GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza2
INTECO
Instituto Nacional de Tecnologías de la Comunicación

RIESGOS Y AMENAZAS EN *CLOUD COMPUTING*

INTECO-CERT

Marzo 2011

La presente publicación pertenece al Instituto Nacional de Tecnología de la Comunicación (INTECO) y esta bajo licencia Reconocimiento-No comercial 3.0 España de Creative Commons, y por ello estar permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: www.inteco.es. Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.

- Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO. http://creativecommons.org/licenses/by-nc-sa/3.0/es/

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format). Así, se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es

ÍNDICE

1. INTRODUCCIÓN

En la actualidad una de las tendencias del mercado de los sistemas de información es la proliferación de los servicios operando en la nube, los cuales son servicios que permiten la asignación dinámica de recursos en función de necesidades de los clientes y que aportan una reducción de costes en infraestructuras considerable.

La reciente publicación del NIST (*National Institute of Standards and Technologies*) «*Guidelines on Security and Privacy in Public Cloud Computing*» pone de manifiesto, además de la actualidad de este nuevo modelo para la distribución de servicios y aplicaciones, la necesidad de difundir buenas prácticas de seguridad para este modelo. Este no es el único documento que refleja la creciente preocupación por la seguridad en estas plataformas, como se refleja en documentos de entidades de referencia que también abordan este tema.

El informe siguiente resume algunos de estos documentos con el propósito de facilitar una visión general de amenazas, riesgos y aspectos a considerar en la seguridad en *cloud*.

Este informe realiza, en primer lugar, una descripción de los tipos de infraestructuras y servicios *cloud* para, a continuación, abordar los distintos elementos que han de tenerse en cuenta para abordar su seguridad, según el citado documento del NIST e informes recientes de la organización internacional CSA (*Cloud Security Alliance*) y de la consultora Gartner.

Las preocupaciones que derivan de estos informes se centran en aspectos la **gestión de los datos**, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte de los proveedores, así como en la **identificación y control de acceso** a los recursos.

2. *CLOUD COMPUTING*

Cloud computing se ha definido por el NIST1 como un modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios…) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con un mínimo esfuerzo de gestión e interacción por parte del proveedor del *cloud*.

El origen del término está en el gráfico de uso común para representar Internet como si fuera una nube (*cloud*). Los recursos de computación (hardware y software) de estos modelos están disponibles a través de Internet.

A continuación, se describen los distintos tipos de infraestructuras y servicios *cloud*.

2.1. TIPOS DE INFRAESTRUCTURAS *CLOUD*

Atendiendo a la titularidad de la infraestructura en la nube se pueden distinguir tres tipos de infraestructuras *cloud*: privada, pública y comunitaria. A continuación se presentan las ventajas e inconvenientes de cada uno.

2.1.1. Público

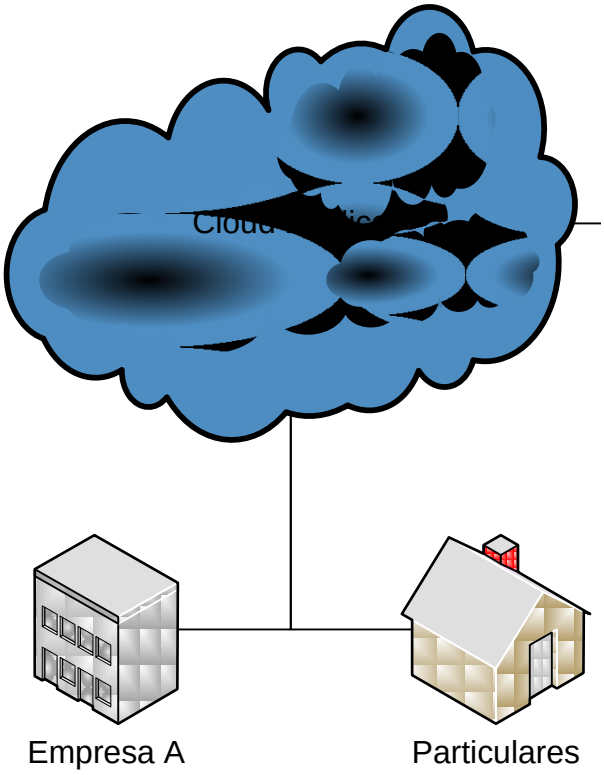
Es aquel tipo de *cloud* en el cual la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet.

Suele ser propiedad de un proveedor que gestiona la infraestructura y el servicio o servicios que se ofrecen.

Ventajas	Inconvenientes
Escalabilidad.	Se comparte la infraestructura con más organizaciones.
Eficiencia de los recursos mediante los modelos de pago por uso.	Poca transparencia para el cliente, ya que no se conoce el resto de servicios que comparten recursos, almacenamiento, etc.
Gran ahorro de tiempo y costes.	Dependencia de la seguridad de un tercero.

[1] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009, <URL: http://csrc.nist.gov/groups/SNS/cloud-computing>.

Imagen 1: *Cloud* Público



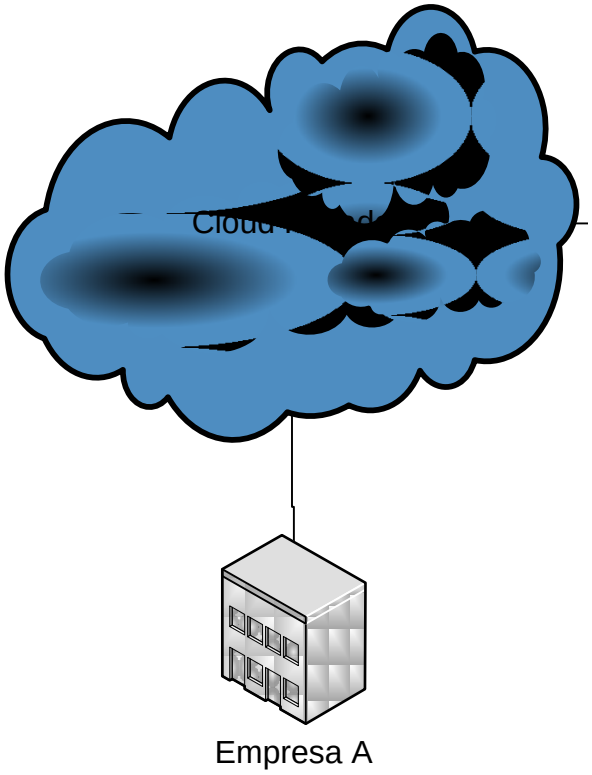
Fuente: INTECO-CERT

2.1.2. Privado

Este tipo de infraestructuras *cloud* se crean con los recursos propios de la empresa que lo implanta, generalmente con la ayuda de empresas especializadas en este tipo de tecnologías.

Ventajas	Inconvenientes
Cumplimiento de las políticas internas.	Elevado coste material.
Facilidad para trabajo colaborativo entre sedes distribuidas.	Dependencia de la infraestructura contratada.
Control total de los recursos.	Retorno de inversión lento dado su carácter de servicio interno.

