AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad en la nube

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-1379-120120*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*20/01/2011*
N° de Páginas	*1 de 20*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía una aproximación al paradigma de "computación en la nube" o "cloud computing" centrándonos en las principales implicaciones en cuanto a seguridad y privacidad.

3 ALCANCE

El documento va destinado al personal de la Junta de Andalucía y público en general.

4 INTRODUCCIÓN

"Los servicios bajo modelo Cloud, tienen que beneficiarse de todas las garantías con las que cuentan el resto de servicios, como la seguridad y la continuidad de servicio."

La nube es Internet. La computación en la nube es la computación en Internet y eso quiere decir que **todas las aplicaciones y datos que están en la nube, están en Internet**, fuera de nuestras máquinas, en las máquinas del proveedor de servicios.

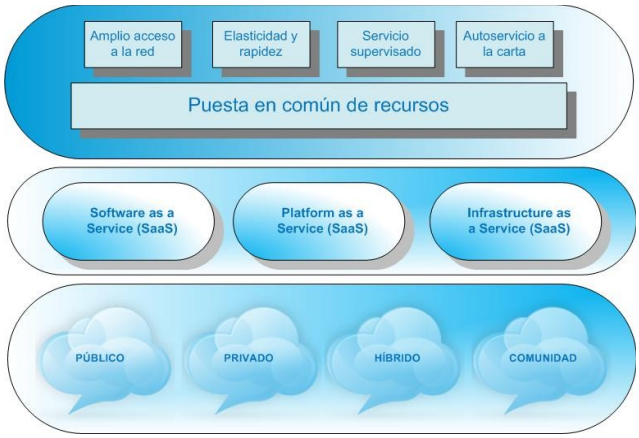
A esto es básicamente a lo que nos referimos cuando hablamos de **cloud computing** o **computación en la nube**. Un paradigma que permite ofrecer servicios de computación a través de Internet.

La CSA (Cloud Security Alliance) define formalmente los entornos de cloud computing de la siguiente manera:

> *"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."*

Este modelo consta de:

- 5 características esenciales.
- 3 modelos de servicio.
- 4 modos de despliegue.



4.1 Las 5 características del Cloud computing

- **Acceso ubicuo a los datos**

La principal característica del cloud computing es el acceso ubicuo (desde cualquier lugar) a los datos. Solo se necesita un navegador web y conexión a Internet para disfrutar de los servicios en la nube, no hace falta tener un sistema operativo determinado o instalar un software específico en cada cliente. Se puede utilizar un portátil, un teléfono móvil o una tablet conectada a la Red para acceder a las aplicaciones de la nube en cualquier momento.

Actualmente, las tecnologías móviles son una parte importante dentro del modelo de negocio de una empresa. La combinación de dispositivos móviles y fijos crea nuevas oportunidades en el desarrollo de la actividad empresarial permitiendo plena operatividad.

Esta característica supone una gran ventaja frente a otras tecnologías, aunque es importante puntualizar que existen limitaciones, por ejemplo, no es posible utilizar las aplicaciones en la nube si no hay conexión a Internet. Además, la calidad y la velocidad de la conexión deben ser altas para poder utilizar el servicio de forma correcta. Por norma general, las aplicaciones de escritorio (aquellos programas que están instalados en un ordenador) tienen un rendimiento mayor que las aplicaciones web debido a que aprovechan mejor todos los recursos del equipo.

- **Reducción de costes**

A la hora de desplegar un nuevo servicio, el modelo informático basado en cloud computing permite reducir costes con respecto al modelo tradicional, ya que los recursos que la entidad debe destinar son menores, tanto directos (en cuanto a hardware, mantenimiento, personal, etc.) como indirectos (instalaciones, suministros, etc.), de tal forma que parte de los costes fijos pasan a ser variables.

A la vez, las entidades pueden contratar un servicio en la nube por una cantidad al mes y en función de cómo evolucionen sus necesidades, aumentar o disminuir los recursos de procesamiento, sabiendo que se va a pagar por uso efectivo.

