que protejan datos críticos para la misión, sería devastadora para un negocio, por lo que deben implementarse soluciones de backup y recuperación seguras.

Hay una serie de estándares e información orientativa que son aplicables a la gestión de claves en la nube. El Protocolo de Interoperabilidad de la Gestión de Claves (KMIP) de OASIS es un estándar emergente para la gestión de claves interoperable en la nube. Los estándares IEEE 1619.3 cubren el cifrado del almacenamiento y la gestión de claves, especialmente cuando hacen referencia a la IaaS de almacenamiento.

Recomendaciones

- √ Utilizar el cifrado para separar la tenencia de datos del uso de datos.
- √ Separar la gestión de claves del proveedor de la nube que hospeda los datos, creando una cadena de separación. Esto protege tanto al proveedor de la nube como al cliente contra conflictos cuando se le obligue a proporcionar datos por mandato legal.
- √ Al estipular el cifrado en el redactado del contrato, debe garantizarse que el cifrado se ajusta a los estándares existentes del sector o del gobierno, según corresponda.
- √ Comprender si las instalaciones del proveedor de la nube proporcionan gestión de funciones y separación de deberes.
- √ Comprender los procesos del proveedor para el ciclo de vida de la gestión de claves: ¿cómo se generan, se usan, se almacenan, se hacen copias de seguridad, se recuperan y se borran las claves?
- √ Comprender si se utiliza la misma clave para cada cliente o si cada cliente tiene sus propias claves.
- √ Asegurarse de que los datos de clientes regulados y/o sensibles son cifrados en tránsito por la red interna del proveedor de la nube, además de ser cifrados en estático. Quedará a discreción del cliente de la nube implementar en los entornos IaaS una responsabilidad compartida entre el cliente de la nube y el proveedor de la nube en entornos PaaS y la responsabilidad del proveedor de la nube en entornos SaaS.
- √ Solicitar el cifrado para backups y archivos al proveedor de la nube.

Colaboradores: John Arnold, Girish Bhat, Jon Callas, Sergio Loureiro, Jean Pawluk, Joel Weise.

Dominio 12: Gestión de acceso e identidades

La gestión de identidades y el control de acceso para las aplicaciones de empresas sigue siendo uno de los grandes retos a los que se enfrenta actualmente la informática. Aunque una empresa puede ser capaz de sacar partido a diversos servicios de cloud computing sin una buena estrategia de gestión de identidades y acceso, a largo plazo, desplegar los servicios de identidad de una organización a la nube es una condición necesaria para el uso estratégico de servicios de computación a la carta. Mantener la actual adopción agresiva de un ecosistema de nube que debe admitirse que es inmaduro requiere una evaluación honesta de la capacidad de la organización para llevar a cabo la gestión de identidades y del acceso a la nube, así como comprender las capacidades de los proveedores de cloud computing de esa organización.

A continuación trataremos las principales funciones de la gestión de identidades y acceso que son esenciales para la gestión exitosa y efectiva de identidades en la nube:

- Abastecimiento/Desabastecimiento de identidades
- Autenticación
- Federación
- Gestión de perfiles de usuario y autorizaciones
- Soporte para el cumplimiento normativo

Abastecimiento de identidades – Uno de los retos más importantes para las organizaciones que adoptan servicios de cloud computing es la gestión segura y puntual de las altas (abastecimiento) y las bajas (desabastecimiento) de usuarios en la nube. Asimismo, las empresas que han invertido en los procesos de gestión de usuarios dentro de una empresa buscarán extender esos procesos y prácticas a los servicios en la nube.

Autenticación - Cuando las organizaciones empiezan a utilizar los servicios en la nube, autenticar a los usuarios de forma fiable y gestionable es un requisito fundamental. Las organizaciones deben afrontar los retos relacionados con la autenticación como la gestión de credenciales, autenticación fuerte, autenticación delegada, y la confianza en la gestión en todos los tipos de servicios en la nube.

