enisa
European Network and Information Security Agency

ACERCA DE ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) es una agencia de la Unión Europea creada para contribuir al correcto funcionamiento del mercado interior. ENISA es un centro de excelencia para los Estados miembros y las instituciones europeas en lo relativo a la seguridad de las redes y de la información, que presta asesoramiento, emite recomendaciones y actúa como central de información sobre buenas prácticas. Por otra parte, la agencia facilita el contacto entre las instituciones europeas, los Estados miembros y las empresas privadas e interlocutores del sector.

Esta labor se desarrolla en el contexto del programa de riesgos emergentes y futuros de ENISA.

INFORMACIÓN DE CONTACTO:

El presente informe ha sido editado por:

Correo electrónico: Daniele.catteddu@enisa.europa.eu y Giles.hogben@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

LISTA DE COLABORADORES

El presente documento ha sido elaborado por los editores de ENISA basándose en contribuciones y comentarios de un grupo seleccionado por su experiencia en el tema, incluidos expertos gubernamentales, académicos y del sector.

Salvo que se indique lo contrario, las opiniones expresadas en esta publicación son las de los editores y no reflejan necesariamente las opiniones de los expertos participantes.

Alessandro Perilli	**Virtualization.info (analista independiente)**
Andrea Manieri	**Ingegneria Informatica**
Avner Algom	**The Israeli Association of GRID Technologies**
Craig Balding	**Cloudsecurity.org**
Dr. Guy Bunker	**Bunker Associates**
John Rhoton	**Asesor independiente**
Matt Broda	**Microsoft**
Mirco Rohr	**Kaspersky**
Ofer Biran	**IBM**
Pete Lindstrom	**Spire Security**
Dr Peter Dickman, Director de Ingeniería	**Google Inc.**
Philippe Massonet	**Reservoir Project, CETIC**
Raj Samani	**Information Systems Security Association, Reino Unido**
Simon Pascoe	**British Telecom**
Srijith K. Nair, Theo Dimitrakos	**The BEinGRID Project, British Telecom**
Dr Simone Balboni	**Universidad de Bologna**
Varios	**Oficina de tecnología del National Health Service (NHS), Reino Unido**
Varios	**RSA**
Varios	**Symantec, Symantec Hosted Services**

El contenido legal ha sido redactado principalmente por

Dr. Paolo Balboni	**Baker & McKenzie – Universidad de Tilburg**
Kieran Mccorry	**Hewlett Packard**
David Snead, P.C.	**Abogado y Consejero**

RESUMEN

La computación en nube es un nuevo modo de facilitar recursos de computación, no una *nueva tecnología*. Ahora los servicios de computación, desde el almacenamiento y procesamiento de datos hasta el software, como la gestión del correo electrónico, están disponibles de forma instantánea, sin compromiso y bajo demanda. Puesto que estamos en un momento en que hay que apretarse el cinturón, este nuevo modelo económico de computación ha caído en tierra fértil y está siendo objeto de una inversión global enorme. Según el análisis del IDC, la previsión mundial para los servicios en nube en 2009 oscilará en torno a los 17 400 millones de dólares (1). La estimación para 2013 asciende a 44 200 millones de dólares, mientras que el mercado europeo pasará de los 971 millones de euros registrados en 2008 a 6 005 millones de euros en 2013 (2).

La principal conclusión de este documento es que, desde el punto de vista de la seguridad, las economías de escala y flexibilidad en nube son elementos tanto favorables como perjudiciales. Las concentraciones masivas de recursos y de datos constituyen un objetivo más atractivo para los atacantes, pero las defensas basadas en la nube pueden ser más robustas, escalables y rentables. El presente documento permite realizar una evaluación informada de los riesgos y ventajas para la seguridad que presenta el uso de la computación en nube, y ofrece orientaciones sobre protección para los usuarios actuales y futuros de la computación en nube.