- **Escalabilidad y flexibilidad**

La sencillez con la que se pueden añadir o eliminar recursos también supone una ventaja frente al modelo tradicional. Fuera de la nube, cuando un administrador del sistema necesita instalar una unidad de disco duro adicional, debe elegir el producto y seguir un protocolo para realizar la compra, recibir, instalar y configurar el equipo para su puesta a punto. Si transcurrido un tiempo el volumen de usuarios desciende o varían las funcionalidades del sistema, ya no se podrá dar marcha atrás.

Debido a la gran escalabilidad y flexibilidad del cloud computing, todos los proveedores de servicios ofrecen la posibilidad de añadir o eliminar recursos en cuestión de minutos, aumentando el almacenamiento o el número de procesadores sin que la aplicación se vea afectada. No hay que instalar nada en el sistema operativo, ni configurar unidades de hardware adicionales. Del mismo modo, si pasado un tiempo se detecta que el servicio en la nube no requiere tanta capacidad de procesamiento, se pueden disminuir sus recursos para adecuarlos al volumen de trabajo necesario en cada momento.

- **Deslocalización de datos y procesos**

En un sistema informático tradicional, el administrador del sistema conoce en qué máquina se almacena cada dato y qué servidor es el encargado de cada proceso. El modelo en la nube hace uso de distintas tecnologías de virtualización para poder ofrecer todas las funcionalidades necesarias, por lo que se pierde el control sobre la localización. Esto no significa que los datos o procesos estén perdidos en Internet, puesto que el cliente mantiene el control sobre quién es capaz de acceder o modificar esta información.

La ventaja es que se pueden llevar tanto los datos como los procesos al lugar más conveniente para la organización. Por ejemplo, se pueden utilizar múltiples copias de un servidor y repartidlas por centros de proceso de datos en distintos puntos del planeta para mejorar los tiempos de acceso de los usuarios. Además, facilita el mantenimiento de copias de seguridad no sólo de los datos sino del servidor entero, del sistema operativo y los programas instalados en él.

La localización de los datos puede incidir significativamente en el régimen jurídico aplicable y en las condiciones del contrato. En determinados casos podría requerirse cumplir con los requisitos previstos para las transferencias internacionales de datos personales.

- **Dependencia de terceros**

Tanto si se trabaja con una nube pública como con una nube híbrida, existirá una empresa contratada para proveer los servicios necesarios. Los beneficios de contar con estas empresas es que se encargan de todo el mantenimiento del hardware, recintos especializados para los centros de procesamiento de datos, suministro eléctrico y conectividad a Internet, etc.

Los proveedores de servicio en la nube no sólo hospedan un servidor web (como ocurre en el hosting tradicional), sino también todos los procesos y datos que están en la nube, además de las copias de seguridad. Es decir, que comparten parte de su control con el usuario u organización.

El establecimiento de un nivel adecuado de transparencia en el mercado a la hora de negociar los términos y condiciones en los contratos es fundamental para contrarrestar la falta de control derivada de la dependencia de terceros.

4.2 Los 3 modelos de servicio

El servicio ofrecido por el cloud computing puede agruparse en tres capas:

- SaaS: Software as a Service / Software como servicio
- PaaS: Platform as a Service / Plataforma como servicio
- IaaS: Infrastructure as a Service / Infraestructura como servicio

- **SaaS - Software como servicio**

Este nivel se encarga de entregar el software como un servicio a través de Internet siempre que lo demande el usuario. Se trata del nivel más bajo que permite el acceso a la aplicación utilizando un navegador web, sin necesidad de instalar programas adicionales en el ordenador o teléfono móvil. Las suites ofimáticas a las que se puede acceder online son un buen ejemplo de este nivel.