Imagen 2: *Cloud* Privado



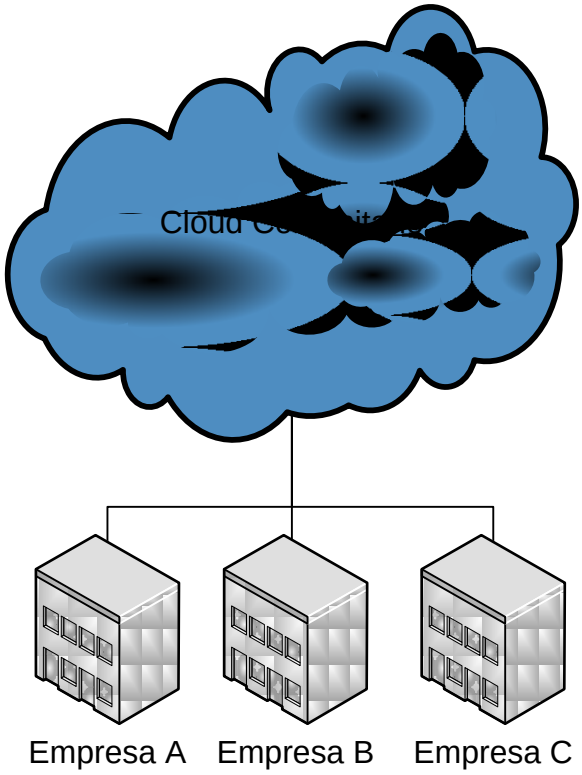
Fuente: INTECO-CERT

2.1.3. Comunitario

Un *cloud* comunitario se da cuando dos o más organizaciones forman una alianza para implementar una infraestructura *cloud* orientada a objetivos similares y con un marco de seguridad y privacidad común.

Ventajas	Inconvenientes
Cumplimiento con las políticas internas.	Seguridad dependiente del anfitrión de la infraestructura.
Reducción de costes al compartir la infraestructura y recursos.	Dependencia de la infraestructura contratada.
Rápido retorno de inversión.	

Imagen 3: *Cloud* Comunitario



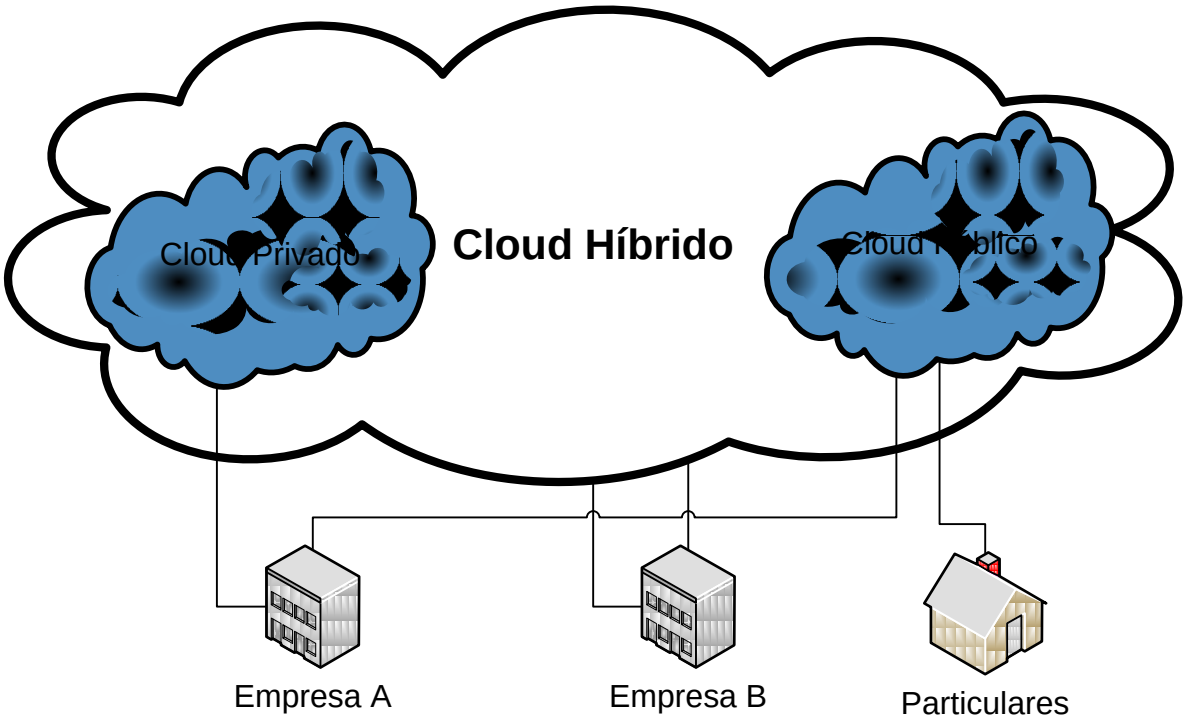
Fuente: INTECO-CERT

2.1.4. Híbridos

Este es un término amplio que implica la utilización conjunta de varias infraestructuras *cloud* de cualquiera de los tres tipos anteriores, que se mantienen como entidades separadas pero que a su vez se encuentran unidas por la tecnología estandarizada o propietaria, proporcionando una portabilidad de datos y aplicaciones.

En este caso las ventajas e inconvenientes son los mismos que los relativos a los tipos de *cloud* que incluya la infraestructura.

Imagen 4: *Cloud* Hibrido



Fuente: INTECO-CERT

2.2. TIPOS DE SERVICIOS *CLOUD*

Los servicios en *cloud* pueden identificarse según se ofrezca software, plataformas o infraestructuras como servicio.

2.2.1. Software como servicio (*SaaS*)

Este modelo, Software como servicio o *SaaS* (del inglés, *Software as a Service*) consiste en un despliegue de software en el cual las aplicaciones y los recursos computacionales se han diseñado para ser ofrecidos como servicios de funcionamiento bajo demanda, con estructura de servicios llave en mano. De esta forma se reducen los costes tanto de software como hardware, así como los gastos de mantenimiento y operación.

Las consideraciones de seguridad son controladas por el proveedor del servicio. El suscriptor del servicio únicamente tiene acceso a la edición de las preferencias y a unos privilegios administrativos limitados.

2.2.2. Plataforma como servicio (*PaaS*)

Este es el modelo de Plataforma como servicio o *PaaS* (del inglés, *Platform as a Service*) en el cual el servicio se entrega como bajo demanda, desplegándose el entorno (hardware y software) necesario para ello. De esta forma, se reducen los costes y la complejidad de la compra, el mantenimiento, el almacenamiento y el control del hardware y el software que componen la plataforma.

El suscriptor del servicio tiene control parcial sobre las aplicaciones y la configuración del entorno ya que la instalación de los entornos dependerá de la infraestructura que el proveedor del servicio haya desplegado. La seguridad se comparte entre el proveedor del servicio y el suscriptor.

2.2.3. Infraestructura como Servicio (*IaaS*)

Es un modelo en el cual la infraestructura básica de cómputo (servidores, software y equipamiento de red) es gestionada por el proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar ejecutar o probar aplicaciones. Se denomina Infraestructura como Servicio o *IaaS* (del inglés, *Infrastructure as a Service*).