La evaluación de seguridad se basa en tres escenarios de uso: 1) La migración de las PYME a los servicios de computación en nube, 2) el impacto de la computación en nube sobre la resistencia del servicio a los fallos, 3) la computación en nube en la «*e-Government*» (o «Administración Electrónica») (p. ej., la salud digital («*eHealth*»).

El nuevo modelo económico también ha impulsado un cambio técnico en cuanto a:

Escala: la normalización de los componentes y el giro hacia la eficiencia económica han generado concentraciones masivas de los recursos de hardware necesarios para la prestación de servicios. Este factor anima a las economías de escala, debido a todas las clases de recursos necesarios para prestar servicios de computación.

Arquitectura: el uso óptimo de los recursos exige disponer de recursos de computación extraídos del soporte físico subyacente. Los clientes no relacionados que comparten recursos de software y hardware se apoyan en mecanismos de aislamiento lógico para proteger sus datos. La computación, el procesamiento y el almacenamiento de contenidos son distribuidos de manera masiva. Los mercados globales de bienes de consumo demandan redes de distribución de proximidad en las que el contenido sea proporcionado y recibido lo más cerca posible del cliente. Esta tendencia hacia la redundancia y la

distribución global implica que los recursos se gestionan habitualmente al por mayor, tanto física como lógicamente.

En vista de la reducción de costes y de la flexibilidad que conlleva, la migración a la computación en nube es una opción irresistible para muchas PYME. No obstante, la encuesta realizada en el marco de este informe (véase *Survey - An SME Perspective on Cloud Computing*) confirma que entre las principales preocupaciones de las PYME que migran a la nube se encuentran la confidencialidad de su información y la responsabilidad derivada de incidentes relacionados con la infraestructura.

Los gobiernos también están interesados en la posibilidad de utilizar la computación en nube para reducir los costes informáticos e incrementar sus capacidades. Por ejemplo, la Administración de Servicios Generales del Gobierno de los Estados Unidos ofrece actualmente un portal de servicios de computación en nube (3). Los gobiernos también deben superar obstáculos considerables, en términos de percepción pública del procesamiento seguro de la información personal de los ciudadanos en las infraestructuras de computación en nube. Además, también existen obstáculos legales y normativos que impiden el cambio de muchas aplicaciones de «administración electrónica» a la nube. Sin embargo, tanto gobiernos como PYME se enfrentan a la realidad de que muchos de sus empleados utilizarán servicios basados en la nube independientemente de que ello forme parte de su política oficial.

Para que la computación en nube alcance todo el potencial que promete la tecnología, debe ofrecer solidez en la seguridad de la información. El presente documento explica, basándose en escenarios concretos, el significado de la computación en nube para la seguridad de la información y de la red, la protección de datos y la privacidad. Consideramos las ventajas de la computación en nube y sus riesgos con respecto a la seguridad. Estudiamos las repercusiones técnicas, políticas y jurídicas. Y lo que es más importante, efectuamos recomendaciones concretas sobre el modo de abordar los riesgos y de optimizar los beneficios.

Por último, es importante destacar que la computación en nube puede referirse a varios tipos de servicio distintos, incluidos la Aplicación/Software como Servicio (SaaS), Plataforma como Servicio (PaaS) y Infraestructura como Servicio (IaaS). Los riesgos y beneficios asociados a cada modelo difieren, al igual que las consideraciones clave a la hora de contratar este tipo de servicio. Las siguientes secciones intentan establecer las distintas situaciones en las que los riesgos o los beneficios se aplican de modo diferente a los distintos modelos de nube.

RECOMENDACIONES PRINCIPALES

GARANTÍAS PARA LOS CLIENTES EN NUBE

Los clientes en nube necesitan que se les garantice que los proveedores aplican prácticas adecuadas de seguridad para mitigar los riesgos a los que se enfrentan el cliente y el proveedor (por ejemplo, los ataques distribuidos de denegación de servicio, o DDoS). Necesitan esta garantía para poder tomar decisiones de negocio correctas y para mantener u obtener certificados de seguridad. Un síntoma inicial de esta necesidad de aseguración es que numerosos proveedores en nube (PN) se ven bombardeados con solicitudes de auditorías.