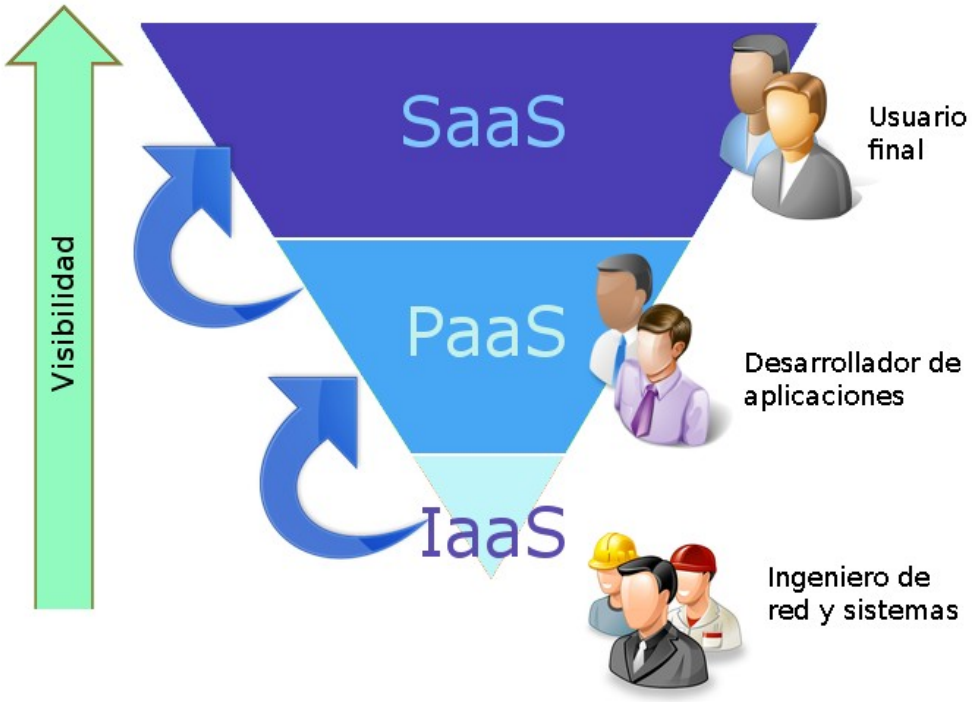
- **PaaS – Plataforma como servicio**

Se trata del nivel intermedio, se encarga de entregar una plataforma de procesamiento completa al usuario, plenamente funcional y sin tener que comprar y mantener el hardware y software. Por ejemplo, un desarrollador web necesita un servidor web que sirva sus páginas, un servidor de bases de datos y un sistema operativo. Este nivel se encarga de proporcionar todos estos servicios.

- **IaaS – Infraestructura como servicio**

Se trata del nivel más alto de servicio. Se encarga de entregar una infraestructura de procesamiento completa al usuario bajo demanda. El usuario dispone de una o varias máquinas virtuales en la nube con las que, por ejemplo, puede aumentar el tamaño de disco duro en unos minutos, obtener mayor capacidad de proceso o enrutadores y pagar solamente por los recursos que utilice. Este nivel

puede ser visto como una evolución de los Servidores Privados Virtuales que ofrecen actualmente las empresas de hosting.
A continuación se muestra un gráfico que nos permitirá visualizar estos conceptos.



4.3 Los 4 modos de despliegue

- **Nube pública**:
  Es aquella en la que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

- **Nube privada**:
  Creadas y administradas por una única entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.

- **Nube híbrida**
  En ésta coexisten los dos modelos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada. De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

- **Nube comunitaria**
  Es compartida entre varias organizaciones que forman una comunidad con principios similares (misión, requerimientos de seguridad, políticas y cumplimientos normativos). Puede ser gestionada por la comunidad o por un tercero. Este modelo puede ser visto como una variación en el modelo de cloud privada.

5 PRINCIPALES RIESGOS DEL CLOUD COMPUTING

- **Abuso y uso malintencionado**

El cloud computing ofrece un gran número de ventajas y oportunidades que también están siendo aprovechadas por los ciberdelincuentes. Ataques como el robo de contraseñas, envío de spam o ataques de denegación de servicio distribuido (DDoS) se vuelven mucho más sencillos y baratos a través de la nube.