Federación - En el entorno del cloud computing, la gestión de identidades federada desempeña un papel vital a la hora de permitir a las organizaciones autenticar a sus usuarios de servicios en la nube utilizando el proveedor de identidades (IdP) elegido por la organización. En este contexto, intercambiar atributos de identidades entre el proveedor del servicio y el IdP de forma segura también es un requisito importante. Las organizaciones que consideren la gestión de identidades federada en la nube deberían comprender los diversos retos y las posibles soluciones para afrontar dichos retos con respecto a la gestión del ciclo de vida de las identidades, métodos de autenticación disponibles para proteger la confidencialidad, y la integridad a la vez que se pueda aplicar el no repudio.

Gestión de perfiles de usuario y autorizaciones – Los requisitos para perfiles de usuario y política de control de acceso variarán en función de si el usuario actúa en su propio nombre (como un consumidor) o como miembro de una organización (como un empresario, universidad, hospital u otro tipo de empresa). Los requisitos

de control de acceso en los entornos SPI incluyen establecer una información fiable de perfil de usuario y de información de políticas, utilizándola para controlar el acceso dentro del servicio en la nube, y haciéndolo de manera auditable.

Abastecimiento de identidades – Recomendaciones

- √ Las capacidades que ofrecen los proveedores de servicios en la nube actualmente no son adecuadas para satisfacer los requisitos de las empresas. Los clientes deberían evitar las soluciones propietarias, como crear conectores personalizados únicos para los proveedores de la nube, puesto que esto exacerbará la complejidad de la gestión.

- √ Los clientes deberían utilizar los conectores estándar proporcionados por los proveedores de servicios en la nube en la medida en que resulte práctico, preferiblemente creados en un esquema SPML. Si tu proveedor en la nube actualmente no ofrece SPML, deberías solicitarlo.

- √ Los clientes de nube deberían modificar o ampliar el depósito fidedigno de datos de identidades de forma que incluya las aplicaciones y procesos presentes en la nube.

Autenticación – Recomendaciones

Tanto el proveedor en la nube como las empresas deberían considerar los retos asociados con la gestión de credenciales, autenticación fuerte e implementar soluciones rentables que reduzcan los riesgos de forma adecuada.

Los proveedores de SaaS y PaaS normalmente proporcionan la opción de prestar servicios de autenticación integrados a sus aplicaciones o plataformas, o de delegar la autenticación a la empresa.
Los clientes tienen las siguientes opciones:

- √ Autenticación para empresas. La empresa debería considerar utilizar la opción de autenticar a los usuarios utilizando su Proveedor de Identidades (IdP) y establecer un vínculo de confianza con el distribuidor de SaaS mediante una Federación.

- √ Autenticación para usuarios individuales (que actúan en su propio nombre). Debería considerarse la autenticación centrada en el usuario como Google, Yahoo, OpenID, Live ID, etc., para permitir el uso de un único conjunto de credenciales que puedan utilizarse en diversos sitios.

- √ Cualquier proveedor de SaaS que requiera métodos propietarios para delegar la autenticación (p.ej. confianza en el manejo a través de una cookie cifrada compartida y otros medios) debería considerarlo en profundidad y realizar la evaluación de seguridad adecuada antes de tomar esa vía. La preferencia general debería ser el uso de estándares abiertos.

En el caso de la IaaS, las estrategias de autenticación pueden aprovechar las capacidades existentes de la empresa.

Para el personal informático, establecer una VPN dedicada será una mejor opción, ya que así podrán sacar partido a los sistemas y procesos ya existentes.

- √ Algunas posibles soluciones son crear un túnel de VPN dedicada a la federación o red corporativa. Un túnel de VPN dedicada funcionará mejor cuando la aplicación aproveche los sistemas de identidad existentes (como una solución SSO o autenticación basada en LDAP que aportan una fuente fidedigna de datos de identidad).