El fin principal de este modelo es evitar la compra de recursos por parte de los suscriptores, ya que el proveedor ofrece estos recursos como objetos virtuales accesibles a través de un interfaz de servicio.

El suscriptor mantiene generalmente la capacidad de decisión del sistema operativo y del entorno que instala. Por lo tanto, la gestión de la seguridad corre principalmente a cargo del suscriptor.

3. SEGURIDAD EN *CLOUD*

Se plantean, a continuación, las consideraciones de seguridad de infraestructuras y servicios en *cloud*.

Se analizan las amenazas, los riesgos y las recomendaciones que han descrito los líderes del sector: la organización internacional CSA (*Cloud Security Alliance*), la consultora Gartner y el instituto norteamericano NIST (*National Institute of Standards and Technology)*.

3.1. AMENAZAS SEGÚN *CSA* (*CLOUD SECURITY ALLIANCE*)

La *Cloud Security Alliance* se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en *cloud*.

En marzo del 2010 publicó un informe «*Top Threats to Cloud Computing V1.0*» sobre las siete mayores amenazas de la infraestructuras *cloud*, con el propósito de asistir a las organizaciones en la toma de decisiones y en la adopción de estrategias que incluyan *cloud computing.* Estas amenazas se actualizan regularmente buscando el consenso de los expertos. A continuación, se resumen las amenazas descritas en este informe.

3.1.1. Abuso y mal uso del *cloud computing*

Esta amenaza afecta principalmente a los modelos de servicio *IaaS* y *PaaS* y se relaciona con un registro de acceso a estas infraestructuras/plataformas poco restrictivo. Es decir, cualquiera con una tarjeta de crédito válida puede acceder al servicio, con la consecuente proliferación de *spammers,* creadores de código malicioso y otros criminales que utilizan la nube como centro de operaciones.

- **Ejemplos:**
  - *IaaS* que han albergado la *Zeus Botnet*
  - *Botnets* que han alojado sus centros de control en infraestructuras cloud
  - rangos completos de direcciones de infraestructuras *cloud* bloqueadas por envío de correo basura

- **Recomendaciones:**
  - implementar un sistema de registro de acceso más restrictivo
  - coordinar y monitorizar el fraude en tarjetas de crédito
  - monitorizar el trafico de clientes para la detección de posibles actividades ilícitas
  - comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas

3.1.2. Interfaces y *API* poco seguros

Generalmente los proveedores de servicios en la nube ofrecen una serie de interfaces y *API (*del inglés, *Application Programming Interface)* para controlar e interactuar con los recursos. De este modo, toda la organización, el control, la provisión y la monitorización de los servicios *cloud* se realiza a través de estos *API* o interfaces.

Dado que todo (autenticación, acceso, cifrado de datos, etc.) se realiza a través de estas herramientas, se hace necesario que los interfaces estén diseñados de forma segura, evitando así los problemas de seguridad, tanto los que son intencionados como los que se producen de forma accidental.

- **Ejemplos:**
  - permitir acceso anónimo, reutilización de *tokens*, autenticación sin cifrar, etc.
  - limitaciones a la hora de gestión de *logs* (registros de actividad) y monitorización

- **Recomendaciones:**
  - analizar los problemas de seguridad de las interfaces de los proveedores de servicio
  - asegurarse que la autenticación y los controles de acceso se implementan teniendo en cuenta el cifrado de los datos

3.1.3. Amenaza interna

Como en todos los sistemas de información, la amenaza que suponen los propios usuarios es una de las más importantes, dado que tienen acceso de forma natural a los datos y aplicaciones de la empresa. En un entorno *cloud* esto no es en absoluto diferente ya que se pueden desencadenar igualmente incidentes de seguridad provocados por empleados descontentos y accidentes por error o desconocimiento.

Además, en muchos casos, es el propio proveedor del servicio el que gestiona las altas y bajas de los usuarios, produciéndose brechas de seguridad cuando el consumidor del servicio no informa al proveedor de las bajas de personal en la empresa.

Como es lógico, estos incidentes repercuten de forma importante en la imagen de la empresa y en los activos que son gestionados.

Los proveedores de servicio deberán proveer a los consumidores del servicio de medios y métodos para el control de las amenazas internas.

- **Recomendaciones:**
  - especificar cláusulas legales y de confidencialidad en los contratos laborales
  - determinar los posibles problemas en los procesos de notificación

3.1.4. Problemas derivados de las tecnologías compartidas

Esta amenaza afecta a los modelos *IaaS*, ya que en un modelo de Infraestructura como Servicio los componentes físicos (CPU, GPU, etc.) no fueron diseñados específicamente para una arquitectura de aplicaciones compartidas. Se han dado casos en los que los hipervisores de virtualización podían acceder a los recursos físicos del anfitrión provocando, de esta forma, incidentes de seguridad.

Para evitar este tipo de incidentes se recomienda implementar una defensa en profundidad con especial atención a los recursos de computación, almacenamiento y red. Además, se ha de generar una buena estrategia de seguridad que gestione correctamente los recursos para que las actividades de un usuario no puedan interferir en las del resto.

- **Ejemplos:**
  - exploits o *malware* que consiguen acceder a los recursos del equipo anfitrión de la virtualización

- **Recomendaciones:**
  - diseñar buenas prácticas para la instalación y configuración
  - monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad
  - proporcionar autenticación fuerte y control de acceso para el acceso de administración
  - adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades

3.1.5. Pérdida o fuga de información

Existen muchas formas en las que los datos se pueden ver comprometidos. Por ejemplo, el borrado o modificación de datos sin tener una copia de seguridad de los originales, supone una pérdida de datos.

En la nube, aumenta el riesgo de que los datos se vean comprometidos ya que el número de interacciones entre ellos se multiplica debido a la propia arquitectura de la misma. Esto deriva en pérdida de imagen de la compañía, daños económicos y, si se trata de fugas, problemas legales, infracciones de normas, etc.

- **Ejemplos:**
  - mal uso de las claves de cifrado y de software
  - autenticación, autorización y auditoria débil

- **Recomendaciones:**
  - implementar *API* potentes para el control de acceso
  - proteger el tránsito de datos mediante el cifrado de los mismos

- analizar la protección de datos tanto en tiempo de diseño como en tiempo de ejecución
- proporcionar mecanismos potentes para la generación de claves, el almacenamiento y la destrucción de la información
- definir, por contrato, la destrucción de los datos antes de que los medios de almacenamiento sean eliminados de la infraestructura, así como la política de copias de seguridad

3.1.6. Secuestro de sesión o servicio

En un entorno en la nube, si un atacante obtiene las credenciales de un usuario del entorno puede acceder a actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos.

- **Recomendaciones:**
  - prohibir, mediante políticas, compartir credenciales entre usuarios y servicios
  - aplicar técnicas de autenticación de doble factor siempre que sea posible
  - monitorizar las sesiones en busca de actividades inusuales

3.1.7. Riesgos por desconocimiento

Uno de los pilares de las infraestructuras *cloud* es reducir la cantidad de *software* y *hardware* que tienen que adquirir y mantener las compañías, para así poder centrarse en el negocio. Esto, si bien repercute en ahorros de costes tanto económicos como operacionales, no puede ser motivo para el deterioro de la seguridad por falta de conocimiento de esta infraestructura.