Los ciberdelincuentes pueden planear sus ataques contratando servicios en la nube para posteriormente ejecutarlos en cuestión de horas. Además, los recursos que utilicen se borrarán una vez concluya el ataque, lo que dificulta mucho su seguimiento.

Del mismo modo, pueden contratar servicios de almacenamiento en la nube para guardar datos maliciosos o robados. De esta forma, dificultan que las autoridades puedan acceder a esta información (por la complejidad que supone) para actuar contra los atacantes.

- **Interfaces y APIs inseguras**

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. Las APIs suelen ser el único punto de interacción con los programas que se están ejecutando en la nube. Al ser las puertas de entrada hacia los servicios en la nube, se convierten en un punto crítico de la seguridad y privacidad del sistema.

Cada proveedor de servicios en la nube ofrece sus propias APIs de conexión que permiten desde arrancar o parar los servicios en la nube hasta aumentar o disminuir los recursos de los mismos.

Sin una correcta política de seguridad, las APIs pueden sufrir ataques de malware para que realicen acciones adicionales o diferentes para las que originalmente fueron programadas. Con ello, los atacantes persiguen el robo y/o acceso a la información de la víctima.

- **Amenazas internas**

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. Algunas de estas medidas pasan por incorporar cláusulas de confidencialidad en los contratos laborales o el establecimiento de políticas de seguridad.

- **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.

En esta línea se debe prestar especial atención al aislamiento necesario de la información de diferentes usuarios en una misma infraestructura. Ante esto, los proveedores de servicios cloud deben mantener sus esfuerzos para asegurar un servicio sin fisuras en el que cada usuario tenga acceso únicamente a su propia información.

- **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.

Para evitar esta situación es recomendable proteger el tránsito de datos mediante el cifrado de los mismo y usar métodos robustos de control de acceso.

- **Suplantación de identidad**

La suplantación de la identidad es un riesgo presente tanto en los sistemas informáticos tradicionales como en el modelo de cloud computing. Sin embargo, tiene una especial relevancia en éste último.

En la mayoría de los sistemas informáticos es necesario identificarse antes de realizar cualquier tarea. Habitualmente, esta identificación se produce mediante la combinación del nombre de usuario y una clave secreta o password.

Dependiendo del uso que se esté haciendo del cloud computing, esta combinación tradicional de usuario y contraseña puede no resultar lo suficientemente robusta. Es necesario investigar otros sistemas mucho más seguros para evitar la suplantación de identidad en la Red.

Una solución para incrementar la seguridad es la utilización del DNI electrónico como mecanismo de identificación,

ya que incluye medidas criptográficas y biométricas como complemento a las tradicionales medidas de seguridad.

- **Desconocimiento del perfil de riesgo**

La gestión de la seguridad en los entornos informáticos tradicionales se ha estudiado durante mucho tiempo. Es relativamente sencillo aplicar soluciones informáticas para aumentar la seguridad, dificultando las entradas no autorizadas o disminuyendo las vulnerabilidades del sistema.

Sin embargo, el cloud computing entraña una evolución no conocida anteriormente. Ofrece nuevas funcionalidades e incrementa las oportunidades de negocio, pero a su vez es un modelo que puede ser explotado por nuevas amenazas en la Red.

Esto no significa que sea menos seguro que los modelos anteriores, simplemente que hay menos experiencia de ataques y los expertos en seguridad estudian los nuevos "modus operandis" de los usuarios malintencionados a la vez que los posibles fallos de diseño.