Por este motivo, hemos expresado muchas de las recomendaciones del informe en forma de listado de cuestiones que puede ser utilizado para ofrecer o recibir aseguraciones.

Los documentos basados en la lista de comprobación deben aportar a los clientes medios para:

1. evaluar el riesgo de utilizar servicios en nube;
2. comparar las ofertas de los distintos proveedores en nube;
3. obtener aseguraciones de los proveedores en nube seleccionados:
4. reducir la carga de la aseguración con respecto a los proveedores en nube.

La lista de comprobación de seguridad abarca todos los aspectos de los requisitos en materia de seguridad, incluidas la seguridad física y las implicaciones legales, políticas y técnicas.

RECOMENDACIONES LEGALES

La mayoría de cuestiones legales asociadas a la computación en nube se suele resolver durante la evaluación (es decir, al comparar los distintos proveedores) o la negociación del contrato. El caso más común de computación en nube es la selección de los distintos contratos que ofrece el mercado (evaluación de contratos), en contraste con la negociación del contrato. No obstante, podría haber oportunidades para que clientes potenciales de servicios en nube seleccionaran proveedores con contratos negociables.

A diferencia de los servicios tradicionales de Internet, se recomienda revisar detenidamente las cláusulas estándar del contrato, debido a la naturaleza de la computación en nube. Las partes del contrato deben prestar especial atención a sus derechos y obligaciones en lo que respecta a las notificaciones de incumplimiento de los requisitos de seguridad, transferencias de datos, creación de obras derivadas, cambio de control y acceso a los datos por parte de las fuerzas policiales. Debido a que la nube puede utilizarse para subcontratar infraestructura interna crítica, y a que la interrupción de dicha infraestructura puede tener consecuencias de gran alcance, las partes deben considerar detenidamente si las limitaciones estándar de la responsabilidad se ajustan a las asignaciones de

responsabilidad, habida cuenta del uso de la nube por las distintas partes, o a las responsabilidades en cuanto a la infraestructura.

Hasta que los reglamentos y precedentes legales aborden las preocupaciones concretas en materia de seguridad relativas a la computación en nube, los clientes y los proveedores en nube deben asegurarse de que las condiciones de su contrato abordan de manera efectiva los riesgos de seguridad.

RECOMENDACIONES LEGALES PARA LA COMISIÓN EUROPEA

Recomendamos que la Comisión Europea estudie o aclare lo siguiente:

- determinadas cuestiones relativas a la Directiva de protección de los datos personales y a las recomendaciones del grupo de protección de las personas en lo que respecta al tratamiento de datos personales mencionado en el artículo 29.
- la obligación de los proveedores en nube de notificar a sus clientes los incumplimientos relativos a la seguridad de los datos;
- el modo en que las exenciones de responsabilidad de los intermediarios derivadas de los artículos 12 a 15 de Directiva sobre comercio electrónico se aplican a los proveedores en nube;
- el mejor modo de apoyar las normas mínimas de protección de datos y los sistemas de certificación de privacidad comunes a todo los Estados miembros.

RECOMENDACIONES EN MATERIA DE INVESTIGACIÓN

Recomendamos ámbitos prioritarios de investigación a fin de mejorar la seguridad de las tecnologías de computación en nube. Hemos considerado las siguientes categorías, con algunos ejemplos de ámbitos específicos extraídos la lista completa:

CREACIÓN DE UN CLIMA DE CONFIANZA EN LA NUBE

- Efectos de las distintas formas de notificación de los incumplimientos relativos a la seguridad
- Confidencialidad integral de los datos en la nube y más allá
- Nubes con mayor aseguración, nubes privadas virtuales (VPC), etc.