- √ En los casos en los que no sea viable un túnel de VPN dedicada, las aplicaciones deberían designarse para aceptar las aserciones de autenticación en varios formatos (SAML, WS-Federation, etc.), en combinación con el cifrado web estándar como el SSL. Este acercamiento permitirá a las organizaciones desplegar SSO federados no solo dentro de la empresa, sino ampliarlo a sus aplicaciones de nube.

- √ OpenID es otra opción cuando la aplicación se destina más allá de los usuarios de la empresa. Sin embargo, debido a que el control de las credenciales de OpenID queda fuera de la empresa, los privilegios de acceso ampliados a dichos usuarios debería limitarse de forma adecuada.

- √ Cualquier servicio de autenticación localmente implementado dentro del proveedor de la nube debería ser conforme a la OATH. Con una solución conforme a la OATH, las empresas pueden evitar quedar bloqueadas en una de las credenciales de autenticación del distribuidor.

- √ Al objeto de permitir una autenticación fuerte (con independencia de la tecnología), las aplicaciones de nube deberían disponer de la capacidad de delegar autenticación a la empresa que consume los servicios, como a través de SAML.

- √ Los proveedores en la nube deberían considerar la posibilidad de varias opciones de Autenticación Fuerte como Contraseñas de un solo uso, Biométricas, Certificados Digitales, y Kerberos. Esto proporcionará otra opción para que las empresas utilicen su infraestructura existente.

Recomendaciones para la federación

En el entorno de cloud computing, la federación de identidades desempeña un papel clave a la hora de permitir a las empresas aliadas autenticar, proporcionar un log-in único (SSO) o reducido e intercambiar atributos de identidad entre el Proveedor del Servicio y el Proveedor de Identidades (IdP). Las organizaciones que estén considerando la gestión de identidades federada en la nube deberían comprender los diversos retos y las posibles soluciones para afrontar dichos retos en relación con la gestión del ciclo de vida de las identidades, los métodos de autenticación, los formatos de tokens y el no repudio.

- √ Las empresas que buscan un proveedor en la nube deberían verificar que el proveedor en la nube cumple por lo menos uno de los principales estándares (SAML y WS-Federation). El SAML es un estándar de federación emergente y cada vez más extendido y lo cumplen la mayoría de proveedores de servicios en la nube de SaaS y PaaS. Cumplir diversos estándares permitirá un mayor grado de flexibilidad.

- √ Los proveedores en la nube deberían tener flexibilidad para aceptar los formatos de federación estándar procedentes de diferentes proveedores de identidades. Sin embargo, la mayoría de proveedores de servicios en la nube, en el momento de redactar este texto, cuentan con un único estándar (p.ej. SAML 1.1 o SAML 2.0). Los proveedores de servicios en la nube que deseen disponer de diversos formatos de tokens de federación deberían considerar implementar algún tipo de pasarela para la federación.

- √ Las organizaciones podrían desear evaluar el SSO Público Federado en relación con el SSO Privado Federado. El SSO Público Federado se basa en estándares como el SAML o el WS-Federation por parte del proveedor de la nube, mientras que en el SSO Privado Federado, las organizaciones aprovechan su arquitectura SSO existente sobre una VPN. A largo plazo, el SSO Público Federado será ideal, aunque una organización con una arquitectura SSO madura y un número limitado de nubes pueda obtener beneficios a corto plazo en cuanto a los costes con un SSO Privado Federado.

- √ Las organizaciones pueden desear optar por pasarelas de federación al objeto de externalizar su implementación de la federación para gestionar la emisión y verificación de tokens. Utilizando este método, las organizaciones pueden delegar la emisión de varios tipos de tokens a la pasarela de la federación, y la pasarela de la federación se encarga del trabajo central de traducir los tokens de un formato a otro.

Recomendaciones de control de acceso

El reto de seleccionar o revisar la adecuación de las soluciones de control de acceso para servicios en la nube tiene muchos aspectos y puede encararse teniendo en cuenta lo siguiente:

- √ Revisar la adecuación del modelo de control de acceso para el tipo de servicio o datos.