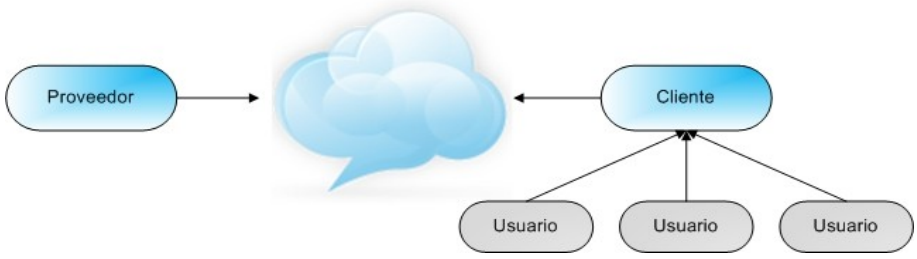
6 MODELO DE SEGURIDAD DEL CLOUD COMPUTING

Al hacer uso del cloud computing, una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.

Para entender el modelo de seguridad de la información aplicado en este modelo es necesario conocer los distintos actores que participan en él:

- **Proveedor de servicios en la nube**: Empresa que dispone de la infraestructura informática necesaria para hospedar los programas siguiendo el modelo de cloud computing.
- **Cliente**: Persona, organización o empresa que contrata los servicios en la nube.
- **Usuario final**: Persona, organización o empresa que utiliza el servicio, programa o infraestructura en la nube.

Estos actores pueden ser entidades diferentes o ser la misma entidad. Por ejemplo, una empresa puede contratar servicios en la nube para hospedar un servidor web al que accederán sus empleados, como se muestra en la siguiente imagen.



Los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un trabajo colaborativo entre proveedor de servicios en la nube y cliente, ya que ambas deben asumir unas responsabilidades. La realización de auditorias de seguridad conjuntas es una buena práctica para revisar que todo el sistema está protegido frente a posibles amenazas.

6.1 Seguridad en el lado del proveedor

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos. Deberá impedir que personas no autorizadas entren en dichos edificios para, por ejemplo, robar sus equipos. Del mismo modo, deberá mantener sus equipos actualizados tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet.

El proveedor utiliza mecanismos como la virtualización y la segmentación de datos para reforzar la seguridad de sus servicios en la nube.

- La **virtualización** puede ser vista como una forma de aumentar la seguridad de los procesos que se ejecutan en la nube. Varias máquinas virtuales pueden ser ejecutadas en un único servidor pero cada máquina virtual ejecuta un sistema operativo de forma aislada. El espacio de memoria y disco están controlados por un *hipervisor* que impide que los procesos ejecutados en distintas máquinas virtuales puedan interactuar entre ellos.

  El mayor riesgo al que debe enfrentarse el proveedor de servicios en cuanto a este mecanismo es el control y eliminación del software malintencionado que pretenda burlar las protecciones del hipervisor para tener acceso a otras máquinas virtuales o incluso al sistema anfitrión.

- La **deslocalización** de los datos es una característica que también puede ser explotada como un mecanismo de seguridad en sí misma. La segmentación de datos permite que los datos de un cliente residan en diferentes servidores, incluso en diferentes centros de datos. De esta forma se protegen dichos datos frente a un hipotético robo en las instalaciones del proveedor de servicios.

  Además, al poder mantener los datos en varias localizaciones de forma simultánea, se dispone de un sistema de copias de seguridad prácticamente en tiempo real. Así, ante fallos de seguridad, se puede recuperar rápidamente la actividad, permitiendo la continuidad del negocio.

6.2 Seguridad en el lado del cliente

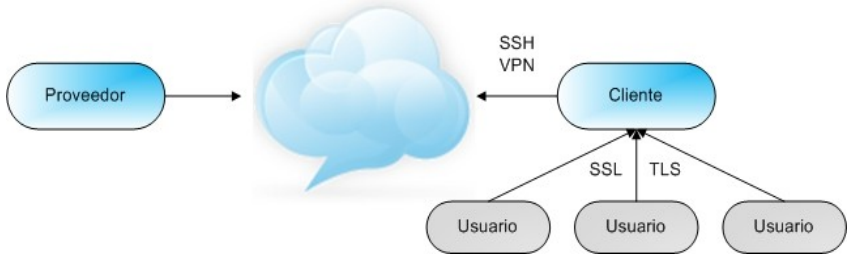
El cliente es responsable de mantener el sistema operativo actualizado e instalar los parches de seguridad que aparezcan. Igualmente es necesario mantener políticas de seguridad tradicionales como el control de usuarios, el borrado de cuentas de usuario que ya no se utilizan, o la revisión del software para comprobar que no tiene vulnerabilidades, entre otras.