PROTECCIÓN DE DATOS EN LOS GRANDES SISTEMAS INTERORGANIZACIONES

- Informática forense y mecanismos de recogida de pruebas.
- Gestión de incidentes – seguimiento y localización
- Diferencias internacionales en la normativa aplicable, incluida la privacidad y la protección de datos

INGENIERÍA DE SISTEMAS DE COMPUTACIÓN A GRAN ESCALA

- Mecanismos de aislamiento de recursos: datos, procesamiento, memoria, registros, etc.
- Interoperabilidad entre proveedores en nube.
- Resistencia a los fallos de la computación en nube. ¿Cómo puede la nube mejorar esa resistencia?

PRINCIPALES VENTAJAS EN TÉRMINOS DE SEGURIDAD

LA SEGURIDAD Y LAS VENTAJAS DE LA ESCALA: En pocas palabras, todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección. Aquí se incluyen las distintas medidas defensivas, como el filtrado, la administración de parches, el refuerzo de máquinas virtuales (VM) e hipervisores, etc. Otras ventajas de la escala son: las ubicaciones múltiples, las redes de proximidad (entrega o procesamiento de contenidos más cerca de su destino), la oportunidad de la respuesta ante los incidentes y la gestión de las amenazas.

LA SEGURIDAD COMO ELEMENTO DIFERENCIADOR DEL MERCADO: la seguridad constituye una prioridad para muchos clientes en nube; gran parte de ellos toman las decisiones relativas a las adquisiciones basándose en el renombre del proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el mismo. Éste es un motivo de peso para que los proveedores en nube mejoren sus prácticas de seguridad.

INTERFACES NORMALIZADAS PARA SERVICIOS DE SEGURIDAD GESTIONADOS: los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionada. De este modo se genera un mercado de servicios de seguridad más abierto y con mayor disponibilidad.

ESCALADA RÁPIDA E INTELIGENTE DE RECURSOS: la capacidad del proveedor en nube de reasignar dinámicamente los recursos de filtrado, catalogación de tráfico, autenticación, codificación, etc., para las medidas defensivas (por ejemplo, frente a los ataques distribuidos de denegación de servicio, o DDoS) tiene ventajas evidentes para la resistencia a los fallos.

AUDITORÍA Y RECOGIDA DE PRUEBAS: cuando utiliza la virtualización, la computación en nube puede proporcionar imágenes forenses de pago por la utilización de las máquinas virtuales a las que se puede acceder sin desconectar la infraestructura, lo cual reduce el tiempo de espera para realizar un análisis minucioso. También puede aportar un almacenamiento de registros más rentable a la vez que permite una actividad de registro más exhaustiva sin afectar al rendimiento.

ACTUALIZACIONES Y OPCIONES POR DEFECTO MÁS PUNTUALES, EFECTIVAS Y EFICACES: las imágenes por defecto de las máquinas virtuales y los módulos de software utilizados por los clientes pueden ser reforzados y actualizados previamente con los últimos parches y configuraciones de seguridad, conforme a procesos ajustados; las API del servicio en nube de la IaaS también permiten tomar imágenes de la infraestructura virtual de manera frecuente y comparada con un punto inicial. Las actualizaciones pueden aplicarse con mucha más rapidez en una plataforma homogénea que en los sistemas tradiciones de los clientes, que se apoyan en el modelo de parches.

BENEFICIOS DE LA CONCENTRACIÓN DE RECURSOS: Aunque sin duda la concentración de recursos tiene desventajas para la seguridad [véase Riesgos], posee el beneficio evidente de abaratar la perimetrización y el control de acceso físicos (por recurso unitario) y permite una aplicación más sencilla y económica de numerosos procesos vinculados a la seguridad.