- √ Identificar la fuente fidedigna de la información de perfil de usuario y de políticas.

- √ Evaluar el cumplimiento de las políticas de privacidad necesarias para los datos.

- √ Seleccionar un formato con el cual especificar la información sobre políticas y usuarios.

- √ Determinar el mecanismo para transmitir las políticas desde un Punto de Administración de Políticas (PAP) a un Punto de Decisión de Políticas (PDP).

- √ Determinar el mecanismo para transmitir la información del usuario desde un Punto de Información de Políticas (PIP) a un Punto de Decisión de Políticas (PDP).

- √ Solicitar una decisión de políticas desde un Punto de Decisión de Políticas (PDP).

- √ Aplicar la decisión de políticas en el Punto de Aplicación de Políticas (PEP, en sus siglas inglesas).

- √ Información de registro necesaria para auditorías.

Recomendaciones para IDaaS

La Identidad como Servicio (IDaaS) debería seguir las mismas mejores prácticas que una implementación interna de gestión de identidades y acceso, junto con las consideraciones adicionales de privacidad, integridad y auditabilidad.

- √ Para los usuarios internos de la empresa, los custodios deben revisar las opciones, el proveedor de la nube debe proporcionar acceso seguro a la nube, bien a través de una VPN directa, o a través de un estándar del sector como SAML y autenticación fuerte. La reducción de costes utilizando la nube debe equilibrarse con medidas de mitigación de riesgos para afrontar las consideraciones de privacidad inherentes a tener información de empleados almacenada de forma externa.

- √ Para los usuarios externos, como los socios, "Usuario Externo": Los propietarios de la información para usuarios externos deben incorporar interacciones con proveedores de gestión de identidades y acceso en su SDLC, así como en su evaluación de amenazas. La seguridad de las aplicaciones –las interacciones de los diversos componentes entre ellos, y las vulnerabilidades creadas por las mismas (como SQL Injection y Cross Site Scripting, entre muchas otras)– también deben tenerse en cuenta e implementar protecciones.

- √ Los clientes PaaS deberían estudiar la medida en que el distribuidor de IdaaS cumple los estándares del sector para el abastecimiento, autenticación, comunicación sobre políticas de control de acceso e información de auditorías.

- √ Las soluciones propietarias suponen un riesgo significativo para los componentes de tu entorno de gestión de identidades y accesos en la nube, debido a la falta de transparencia en los componentes propietarios. Los protocolos de red propietarios, los algoritmos de cifrado, y la comunicación de datos a menudo son menos seguros, menos robustos y menos interoperables. Es importante utilizar unos estándares abiertos para los componentes de gestión de identidades y accesos que estás externalizando desde tu implementación.

- √ Para los clientes IaaS, las imágenes de terceros utilizadas para lanzar servidores virtuales deben ser verificadas para la autenticidad de usuarios e imágenes. Un examen del soporte previsto para la gestión del ciclo de vida de la imagen debe tener los mismos principios utilizados para el software instalado en la red dentro de tu infraestructura.

Colaboradores: Subra Kumaraswamy Sitaraman Lakshminarayanan, Michael Reiter, Joseph Stein, Yvonne Wilson.

Dominio 13: Virtualización

La capacidad para prestar servicios en la nube multiposesión en el nivel de la infraestructura, plataforma o software a menudo se ve sostenida por la capacidad de proporcionar algún tipo de virtualización para crear una escalada en la economía. No obstante, el uso de estas tecnologías genera problemas de seguridad adicionales. Este dominio trata sobre estos problemas de seguridad. Aunque hay diversas formas de virtualización, de lejos, el uso más habitual es el sistema operativo virtualizado, y este es el punto principal de esta versión de nuestra orientación. Si se utiliza la tecnología de Máquina Virtual (VM, en sus siglas inglesas) en la infraestructura de los servicios en la nube, entonces debemos preocuparnos por compartimentar y aumentar la seguridad de dichos sistemas de VM.