Los mecanismos específicos que puede adoptar el cliente para reforzar la seguridad en la nube engloban el control perimetral, la criptografía y la gestión de logs o archivos de registro de eventos.

- **Control perimetral**. Para llevarlo a cabo, es recomendable la instalación y configuración de un firewall o cortafuegos, aplicación informática que se encarga de **controlar** todas las comunicaciones que se realizan desde o hacia el equipo o la red y decide si las permite dependiendo de las reglas establecidas por el administrador del sistema.

Igualmente recomendable es la instalación y configuración de un *IDS* para la monitorización de posibles intentos de intrusión.

- **Criptografía**. Proporciona un nivel superior de seguridad en tres aspectos principales:
  - Protección de las **conexiones de red entre los usuarios y las aplicaciones** en la nube. El uso de SSL y TLS permiten que todos los datos que viajen desde el servidor en la nube hasta el usuario estén cifrados impidiendo su acceso a terceras personas incluso cuando se utiliza una red Wi-Fi no segura.
  - Protección de las **conexiones entre los administradores del sistema y los servicios** de la nube. En este caso, el uso de SSH y VPN permitirá a los administradores del sistema o desarrolladores de las aplicaciones mantener una canal seguro de comunicación con los sistemas en la nube.



  - Protección de los **datos** utilizando criptografía. Si se utiliza la nube como un sistema de almacenamiento de datos es muy recomendable utilizar un nivel de cifrado adecuado para aquellos datos sensibles que vayan a ser depositados allí. De esta forma, si algún usuario no autorizado intercepta los datos o tiene acceso al sistema de ficheros de la nube, no podrá leer el contenido allí depositado sin conocer la clave de cifrado.
- **Gestión de logs**. Nos permite comprobar la actividad informática, detectar incidentes y formular un plan de acción para evitar que vuelvan a suceder en el futuro. Aunque es muy posible que no se tenga acceso a toda la información sobre los eventos del sistema, el cliente debe almacenar y revisar todos los logs que estén bajo su responsabilidad. Por ejemplo, el registro de usuarios que acceden a la aplicación, manipulan o borran ficheros en la máquina virtual, o el registro de conexiones potencialmente peligrosas detectadas por el IDS y por el cortafuegos.

  Además, es recomendable realizar copias de seguridad frecuentes de estos logs e incluso almacenarlos en una máquina distinta ya que si un atacante se hace con el control del sistema en la nube podría destruir los ficheros de registro borrando así sus huellas.

7 PRIVACIDAD EN LA NUBE

La información es el activo más importante de las organizaciones. Asegurar la privacidad de la información durante su ciclo de vida es crucial a la hora de utilizar servicios de cloud computing.

7.1 Protección de datos

El ciclo de vida que siguen los datos que son procesados en la nube es el siguiente:

- Los datos son preparados para poder adaptarse a la nube adecuando su formato o creando un fichero que contenga toda la información necesaria.
- Los datos "viajan" a la nube a través de una conexión a Internet, mediante un correo electrónico, una aplicación específica para importarlos o la transferencia a la nube de la copia de seguridad obtenida de un servidor en la organización.
- Los datos son procesados en la nube, desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Es importante mencionar que los datos pueden almacenarse en copias de seguridad en la nube para facilitar futuros accesos.
- Los datos finales "viajan" de vuelta al usuario. Una vez terminado el procesamiento, el resultado debe volver al usuario con el valor añadido de la información generada en la nube.