Para asistir en la toma de decisiones sobre las medidas de seguridad que se han de implantar en un entorno *cloud* es conveniente conocer, al menos en parte, la información técnica de la plataforma. Datos como con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad.

La carencia de información de este tipo puede derivar en brechas de seguridad desconocidas por el afectado.

- **Recomendaciones:**
  - tener acceso a los *logs* (registros de actividad) de aplicaciones y datos
  - estar al corriente, total o parcialmente, de los detalles de la infraestructura
  - monitorizar y recibir alertas sobre el uso de información crítica

3.2. RIESGOS DETECTADOS POR GARTNER

Gartner S.A. es una compañía de investigación y consultoría de tecnologías de la información, con sede en Stamford, Connecticut, Estados Unidos. Se conocía como Grupo Gartner hasta 2001.

Gartner tiene como clientes a grandes empresas, agencias de gobierno, empresas tecnológicas y agencias de inversión. Fue fundada en 1979, tiene actualmente 4.000 socios y dispone de 1.200 analistas y consultores con presencia en 75 países por todo el mundo.

Desde su posición de analista de las tecnologías de la información, también ha realizado recientemente el informe «*Assessing the Security Risks of Cloud Computing*» sobre los principales riesgos en *cloud computing*. A continuación, se incluye un extracto de las recomendaciones y buenas prácticas del citado informe.

3.2.1. Accesos de usuarios con privilegios

El procesamiento o tratamiento de datos sensibles fuera de las instalaciones de la empresa conlleva un riesgo inherente, ya que es posible que estos servicios externos sorteen los controles físicos, lógicos y humanos siendo, por este motivo, necesario conocer quién maneja dichos datos.

Por tanto, se hace obligatorio consensuar con el proveedor los usuarios que tendrán acceso a esos datos, para minimizar así los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los datos.

3.2.2. Cumplimento normativo

Los clientes son en última instancia responsables de la seguridad e integridad de sus datos, aunque estos se encuentren fuera de las instalaciones y gestionados por un proveedor de servicios *cloud*.

Los prestadores de servicios tradicionales se hallan sujetos a auditorías externas y certificaciones de seguridad, por lo tanto los proveedores de servicios en la nube también deben acogerse a este tipo de prácticas. Si se negasen a este tipo de auditorías no se les debería confiar los datos sensibles de la empresa.

3.2.3. Localización de los datos

Al utilizar entornos en la nube no se conoce de forma exacta en qué país están alojados.

Se debe consultar con los proveedores cuál es el marco regulatorio aplicable al almacenamiento y procesado de datos, siendo una buena práctica cerrar un acuerdo con el proveedor para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio.

3.2.4. Aislamiento de datos

Los datos en los entornos *cloud* comparten infraestructura con datos de otros clientes. El proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. El cifrado de los datos es una buena práctica, pero el problema es cómo aislar los datos cuando se encuentran en reposo ya que el cifrado, cuando no se hace uso de los datos, puede resultar una operación costosa.

El prestador del servicio debe garantizar que los datos en reposo estarán correctamente aislados y que los procedimientos de cifrado de la información se realizarán por personal experimentado, ya que el cifrado de los datos mal realizado también puede producir problemas con la disponibilidad de los datos o incluso la pérdida de los mismos.

3.2.5. Recuperación

Los proveedores de servicio deben tener una política de recuperación de datos en caso de desastre. Asimismo, es muy recomendable que los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general.

Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar.

3.2.6. Soporte investigativo

La investigación de actividades ilegales en entornos *cloud* puede ser una actividad casi imposible, porque los datos y *logs* (registros de actividad) de múltiples clientes pueden estar juntos e incluso desperdigados por una gran cantidad de equipos y centros de datos.

Lo recomendable será que el proveedor garantice que los *logs* y los datos de los incidentes se gestionan de una forma centralizada.

3.2.7. Viabilidad a largo plazo

En un entorno ideal un proveedor de servicios *cloud* siempre permanecerá en el mercado dando un servicio de calidad y con una disponibilidad completa, pero el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos.

El cliente debe asegurarse que podrá recuperar sus datos aún en el caso de que el proveedor sea comprado o absorbido por otro o bien contemplar la posibilidad de que los datos puedan ser migrados a la nueva infraestructura.

3.3. ASPECTOS CLAVE DE SEGURIDAD EN *CLOUD* SEGÚN NIST

El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, *National Institute of Standards and Technology*) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es

promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

En este sentido, también ha publicado recientemente un borrador de una de sus guías «*Guidelines on Security and Privacy in Public Cloud Computing*» en las que propone unos refuerzos de seguridad centrándose en una clasificación particular. Se resume a continuación.

3.3.1. Gobernanza

La gobernanza implica el control y la supervisión de las políticas, los procedimientos y los estándares para el desarrollo de aplicaciones, así como el diseño, la implementación, las pruebas y la monitorización de los servicios distribuidos. El *cloud*, por su diversidad de servicios y su amplia disponibilidad, amplifica la necesidad de una buena gobernanza.

Garantizar que los sistemas son seguros y que los riesgos están gestionados es un reto en cualquier entorno *cloud*. Es un requisito de seguridad instalar adecuadamente los mecanismos y herramientas de auditoría para determinar cómo se almacenan los datos, cómo se protegen y cómo se utilizan tanto para validar los servicios y como para verificar el cumplimiento de las políticas.

Por otra parte, se ha de prestar especial atención a los roles y las responsabilidades involucrados en la gestión de riesgos. Es muy recomendable poner en marcha un programa de gestión de riesgos que sea suficientemente flexible para tratar con un entorno de riesgos variables y en continua evolución.

3.3.2. Cumplimiento

El cumplimiento obliga a la conformidad con especificaciones estándares, normas o leyes establecidas. La legislación y normativa relativa a privacidad y seguridad varía mucho según los países con diferencias, en ocasiones, a nivel nacional, regional o local haciendo muy complicado el cumplimiento en *cloud computing*.

- **Ubicación de los datos**

  Uno de los principales problemas de los servicios en *cloud computing* es la ausencia de información acerca de cómo se ha implantado la infraestructura, por lo cual el suscriptor no tiene prácticamente información de cómo y dónde son almacenados los datos ni de cómo se protegen los mismos. La posesión de certificaciones de seguridad o la realización de auditorías externas por parte del proveedor mitiga, en parte, el problema aunque tampoco es una solución.

  Cuando la información se mueve por diferentes países, sus marcos legales y regulatorios cambian y esto, obviamente, afecta a la forma de tratar los datos. Por ejemplo, las leyes de protección de datos imponen obligaciones adicionales a los procedimientos de manejo y procesamiento de datos que se transfieren a EEUU.