PRINCIPALES RIESGOS EN TÉRMINOS DE SEGURIDAD

Los tipos más importantes de riesgos específicos de la nube que identificamos en el presente documento son los siguientes:

PÉRDIDA DE GOBERNANZA: al utilizar las infraestructuras en nube, el cliente necesariamente cede el control de una serie de cuestiones que pueden influir en la seguridad al proveedor en nube. Al mismo tiempo, puede ocurrir que los Acuerdos de nivel de servicio no incluyan la prestación de dichos servicios por parte del proveedor en nube, dejando así una laguna en las defensas de seguridad.

VINCULACIÓN: la oferta actual en cuanto a herramientas, procedimientos o formatos de datos estandarizados o interfaces de servicio que puedan garantizar la portabilidad del servicio, de las aplicaciones y de los datos resulta escasa. Por este motivo, la migración del cliente de un proveedor a otro o la migración de datos y servicios de vuelta a un entorno de tecnologías de la información interno puede ser compleja. Ello introduce la dependencia de un proveedor en nube concreto para la prestación del servicio, especialmente si no está activada la portabilidad de los datos como aspecto más fundamental.

FALLO DE AISLAMIENTO: la multiprestación y los recursos compartidos son características que definen la computación en nube. Esta categoría de riesgo abarca el fallo de los mecanismos que separan el almacenamiento, la memoria, el enrutamiento e incluso el renombre entre los distintos proveedores (por ejemplo, los denominados ataques «*guest hopping*». No obstante, debe considerarse que los ataques a los mecanismos de aislamiento de recursos (por ejemplo, contra hipervisores) todavía son menos numerosos, y su puesta en práctica para el atacante presenta una mayor dificultad en

comparación con los ataques a los sistemas operativos tradicionales.

RIESGOS DE CUMPLIMIENTO: la inversión en la obtención de la certificación (por ejemplo, requisitos reglamentarios o normativos del sector) puede verse amenazada por la migración a la nube:

- si el proveedor en nube no puede demostrar su propio cumplimiento de los requisitos pertinentes
- si el proveedor en nube no permite que el cliente en nube realice la auditoría.

En determinados casos, también significa que el uso de una infraestructura pública en nube implica que no pueden alcanzarse determinados niveles de cumplimiento (por ejemplo, con PCI DSS (4)).

COMPROMISO DE INTERFAZ DE GESTIÓN: las interfaces de gestión de cliente de un proveedor en nube público son accesibles a través de Internet, y canalizan el acceso a conjuntos de recursos más grandes (que los proveedores tradicionales de alojamiento), por lo que plantean un riesgo mayor, especialmente cuando son combinados con el acceso remoto y las vulnerabilidades del navegador de web.

PROTECCIÓN DE DATOS: la computación en nube plantea varios riesgos relativos a la protección de datos tanto para clientes en nube como para proveedores en nube. En algunos casos, puede resultar difícil para el cliente en nube (en su función de controlador de datos) comprobar de manera eficaz las prácticas de gestión de datos del proveedor en nube, y en consecuencia, tener la certeza de que los datos son gestionados de conformidad con la ley. Este problema se ve exacerbado en los casos de transferencias múltiples de datos, por ejemplo, entre nubes federadas. Por otra parte, algunos proveedores en nube sí proporcionan información sobre sus prácticas de gestión de datos. Otros también ofrecen resúmenes de certificación sobre sus actividades de procesamiento y seguridad de datos y los controles de datos a que se someten, por ejemplo, la certificación SAS 70.

SUPRESIÓN DE DATOS INSEGURA O INCOMPLETA: cuando se realiza una solicitud para suprimir un recurso en nube, al igual que sucede con la mayoría de sistemas operativos, en ocasiones el proceso no elimina definitivamente los datos. En ocasiones, la supresión adecuada o puntual de los datos también resulta imposible (o no deseable, desde la perspectiva del cliente), bien porque existen copias adicionales de datos almacenadas pero no disponibles o porque el disco que va a ser destruido también incluye datos de otros clientes. La multiprestación y la reutilización de recursos de hardware representan un riesgo mayor para el cliente que la opción del hardware dedicado.