El mero hecho de que los datos abandonen la organización puede constituir un riesgo desde el punto de vista de la privacidad: un usuario malintencionado podría interceptar los datos mientras están siendo transferidos por Internet. Incluso si no son interceptados, están siendo almacenados y procesados en una infraestructura informática ajena al control del usuario.

Los mecanismos para minimizar estos riesgos de privacidad son muy sencillos. Antes de migrar los procesos a la nube conviene preguntarse:

"¿Es realmente necesario que todos los datos de la organización pasen a estar en la nube?".

El siguiente ejemplo aclara este interrogante.

Una empresa encargada de tramitar las nóminas de empleados decide utilizar servicios en la nube. Esta empresa tiene bases de datos de miles de trabajadores con DNI, nombre, dirección postal, sueldo bruto, puesto de trabajo, porcentaje de retenciones, número de horas trabajadas, etc.

La operación matemática que esta empresa desea realizar en la nube es el cálculo del sueldo neto que debe ser entregado a cada empleado a final de mes. ¿Es necesario que todos los datos de los empleados sean migrados a la nube? ¿Realmente se necesita el DNI de un empleado para descontarle el porcentaje de IRPF?

Una solución segura es enviar a la nube solo los datos necesarios para realizar el cálculo del salario que son el sueldo bruto y el porcentaje de retenciones. En lugar de enviar a la nube el nombre o el DNI para identificar al trabajador, se crea un nuevo identificador (por ejemplo un número) que permite asignar correctamente el nuevo valor a cada trabajador. De este modo, se impide a un posible atacante que intercepte las

comunicaciones traducir esos datos. Además, el proveedor de servicios en la nube nunca tendrá datos sensibles en sus sistemas, solo contendrá valores matemáticos sin saber a quién pertenecen o qué contienen.

7.2 Integridad

Mantener una correcta integridad de los datos significa que estos permanecen idénticos durante las operaciones de transferencia, almacenamiento o recuperación. En el ámbito del cloud computing, la integridad de los datos es especialmente crítica: los datos están siendo transferidos constantemente entre los servicios en la nube y los distintos usuarios que acceden a ellos.

La mayor amenaza para la integridad de los datos en la nube es que los datos se acaben corrompiendo debido a errores en su manipulación. Si no se detecta que ha habido un problema en la transferencia y los datos se almacenan erróneamente, la próxima vez que el usuario quiera acceder a ellos no podrá utilizarlos.

Para evitar que los datos en la nube no puedan utilizarse o que no estén disponibles se utilizan principalmente tres mecanismos: control de integridad, gestión de cambios y copias de seguridad.

- El **control de integridad** hace uso de funciones matemáticas (funciones resumen o hash) para verificar que los datos no han sufrido modificaciones durante su traslado. El proceso consiste en obtener un valor para la función hash antes de mover el dato y otro cuando se ha terminado de mover. Si dichos valores no coinciden es que ha habido un problema en la transacción y debe ser repetida. En el caso del cloud computing no se utilizan funciones resumen solo para ficheros, sino también para máquinas virtuales completas o para las copias de seguridad.
- La **gestión de cambios** mantiene un historial de modificaciones de los datos o ficheros almacenados en la nube. Cada modificación lleva asociada un sello de fecha y el usuario que lo produjo. Si se detecta que varios usuarios han modificado el recurso a la vez se puede analizar el sello de fecha para comprobar qué versión tiene validez. Del mismo modo, si se detecta un error de integridad en el recurso se puede volver a una versión anterior que sea correcta.
- Las **copias de seguridad** son la última línea defensiva para garantizar la integridad de los datos. Utilizando adecuadamente las herramientas en la nube se pueden programar copias de seguridad cada cierto tiempo. Si se detecta un fallo de integridad a nivel general, la única forma de solucionarlo es volver a una versión anterior del sistema almacenada en la copia de seguridad.