La principal preocupación del cumplimiento radica en conocer los límites en los que deja de aplicar la legislación del país que recoge los datos y comienza a aplicar la legislación del país destino de los mismos así como si la legislación en el destino supone algún riesgo o beneficio adicional. Por lo general aplican las salvaguardas técnicas, físicas y administrativas, como los controles de acceso.

- **Investigación electrónica**

La investigación electrónica se ocupa de la identificación, la recolección, el procesamiento, el análisis y la producción de los documentos en la fase de descubrimiento de un procedimiento judicial. Las organizaciones también tienen obligaciones para la preservación y la generación de los documentos, tales como cumplir con las auditorías y solicitudes de información. Estos documentos no sólo incluyen correos electrónicos, adjuntos del correo y otros datos almacenados en los sistemas, sino también metadatos como fechas de creación y modificación.

Las capacidades de un proveedor *cloud* y las herramientas de investigación disponibles pueden dificultar el cumplimiento de las obligaciones de la organización. Por ejemplo, si los elementos de almacenamiento de un proveedor no guardan los metadatos originales y suceden daños intencionados (borrado de datos, pérdida, alteración material o bloqueo de evidencias que son básicas para la investigación) la carencia de estos metadatos tiene un impacto negativo en la investigación.

3.3.3. Confianza

En *cloud computing* la organización cede el control directo de muchos aspectos de la seguridad confiriendo un nivel de confianza sin precedentes al proveedor de *cloud*.

- **Acceso desde dentro**

Los datos almacenados fuera de los límites de una organización están protegidos por cortafuegos y otros controles de seguridad que conllevan en sí mismos un nivel de riesgo inherente. Las amenazas internas son un problema conocido por la mayoría de las organizaciones y aunque su nombre no lo refleje aplica también en los servicios *cloud*.

Estas amenazas pueden ser provocadas tanto por los antiguos como por los actuales empleados así como por las empresas asociadas, las asistencias técnicas y otros actores que reciben acceso a las redes corporativas y datos para facilitar las operaciones. Los incidentes pueden ser tanto intencionados como no intencionados y de muy diversos tipos incluyendo fraude, sabotaje de los recursos de información, robo de información confidencial.

Al traspasar los datos a un entorno *cloud* operado por un proveedor, las amenazas internas se extienden no sólo al personal del proveedor sino también a los consumidores del servicio. Un ejemplo de esto se demostró por una denegación de servicio realizada por un atacante interno. El ataque fue realizado por un suscriptor que creó 20 cuentas y

lanzó una instancia de máquina virtual por cada una de ellas, a su vez cada una de estas cuentas seguía creando 20 cuentas cada una haciendo que el crecimiento exponencial llevase los recursos a los límites de fallo.

- **Propiedad de los datos**

Cuando se establece un contrato con un proveedor se deben definir de forma clara los derechos sobre los datos y así crear un primer marco de confianza. Existe una controversia importante en torno a los términos ambiguos que utilizan las redes sociales en sus políticas de privacidad y propiedad de los datos. El contrato debe establecer de una forma clara que la organización mantiene la propiedad de todos sus datos, pero también debe asegurar que el proveedor no adquiere derechos o licencias a través de los acuerdos para usar los datos en su propio beneficio.

- **Servicios complejos**

Los servicios *cloud* en sí mismos suelen estar formados por la colaboración y unión de otros servicios. El nivel de disponibilidad de un servicio *cloud* depende de la disponibilidad de los servicios que lo componen. Aquellos servicios que dependan de terceros para su funcionamiento deben considerar el establecimiento de un marco de control con dichos terceros para definir las responsabilidades y las obligaciones, así como los remedios para los posibles fallos.

Las garantías de responsabilidad y rendimiento pueden convertirse en un problema serio en servicios complejos. Un ejemplo de esto es una red social que suscribía servicios de almacenamiento en la nube y cerró por perder el acceso a gran cantidad de datos de 20.000 suscriptores. El problema fue que los datos antiguos, las nuevas aplicaciones y las bases de datos se encontraban en diferentes proveedores de servicios *cloud*.

- **Visibilidad**

La migración a servicios *cloud* públicos cede el control de los sistemas de seguridad a los proveedores que operan los datos de la organización. La administración, los procedimientos y los controles usados en el *cloud* deben guardar cierta analogía con los implantados en la propia organización interna para evitar posibles agujeros de seguridad.

Los proveedores de *cloud* suelen ser bastante celosos para dar los detalles de sus políticas de seguridad y privacidad, ya que dicha información podría ser utilizada para realizar un ataque. Por lo general, los detalles de la red y los niveles de monitorización de los sistemas no forman parte de los acuerdos de servicio.

La transparencia de la forma en la que los proveedores operan es un asunto vital para la supervisión de los sistemas de seguridad y privacidad de una organización. Para

asegurar que las políticas se cumplen durante el ciclo de vida de los sistemas, los acuerdos de servicio deben incluir algunas cláusulas para obtener visibilidad de los controles de seguridad y los procesos empleados por los proveedores. Lo ideal sería que la organización tuviese el control sobre ciertos aspectos tales como la definición de los límites que lanzan alertas, los niveles de detalle de los informes, etc. para que se adecúen a las necesidades de la empresa.

- **Gestión de riesgos**

Con los servicios basados en *cloud* muchos componentes de los sistemas de información quedan fuera del control directo de la organización suscriptora. Mucha gente se siente mejor con un riesgo siempre y cuando tengan mayor control sobre los procesos y los equipos involucrados. La gestión de riesgos es el proceso de identificar y valorar los riesgos realizando los pasos necesarios para reducirlos a un nivel asumible. Los sistemas *cloud* públicos requieren, al igual que los sistemas tradicionales, que los riesgos sean gestionados a lo largo de su ciclo de vida.

Valorar y gestionar riesgos en sistemas que utilizan servicios *cloud* puede llegar a ser un desafío. Para llevarlo a la práctica, la organización debe confirmar que los controles de seguridad están implementados correctamente y cumplen con los requisitos de seguridad de la empresa. El establecimiento de un nivel de confianza depende del grado de control que una organización esté dispuesta a delegar en el proveedor para que sea éste el que implemente los controles de seguridad necesarios para la protección de los datos y las aplicaciones de la organización, así como las pruebas de la efectividad de dichos controles.

Si el nivel de confianza baja por debajo de las expectativas y la organización no puede aplicar medidas correctivas, ésta debe decidirse entre la aceptación de un riesgo mayor o el rechazo del servicio.

3.3.4. Arquitectura

La arquitectura de una infraestructura *cloud* comprende tanto *hardware* como *software*. Las máquinas virtuales se utilizan como unidades de distribución del *software* asociadas a dispositivos de almacenamiento. Las aplicaciones son creadas mediante las interfaces de programación. Suelen englobar a múltiples componentes de la infraestructura que se comunican entre sí a través de estas interfaces. Esta comunicación global de la infraestructura puede derivar en fallos de seguridad.

- **Superficie de ataque**

El hipervisor de las máquinas virtuales se superpone como una capa extra de software entre el sistema operativo y los recursos hardware y se utiliza para ejecutar las máquinas virtuales multiusuario. La inclusión de estos hipervisores supone añadir un punto de ataque extra con respecto a las arquitecturas tradicionales.