La realidad de las prácticas actuales relacionadas con la gestión de los sistemas operativos virtuales es que muchos procesos que proporcionan seguridad por defecto han desaparecido, y hay que poner una atención especial para sustituirlos. La propia tecnología de virtualización central introduce nuevas superficies de ataque con el hipervisor y otros componentes de gestión, pero más importante es el grave impacto que tiene la virtualización en la seguridad de la red. Las máquinas virtuales ahora se comunican a través de una placa de fondo de hardware, no de una red. De este modo, los controles de seguridad de red estándar ahora no sirven para este tráfico y no pueden ejercer su función de seguimiento ni otras funciones de bloqueo en línea. Estos controles deben adquirir una nueva forma para funcionar en el entorno virtual.

La mezcla de datos que se deriva de los depósitos y servicios centralizados es un problema. Una base de datos centralizada como la que proporciona un servicio de cloud computing en teoría debería mejorar la seguridad sobre los datos distribuidos sobre una amplia cantidad y variedad de puntos finales. Sin embargo, éste es un ejemplo de centralizar el riesgo, y una violación puede tener consecuencias significativas.

Hay otro problema que puede surgir con la mezcla de VMs de diferentes sensibilidades y seguridad. En los entornos de cloud computing, el mínimo común denominador de la seguridad será compartido por todos los poseedores en los entornos virtuales multiposesión a menos que pueda alcanzarse una nueva arquitectura de seguridad que no esté ligada a la dependencia de ninguna red para su protección.

Recomendaciones

- √ Identificar qué tipos de virtualización utiliza tu proveedor en la nube, cuando corresponda.

- √ Los sistemas operativos virtualizados deberían aumentarse con tecnología de seguridad de terceros para proporcionar controles de seguridad por capas y reducir la dependencia del proveedor de la plataforma solamente.

- √ Comprender qué controles de seguridad hay disponibles de forma interna a las VMs, además del aislamiento del hipervisor incorporado, como detección de intrusiones, antivirus, escaneo de vulnerabilidades, etc. La configuración Seguro por defecto debe asegurarse alcanzando o superando las referencias disponibles del sector.

- √ Comprender qué controles de seguridad hay expuestos para los clientes de forma externa a las VMs para proteger las interfaces administrativas (on-line, APIs, etc.).

- √ Validar el pedigrí y la integridad de cualquier imagen o plantilla de VM que se origine del Proveedor de la Nube antes de su uso.

- √ Los mecanismos de seguridad específicos de las VM incrustadas en APIs del hipervisor deben ser utilizados para proporcionar un seguimiento granular del tráfico que cruza las placas de fondo de las VM, que será opaco a los controles de seguridad de red tradicionales.

- √ El acceso y control administrativo de los sistemas operativos virtualizados es fundamental, y debería incluir la autenticación fuerte integrada con la gestión de identidades de la empresa, así como el registro a prueba de inicios de sesión no autorizados y herramientas de seguimiento de la integridad.

- √ Explorar la eficacia y la viabilidad de segregar VMs y crear zonas de seguridad por tipo de uso (p.ej. Escritorio vs Servidor), etapa de producción (p.ej. Desarrollo, Producción, y Test) y sensibilidad de los datos en hardwares físicos separados como servidor, almacenamiento, etc.

- √ Disponer de un mecanismo de generación de informes que aporte evidencias del aislamiento y emita alertas si se produce una violación del aislamiento.

- √ Ser consciente de las situaciones de multiposesión con tus VMs en las que los problemas de cumplimiento normativo puedan justificar la segregación.

Colaboradores: Bikram Barman, Sarabjeet Chugh, Srijith K. Nair, Girish Bhat, Philip Cox, Lee Newcombe, Joe Cupano, Brian O'Higgins.