7.3 Control de acceso

Igual que sucede con las arquitecturas tradicionales, el control de acceso también juega un papel importante en el cloud computing. Aunque esta tecnología se represente informalmente como una nube a la que se conecta todo el mundo desde sus equipos (tanto fijos como dispositivos móviles), no significa en absoluto que cualquier persona pueda acceder a cualquier dato o proceso en la nube.

Se pueden utilizar sistemas de correo electrónico en la nube, como Gmail o MSN Hotmail, y eso no significa que cualquier persona pueda leer el correo de otra libremente. Aunque tal vez el ejemplo más completo para hablar del control de acceso en la nube sea Picasa.

Picasa es un sistema de almacenamiento y organización gratuito de fotos en la nube. Cuando se va a crear un nuevo álbum de todos, el usuario tiene la posibilidad de elegir si esas fotos serán públicas y visibles para todo el mundo, solo podrán ser vistas por un conjunto de personas o si es una galería privada a la que solo el usuario tendrá acceso. En este caso concreto, es el usuario de Picasa el que establece la política de control de acceso utilizando el sistema como un expositor de imágenes para todo el mundo o como un sistema de backups privado de fotos.

Extendiendo el ejemplo anterior, cuando una empresa o entidad utiliza las capacidades de la computación en la nube, necesita que el administrador del sistema establezca un correcto control de acceso para garantizar que los usuarios sólo utilizan los datos o procesos para los que han sido autorizados.

7.4 Prevención frente a pérdidas

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque haya un fallo en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no solo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas. La solución a este problema se enfoca desde dos puntos de vista principales.

- Por un lado, una correcta **política de seguridad** limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos. El proveedor de servicios se encarga de solucionar todos los problemas relacionados con los componentes electrónicos. Si detecta un fallo en uno de los equipos dentro de sus instalaciones, automáticamente lo aísla y todos los procesos que se ejecutan en él se migran a otra máquina que no tenga problemas. Este proceso puede durar tan solo unos minutos e incluso realizarse sin cortar el servicio, permitiendo una disponibilidad ininterrumpida de los servicios en la nube.
- Por otra parte, una correcta **política de copias de seguridad** permite recuperar los datos aún cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. Todos los proveedores de servicios en la nube ofrecen sistemas de copias de seguridad de forma completamente transparente para el usuario. Tan solo es necesario seleccionar los activos que se quieren proteger y la periodicidad con la que se desean estas copias. La recuperación frente a un ataque puede ser tan sencilla como la restauración de un snapshot (copia instantánea de volumen) anterior de la máquina virtual.

Las características anteriormente expuestas permiten disponer de un sistema robusto preparado para realizar una correcta recuperación frente a desastres, es decir, asegurando la continuidad del negocio.

Por último, existe otra ventaja relativa a los dispositivos portátiles, cada vez más utilizados en las empresas y desde los que se accede a la información de la organización: ordenadores portátiles, USBs, móviles, etc. Estos dispositivos pueden ser robados u olvidados exponiendo grandes cantidades de datos a personas completamente ajenas a la organización. Si se utilizan sistemas en la nube, aunque se pierda un teléfono móvil o alguien robe un portátil, la información permanecerá inaccesible para terceros.

8 RECOMENDACIONES DE SEGURIDAD SEGÚN EL 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 del 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.

9 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. A la hora de la elección de servicios cloud es importante 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 privacidad de los datos** es uno de los aspectos clave. Existe 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.

10 DOCUMENTACIÓN DE REFERENCIA

- CSA - https://cloudsecurityalliance.org/
- CSA, 2010, TOP Threats to Cloud Computing
- CSA, 2011, Security Guidance for Critical Areas of Focus in Cloud Computing
- NIST, 2011, Guidelines on Security and Privacy in Public Cloud Computing
- Gartner, 2008, Assessing the Security Risks of Cloud Computing
- INTECO-CERT, 2011, Riesgos y amenazas en Cloud Computing
- INTECO-CERT, 2011, Guía para empresas: seguridad y privacidad del cloud computing