Son ejemplos de posibles incidentes la revelación de datos sensibles al realizar la migración de máquinas virtuales o la ejecución de código arbitrario en el equipo anfitrión al explotar vulnerabilidades en productos de virtualización.

- **Protección de la red virtual**

La mayoría de los productos de virtualización soportan la creación de conmutadores de red virtuales y configuraciones de red como parte del entorno. Así mismo, soportan la creación de subredes privadas para la comunicación entre las maquinas virtuales alojadas en un mismo servidor. Este tráfico no puede ser monitorizado por los elementos físicos típicos de la red (cortafuegos, sistemas de prevención de intrusiones, etc.). Por ello, se deben extremar las precauciones de la seguridad de la red en estas conexiones internas para evitar ataques desde dentro de estas redes virtuales.

- **Datos auxiliares**

Lo más normal es que la seguridad en estos entornos se centre en los datos que gestiona la aplicación, pero también existen otros datos no considerados tan críticos cuya alteración, robo o revelación puede producir serios incidentes de seguridad (por ejemplo: bases de datos de clientes, ficheros de pagos, información de usuarios, etc.).

Otro de los problemas puede producirse al no proteger el acceso a los repositorios de las plantillas de las máquinas virtuales que contienen las configuraciones por defecto de las mismas. Compartir este tipo de datos es una práctica bastante común en entornos *cloud*.

Compartir este tipo de datos puede ofrecer al atacante plataformas para preparar su ataque comprobando las vulnerabilidades que pueden ser inherentes a las mismas, aunque también puede existir el proceso contrario: atacantes que intenten reemplazar una imagen por otra con contenido malicioso instalado.

- **Protección del cliente**

Los navegadores, como parte primordial de los entornos *cloud* (ya que típicamente los accesos se realizan vía web), pueden llevar extensiones o *plugins* con importantes brechas de seguridad.

Mantener la seguridad lógica y física de la parte del cliente puede ser complicado especialmente para entornos móviles ya que, por su tamaño y portabilidad, pueden perderse o ser sustraídos. Así mismo, los sistemas de escritorio no son actualizados de forma sistemática provocando que las vulnerabilidades puedan producir brechas de seguridad importantes.

Otro aspecto a tener en cuenta es la posible presencia de troyanos, puertas traseras o virus que puedan obtener información confidencial o monitorizar a la víctima.

La solución podría partir por reforzar la comprobación de seguridad de los clientes. Por ejemplo, los bancos empiezan a desarrollar medidas para que los navegadores de sus clientes aseguren los datos mediante el cifrado de las comunicaciones y aplicando mecanismos para evitar la intercepción de las pulsaciones de teclado.

- **Protección del servidor**

Los servidores en los entornos *cloud* deben ser protegidos tanto física como lógicamente, de forma que los mismos estén segmentados y separados para que no se puedan producir accesos desde zonas no autorizadas.

Del mismo modo, en la parte del cliente hay que asegurar el parcheo de los servidores para que no tengan vulnerabilidades que comprometan la seguridad del entorno.

Otro aspecto importante en la protección de la parte servidora es la disponibilidad, por lo que será recomendable disponer de sistemas que gocen de ésta, principalmente en aquellos servidores que alojen partes críticas de la infraestructura.

3.3.5. Identidad y control de acceso

Los datos sensibles y la privacidad se han convertido en la principal preocupación en lo que respecta a la protección de las organizaciones y el acceso no autorizado a los recursos de información. La alternativa de usar dos métodos de autenticación, uno para la organización interna y otro para los clientes, puede llegar a ser algo muy complicado. La identidad federada, que se ha vuelto popular con el crecimiento de las arquitecturas orientadas a servicios, puede ser una de las soluciones, pudiendo ser implementada de varias formas siguiendo el estándar SAML (del inglés, *Security Assertion Markup Language*) o el estándar OpenID.

- **Autenticación**

Un número creciente de proveedores de servicios c*loud* soportan el estándar *SAML*, utilizándolo para administrar usuarios y autenticarlos previamente a conceder el acceso a las aplicaciones y datos. Este estándar proporciona un entorno para el intercambio de información para la autenticación entre dominios cooperantes. Las solicitudes y respuestas en este estándar son mapeadas mediante el protocolo *SOAP* (del inglés, *Simple Object Access Protocol*). Los mensajes *SOAP* se firman digitalmente.De esta forma, cuando un usuario dispone de un certificado de clave pública para un entorno *cloud* su clave privada puede ser utilizada para firmar las peticiones *SOAP*.

La validación de una autenticación mediante mensajes *SOAP* es complicada y debe tratarse con cuidado para evitar posibles ataques. Por ejemplo, ya se demostró el éxito de ataques del tipo *XML Wrapping* contra infraestructuras *cloud*. Este tipo de ataques manipulan las peticiones *SOAP* mediante la introducción de envolturas en la cabecera de seguridad *SOAP*, se mueve el cuerpo a dicha envoltura y se sustituye el cuerpo con uno que ejecuta una acción definida por el atacante. Como el mensaje original no se borra, la firma se verifica pero se realiza la ejecución de la acción maliciosa.

- **Control de Acceso**

El estándar *SAML* por sí solo no es suficiente para proporcionar tanto autenticación como controles de acceso en servicios *cloud*. Se hace necesario implementar también un control

de acceso a los recursos. Para ello se puede utilizar el estándar *XACML* (del inglés, *eXtensible Access Control Markup Language*) para controlar los accesos a los recursos. Este estándar complementa *SAML* para entornos de intercambio de autenticación y autorización entre dominios cooperantes. No obstante, los mensajes entre entidades *XACML* pueden ser susceptibles de ataques por parte de terceros, por lo que hay que protegerlos frente a ataques de exposición de la información, repetición, borrado y modificación.

3.3.6. Aislamiento de Software

Para alcanzar tasas altas de eficiencia, los proveedores deben asegurar tanto una provisión dinámica del servicio como el aislamiento de los suscriptores del servicio. La concurrencia de usuarios es realizada en entornos *cloud* mediante la multiplexación de la ejecución de las máquinas virtuales para los diferentes usuarios en un mismo servidor físico. Aún así, las aplicaciones que corren en dichos entornos permiten ser focos de ataque. Las más destacadas son:

- **Complejidad del hipervisor**

  La seguridad de un sistema de computación depende de la calidad del *software* que se ejecuta en su núcleo, el cual controla la ubicación y ejecución de los procesos. Un monitor de máquinas virtuales está diseñado para ejecutar múltiples máquinas de forma concurrente en un mismo anfitrión físico proporcionando aislamiento entre las diferentes máquinas virtuales.

  Normalmente estos hipervisores son menos complejos que un sistema operativo, por lo que el análisis y la mejora de la seguridad es, en teoría, más sencillo. La realidad es que la evolución de estos hipervisores los ha convertido en elementos mucho más complejos y amplios, similares a sistemas operativos. Un caso claro de esto es Xen que contiene un núcleo de Linux modificado para aislar las operaciones de entrada/salida e incluye *KVM* (del inglés, *Kernel-based Virtual Machine*), de forma que transforma el núcleo de Linux e un hipervisor.