MIEMBRO MALICIOSO: aunque no suelen producirse habitualmente, los daños causados por miembros

maliciosos son, con frecuencia, mucho más perjudiciales. Las arquitecturas en nube necesitan ciertas funciones cuyo perfil de riesgo es muy elevado. Algunos ejemplos son los administradores de sistemas de proveedores en nube y los proveedores de servicios de seguridad gestionada.

NB: los riesgos enumerados anteriormente no siguen un orden de criticidad concreto, sino que simplemente constituyen diez de los riesgos más importantes de la computación en nube identificados durante la evaluación. Los riesgos del uso de la computación en nube deben ser comparados con los riesgos derivados de mantener las soluciones tradicionales, como los modelos de sobremesa. Para facilitar este proceso, hemos incluido en el documento principal estimaciones de los riesgos relativos comparados con un entorno tradicional típico.

Adviértase que a menudo es posible, y en algunos casos recomendable, que el cliente en nube transfiera el riesgo al proveedor en nube; *sin embargo, no todos los riesgos pueden ser transferidos*: Si un riesgo provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños. En última instancia, puede subcontratar la responsabilidad, pero no puede subcontratar la obligación de rendir cuentas.

ÍNDICE

PÚBLICO OBJETIVO

El público al que va dirigido el presente informe está formado por:

- gerentes de empresa, de PYME en particular, para facilitar su evaluación y mitigación de los riesgos asociados a la adopción de tecnologías de computación en nube;
- responsables políticos europeos, para ayudarles a adoptar decisiones en materia de política de investigación (para desarrollar tecnologías dirigidas a mitigar riesgos);
- responsables políticos europeos, para ayudarles a establecer los incentivos políticos y económicos adecuados, las medidas legislativas, las iniciativas de sensibilización, etc., con respecto a las tecnologías de computación en nube;
- ciudadanos, para permitirles la evaluación de costes y beneficios derivados del uso de la versión de consumo de estas aplicaciones.

COMPUTACIÓN EN NUBE: DEFINICIÓN OPERATIVA

Ésta será la definición operativa de la computación en nube que utilizamos para los fines del presente estudio. No pretendemos que sea otra nueva definición definitiva. Las fuentes utilizadas para nuestra definición pueden ser consultadas en las secciones (5), (6) y (54).

La computación en nube es un modelo de servicio bajo demanda para la prestación de TI, a menudo basado en la virtualización y en las tecnologías informáticas distribuidas. Las arquitecturas de computación en nube poseen:

- recursos con un alto grado de abstracción
- escalabilidad y flexibilidad prácticamente instantáneas
- prestación casi instantánea
- recursos compartidos (hardware, base de datos, memoria, etc.)
- «servicio bajo demanda», que suele incluir un sistema de facturación de pago por uso
- gestión programática (por ejemplo, mediante la API del WS).

Hay tres categorías de computación en nube:

- **Software como servicio (Saas): es** el software que ofrece un tercero, disponible bajo demanda, normalmente a través de Internet y configurable de forma remota. Entre los ejemplos de este software se encuentran las herramientas de procesamiento de textos y hojas