Asociación Española para el Fomento de la Seguridad de la Información

ISMS Forum Spain es una asociación sin ánimo de lucro, creada en 2007, **para el Fomento de la Seguridad de la Información en España.** Su finalidad es promover el **desarrollo, conocimiento y cultura de la Seguridad de la Información en España** y actuar en beneficio de toda la comunidad implicada en el sector. Se constituye como foro especializado de debate para que todas las empresas; organismos públicos y privados; investigadores y profesionales **colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos** en el ámbito de los SGSI. Todo ello desde la **transparencia**, la **objetividad** y la **neutralidad**.

ISMS Forum Spain nació respaldada por representativas empresas y organizaciones comprometidas con la seguridad de la información. Los socios fundadores proceden de muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Certificación, Seguros, Construcción, Servicios Jurídicos o Telecomunicaciones. La asociación se ha creado con una vocación **plural y abierta**; que quiere representar a todos los sectores implicados. Por ello **invita a todos los profesionales, empresas e instituciones involucrados en la gestión de la seguridad de la información a asociarse.**

ISMS Forum Spain tiene en la actualidad a más de **85 empresas asociadas** (cada una de las cuales puede nombrar hasta ocho socios de pleno derecho). Además, numerosos expertos del sector se han asociado de manera independiente. ISMS Forum Spain cuenta hoy con más de **650 profesionales asociados**, ya sea a través de sus empresas o por iniciativa individual. La Asociación para el Fomento de la Seguridad de la Información es ya, por tanto, la **mayor red activa española de expertos en SGSI.**

Entre los principales objetivos de ISMS Forum Spain destacan:

- Dar **visibilidad** a un sector **estratégico** para el desarrollo económico, como es la Seguridad de la Información, y **difundir** el **talento** de los profesionales que trabajan en él.
- Situar a las empresas y organizaciones españolas a la **vanguardia de conocimientos** e implementación de SGSI.
- Ser **interlocutores** en España de diversas asociaciones y foros internacionales relacionados con la Seguridad de la Información.

Para ello, entre otras actividades, ISMS Forum Spain:

- Organiza **eventos** y **actividades formativas** para sus asociados.
- Prepara **herramientas divulgativas** (informes y estudios monográficos; traducción y edición en castellano de manuales y guías de referencia) **e informativas** (newsletter).
- Ha creado el primer **Registro *online* de Profesionales Certificados** en España, que se ampliará en breve con un nuevo **Registro de Empresas Certificadas en ISO27001 en España**.
- Participa en **foros nacionales e internacionales** y coopera con instituciones públicas y privadas, nacionales e internacionales, para impulsar la cultura de la Gestión de la Seguridad de la Información.

Data Privacy Institute, el nuevo foro específico para los profesionales de la Privacidad

DPI Data Privacy Institute
AN ISMS FORUM INITIATIVE

ISMS Forum Spain ha presentado recientemente el **Data Privacy Institute (DPI),** cuya vocación es aglutinar a todas las personas y organizaciones que tienen interés y responsabilidades en la privacidad y la protección de datos personales, promoviendo la formación y excelencia de sus asociados. Para ello ya ha puesto en marcha la certificación **CDPP (Certified Data Privacy Professional)** específicamente dirigida al área de la Privacidad y pionera en España. El DPI pretende asimismo ser una vía para la difusión de mejores prácticas en el uso y la protección de los datos personales entre las empresas y particulares españoles, y facilitar cauces de interlocución con las administraciones y autoridades de control.

El trámite para hacerse socio de ISMS Forum Spain se realiza online en www.ismsforum.es

Socios Fundadores:

BANKINTER • BT • CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA • ECIJA • FCC • FUTURESPACE • GAS NATURAL • HEWLETT-PACKARD • SANITAS • S21SEC • SGS ICS • UNIVERSIDAD COMPLUTENSE DE MADRID

ISMS Forum Spain está inscrita en el Registro Nacional de Asociaciones Grupo I, Sección I, Número Nacional 588718