  Resulta importante para el proveedor entender el uso de la virtualización para poder comprender los riesgos asociados que pueden producirse.

- **Vectores de ataque**

  La concurrencia de múltiples usuarios compartiendo recursos físicos mediante diferentes máquinas virtuales puede producir nuevas fuentes de amenazas. Una de las principales amenazas es la posibilidad de que códigos maliciosos puedan salir de las máquinas virtuales e interferir con el hipervisor o con otras máquinas virtuales. La posibilidad de la migración en caliente de las máquinas virtuales de un servidor físico a otro, y otras funcionalidades que aportan los hipervisores para facilitar la gestión, aumentan el tamaño y la complejidad del software y por ende añade nuevas zonas para realizar ataques.

La interfaz de programación de los servicios *cloud* suele ser objetivo común para descubrir vulnerabilidades que se pueden explotar. Este tipo de vulnerabilidades suelen ser desbordamientos de *buffer*, que permiten al atacante la ejecución de código arbitrario o fallos que permiten realizar denegaciones de servicio que puedan afectar a la máquina virtual o al propio servidor anfitrión.

También pueden darse ataques indirectos, como los demostrados por algunos desarrolladores, sobre una debilidad en el proceso de migración de máquinas virtuales que permitía a un atacante obtener control administrativo de la máquina mediante un ataque *man-in-the-middle* para modificar el código de autenticación.

Por otra parte, las modificaciones de memoria durante la migración que permiten la instalación de rootkits específicos para máquinas virtuales pueden suponer otro vector de ataque.

Otra opción puede ser la monitorización del uso de recursos en un servidor compartido para recopilar información y, de esa forma, poder obtener información de cuándo es el mejor momento para la realización de un ataque.

3.3.7. Protección de datos

Los datos que se almacenan en entornos *cloud* suelen residir en equipamiento compartido por múltiples clientes. Por ello, las organizaciones que gestionan datos confidenciales en la nube deben preocuparse por la forma en que se accede a estos datos y garantizar que los mismos estén almacenados de forma segura.

- **Aislamiento de datos**

Los datos en los entornos *cloud* pueden tomar muchas formas dependiendo de la actividad a la que se dediquen Si, por ejemplo, la actividad es el desarrollo de aplicaciones, los datos se encontrarán en forma de programas, *scripts* y datos de configuraciones. En cambio, si en la plataforma reside una aplicación ya desarrollada, los datos serán del tipo registros, contenidos creados y usados por la aplicación o información de los usuarios, etc.

Uno de los principales problemas de los entornos *cloud* es la autenticación de la identidad de los usuarios. Los controles de acceso se basan habitualmente en comprobar la identidad.

Un caso particular son los entornos típicos de bases de datos de los entornos *cloud* que se componen de un único sistema gestor de bases de datos con una instancia por máquina virtual. La seguridad y configuración de estas instancias recae en la parte suscriptora del servicio. La segregación de los datos se suele realizar mediante etiquetas para los datos, lo cual proporciona una falsa apariencia de uso exclusivo de las instancias.

Por otra parte, los datos deben ser protegidos cuando se encuentran en descanso, en tránsito. Asimismo, el acceso a los datos debe ser controlado. Los estándares de

comunicaciones y los certificados de clave pública permiten que las transferencias de datos se puedan proteger utilizando criptografía. La seguridad en descanso no es tan sencilla porque los procedimientos no son claros debido a que la mayoría de los sistemas son propietarios, lo cual, a su vez, dificulta la interoperabilidad entre distintos proveedores con sistemas diferentes.

La gestión de las claves criptográficas recae principalmente en el suscriptor del servicio. La generación de estas claves se suele realizar utilizando módulos de seguridad hardware o *HSM (*del inglés*, Hardware Security Module*).

La protección de datos en uso es un área emergente de la criptografía con poco material práctico que ofrecer, dejando que los mecanismos de confianza sean la mayor salvaguarda.

- **Saneamiento de datos**

Saneamiento es la eliminación de datos sensibles de un medio de almacenamiento cuando éste deja de ser utilizado en el entorno o se quiere reutilizar en otro entorno o situación. El saneamiento también aplica a los datos de las copias de seguridad y a los datos residuales que quedan cuando el servicio finaliza.

En entornos *cloud* esta labor puede ser muy complicada ya que los datos de varios clientes comparten almacenamiento por lo cual el saneamiento se debe realizar con gran cautela. Además, mediante técnicas y equipamiento específico, se pueden recuperar datos de medios de almacenamiento previamente borrado, lo cual convierte este saneamiento en una tarea crítica.

3.3.8. Disponibilidad

La disponibilidad puede ser interrumpida de forma temporal o permanente. Los ataques de denegación de servicio, fallos del equipamiento y desastres naturales son todas amenazas a la disponibilidad.

- **Fallos temporales**

A pesar de utilizar infraestructuras orientadas para dar un alto nivel de servicio y una alta disponibilidad, los servicios *cloud* pueden experimentar descensos en el rendimiento o fallos.

Algunos ejemplos de esto son:

  - Febrero 2008: fallos de un servicio de almacenamiento en la nube por un periodo de tres horas que afectó a sus suscriptores, entre ellos Twitter y otras compañías.
  - Febrero 2010: Gmail sufre una pérdida de acceso a 500.000 cuentas por una actualización de software; alguna de las cuentas se restauraron mediante copias de seguridad en cinta.

Con una fiabilidad del 99,95% se producirían 4,38 horas de caída en un año, excluyendo las paradas de mantenimiento, que no se recogen en los acuerdos de nivel de servicio o

SLA (del inglés, *Service Level Agreement*). Los tiempos de recuperación en caso de fallo o pérdida de servicio deben estar recogidos por el proveedor en sus planes de contingencia y continuidad. Así mismo, deben disponer de infraestructuras de respaldo para poder prestar un servicio mientras se prolonga el periodo de recuperación. Otra opción es tener un acuerdo para que otro proveedor procese los datos mientras se realiza la restauración del servicio.

- **Fallos prolongados y permanentes**

Esta posibilidad puede darse en proveedores que experimentan problemas serios como la bancarrota o la pérdida de sus proveedores.

Algunos ejemplos de esto son:

  - Abril 2009: el FBI realiza una intervención en un proveedor *cloud* para llevar a cabo una investigación en un centro de datos en Texas. Los agentes tuvieron que retirar cientos de servidores para investigar unas acusaciones de fraude de empresas que operaban en dicho centro. La pérdida de estos servidores supuso una interrupción del servicio para otros suscriptores de los servicios.

- **Denegación de servicio**

Los ataques de denegación de servicio consisten en saturar el objetivo con multitud de peticiones para que, al alcanzar los límites de operación óptimos, comience a no atender las peticiones legítimas. La forma más común de realizar estos ataques es utilizar múltiples equipos o a través de redes de equipos zombis.