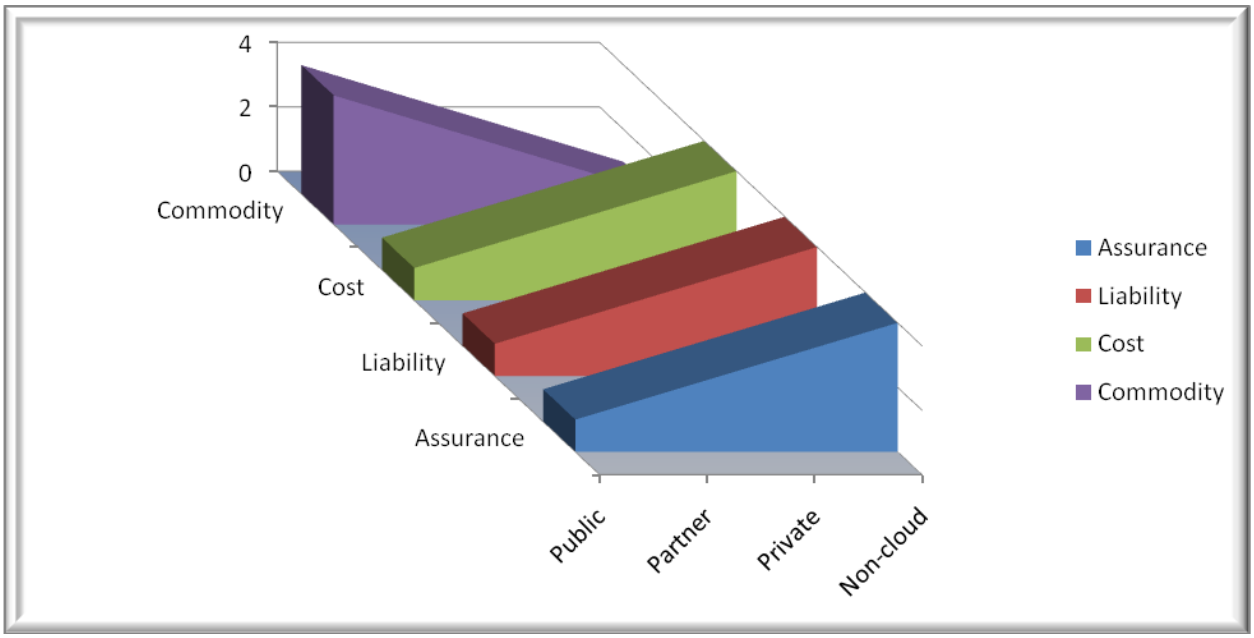
de cálculo en línea, los servicios de gestión de relaciones con los clientes (CRM) y los servicios de entrega de contenido web (*Salesforce* CRM, Google Docs, etc.).

- **Plataforma como servicio (PaaS):** permite que los clientes desarrollen aplicaciones nuevas utilizando las API desplegadas y configurables de forma remota. Las plataformas ofrecidas incluyen herramientas de desarrollo, gestión de la configuración y plataformas de despliegue. Algunos ejemplos son Microsoft Azure, Force y App Engine de Google.
- **Infraestructura como servicio (IaaS):** proporciona máquinas virtuales y otro hardware extraído, así como sistemas operativos que pueden ser controlados a través de una API de servicio. Algunos ejemplos son Amazon EC2 y S3, Enterprise Cloud de Terremark, Windows Live Skydrive y Rackspace Cloud.

Las nubes también pueden ser divididas en:

- **públicas**: disponibles para el público en general: cualquier organización puede suscribirse
- **privadas:** servicios creados conforme a principios de computación en nube a los que sólo se puede acceder dentro de una red privada
- **asociadas:** servicios en nube ofrecidos por un proveedor a un número limitado de partes muy determinadas.

En general, el bien de consumo, el coste, la responsabilidad y la aseguración de las nubes varían en función de la siguiente figura:



Bien de consumo – coste – responsabilidad – aseguración – pública – asociada – privada – sin nube – aseguración – responsabilidad – coste – bien de consumo

FIGURA 1: CARACTERÍSTICAS DE LAS NUBES PÚBLICAS, ASOCIADAS Y PRIVADAS

ESTUDIO DEL TRABAJO EXISTENTE

Durante la elaboración del presente informe, estudiamos el trabajo existente en materia de riesgos de seguridad en la nube y su mitigación, incluidos los títulos *Security Guidance for Critical Areas of Focus in Cloud Computing* (*Cloud security Alliance* (55)) *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration* (Jericho Forum (56)) y *Assessing the Security Risks of Cloud Computing* (Gartner (57)) a fin de averiguar el mejor enfoque de los resultados para obtener el máximo valor añadido.