Aunque los ataques no resulten efectivos, un intento de denegación de servicio produce rápidamente un alto consumo de recursos para realizar la defensa. La distribución dinámica de recursos en los entornos *cloud* facilita la labor a los atacantes, los cuales, utilizando suficientes equipos en los ataques, pueden producir largos periodos de saturación.

Estos ataques también pueden producirse contra los servicios accesibles de forma interna, como aquellos que gestionan la infraestructura.

- **Valor concentrado**

Actualmente las infraestructuras en la nube comienzan a ser objetivo de los ataques porque, en cierto modo, concentran gran cantidad de información sensible, de forma que, con un único ataque, se podría obtener mayor «rendimiento» que realizando varios a infraestructuras más pequeñas.

Se puede acceder de forma más refinada a la infraestructura con la ingeniería social, consiguiendo las credenciales de acceso de los administradores del entorno. Esto se debe a que habitualmente es posible la recuperación de contraseñas mediante el envío

de las mismas al correo electrónico, por lo cual, controlando la cuenta de un usuario, se obtendría de forma sencilla la autenticación.

3.3.9. Respuesta a incidentes

La labor del proveedor es básica en las actividades de respuesta ante la ocurrencia de algún incidente de seguridad. Esto incluye la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio.

La colaboración entre los proveedores y los suscriptores para la detección y reconocimiento de los incidentes es esencial para la seguridad y la privacidad en *cloud computing*, ya que la complejidad de los servicios puede dificultar la labor de la detección. Se hace necesario entender y negociar los procedimientos de respuesta a incidentes antes de firmar un contrato de servicio. La localización de los datos es otro aspecto que puede impedir una investigación, por lo que es otro de los puntos que se deben negociar en los contratos.

La solución que se negocie ha de tener la finalidad de mitigar el incidente en un tiempo que limite los daños y que mejore los tiempos de recuperación. Los equipos para la resolución deberían ser mixtos (proveedor y suscriptor) ya que la solución puede involucrar a alguna de las partes de forma individual o a ambas conjuntamente y el incidente puede incluso afectar a otros suscriptores que comparten la infraestructura.

3.4. RECOMENDACIONES DE SEGURIDAD SEGÚN NIST

Según el informe del NIST, estás son las buenas prácticas generales por área.

Área	Recomendación
Gobernanza	Implantar políticas y estándares en la provisión de servicios *cloud*. Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.
Cumplimiento	Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos *cloud.* Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.
Confianza	Incorporar mecanismos en el contrato que permitan controlar los procesos y controles de privacidad empleados por el proveedor.
Arquitectura	Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y

	seguridad de los controles técnicos.
Identidad y control de acceso	Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso.
Aislamiento de software	Entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados
Disponibilidad	Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.
Respuesta a incidentes	Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización.

4. CONCLUSIONES

El hecho de que los entornos *cloud* proliferen de forma exponencial obliga a los posibles usuarios a comprender mejor estos entornos y sus principales problemáticas. El termino *cloud computing* es amplio y su definición poco precisa. Por ello, a la hora de la elección de servicios *cloud* se ha de tener claro el tipo de infraestructura que lo soporta y el tipo de servicio que se ofrece.

Tras el análisis realizado en este informe se obtiene una visión global de esta problemática y se extraen conclusiones comunes a todos los puntos de vista.

La **seguridad y la propiedad de los datos** es uno de los aspectos clave. Los informes muestran una gran preocupación por la propiedad y el tratamiento de los datos dado que estas infraestructuras pueden gestionar los datos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados. También se plantea que estos entornos, al manejar gran cantidad de datos, pueden ser objeto de fugas de información, ya sean intencionadas o fortuitas.

El **cumplimiento normativo** también es uno de los pilares de la seguridad en entornos *cloud.* En este caso el problema se presenta debido a la falta de transparencia de estas infraestructuras, por lo que es muy recomendable que el suscriptor del servicio se informe claramente de cómo se gestiona el entorno.

Para la creación de un servicio *cloud* interviene multitud de software de distintos proveedores. Es decir, son **entornos complejos** por lo que se ha de poner especial atención a las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado.

Otro de los aspectos considerados importantes es la **identidad y el control de acceso**. Por lo general, la mayoría de las infraestructuras son compartidas por múltiples empresas o usuarios y la mala definición de los controles de acceso puede provocar accesos no autorizados a datos confidenciales. La definición de una buena política de identidad y control de acceso basada en políticas de mínimo privilegio es esencial en entornos *cloud*.

Por último, existe un denominador común a todos estos aspectos mencionados. Se trata de los **contratos de acuerdo de servicio**. Todas las recomendaciones en cuanto a este asunto indican que éstos deben de ser revisados y creados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de recuperación del servicio, etc.

5. GLOSARIO

API: Interfaz de programación de aplicaciones, del inglés, *Application Programming Interface).*

BBDD: Bases de datos.

CPU: Unidad central de proceso del inglés, *Central Process Unit.*

CSA: Organización internacional *Cloud Security Alliance.*

GPU: Unidad de procesamiento de gráficos, del inglés *Graphics Process Unit.*

IaaS: Infraestructura como servicio o *SaaS*, del inglés *Infrastructure as a Service*).

NIST: Instituto Nacional de Estándares y Tecnologías (Estados Unidos) de inglés, *National Institute of Standards and Technologies*).

OpenID: Estándar de identificación digital descentralizado con el que un usuario puede identificarse en una página web a través de una *URL* (o un *XRI* en la versión actual) y puede ser verificado por cualquier servidor que soporte el protocolo.

PaaS: Plataforma como servicio o *SaaS*, del inglés *Platform as a Service*).

SaaS: Software como Servicio o *SaaS*, del inglés *Software as a Service*).

SAML: Lenguaje de marcado de declaración de seguridad del inglés, *Security Assertion Markup Language.* Estándar abierto basado en XML para el intercambio de información de autenticación y autorización entre dominios de seguridad.

SLA: Acuerdo de nivel de servicio, del inglés *Service Level Agreement*.

SOAP: Protocolo simple de acceso de objetos, del inglés, *Simple Object Access Protocol*.Protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos *XML*.

URL: Localizador uniforme de recursos, del inglés *Uniform Resource Locator.*

XACML: Lenguaje de marcado de control de acceso extensible, del inglés, *eXtensible Access Control Markup Language.* Estándar que implementa un lenguaje de políticas de control de acceso, implementado en XML, y un modelo de proceso que describe cómo interpretar dichas políticas.

XML: Lenguaje de marcas extensible, del inglés *eXtesible Markup Language.*

XRI: Identificador de recursos extensible del inglés, *Extensible Resource Identifier.*

6. REFERENCIAS

Los documentos en los que se basa este informe son:

- CSA, 2010, Top Threats to Cloud Computing V1.0
- Gartner, 2008, Assessing the Security Risks of Cloud Computing
- NIST, 2011, Guidelines on Security and Privacy in Public Cloud Computing

Otros documentos de referencia:

- ENISA, 2011, SWOT analysis, Risk Assessment (Public Administration) and Privacy
- ENISA, 2009, Computer Assurance
- ENISA, 2009, Risk Assessment
- CSA, Security Guidance
- CSA, Identity and Access Management:
- World Privacy Forum Report