1. VENTAJAS DE LA COMPUTACIÓN EN NUBE EN TÉRMINOS DE SEGURIDAD

Apenas resulta necesario reproducir las incontables páginas de material escrito sobre las ventajas económicas, técnicas, arquitectónicas y ecológicas de la computación en nube. Sin embargo, a la luz de la experiencia directa de los integrantes de nuestro grupo de expertos y según las noticias recientes del «mundo real», el examen de los riesgos de la computación en nube en materia de seguridad debe tener su contrapunto en una revisión de las ventajas concretas que ofrece en materia de seguridad. La computación en nube posee un potencial considerable para mejorar la seguridad y la resistencia a los fallos. Lo que sigue a continuación es una descripción de las contribuciones clave que puede realizar.

LA SEGURIDAD Y LAS VENTAJAS DE LA ESCALA

En pocas palabras, todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección. Aquí quedan incluidas las distintas medidas defensivas, como el filtrado, la administración de parches, el refuerzo de máquinas virtuales e hipervisores, los recursos humanos y su gestión y control, la redundancia de hardware y software, los sistemas de autenticación seguros, un control eficaz basado en funciones y soluciones federadas de gestión de la identidad por defecto, que también mejora los efectos de red de la colaboración de varios socios implicados en la defensa. Otras ventajas de la escala son:

- **Ubicaciones múltiples:** la mayoría de proveedores en nube cuentan con los recursos económicos necesarios para replicar el contenido en ubicaciones múltiples por defecto. De este modo se aumenta la redundancia y la independencia de los errores y se proporciona un grado de recuperación de desastres listo para su uso.
- **Redes de proximidad:** el almacenamiento, procesamiento y entrega más cerca de la red de proximidad supone una confianza en el servicio y un incremento de la calidad en general; del mismo modo, es menos probable que los problemas de redes locales tengan efectos secundarios globales.
- **Mejora del tiempo de respuesta a los incidentes:** los sistemas a mayor escala gestionados satisfactoriamente, por ejemplo, a raíz de la detección temprana de nuevos despliegues de programas maliciosos, pueden desarrollar capacidades más eficaces de respuesta ante incidentes.
- **Gestión de amenazas:** los proveedores en nube también pueden permitirse contratar a especialistas para que se ocupen de las amenazas concretas a la seguridad, mientras que las compañías más pequeñas sólo se pueden permitir los servicios de un número reducido de profesionales generalistas.

LA SEGURIDAD COMO ELEMENTO DIFERENCIADOR DE MERCADO

La seguridad constituye una prioridad para muchos clientes en nube [véase la encuesta: An SME perspective on Cloud Computing]; los clientes toman las decisiones relativas a la adquisición basándose en el renombre del proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el proveedor, todavía más que en los entornos tradicionales. Éste es un motivo de peso para que los proveedores en nube mejoren sus prácticas de seguridad y generen competencia en este aspecto.

INTERFACES NORMALIZADAS PARA SERVICIOS DE SEGURIDAD GESTIONADOS

Los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionadas que ofrecen servicios a todos sus clientes. Potencialmente, ello genera un mercado más abierto y disponible de servicios de seguridad, donde los clientes pueden cambiar de proveedor con mayor facilidad e incurriendo en menores gastos de configuración.

ESCALADA RÁPIDA E INTELIGENTE DE RECURSOS

La lista de recursos en nube que pueden ser escalados rápidamente bajo demanda ya incluye, entre otros, el almacenamiento, el tiempo de CPU, la memoria, las solicitudes de servicios web y las máquinas virtuales, y el nivel de control granular sobre el consumo de recursos aumenta a medida que las tecnologías mejoran.

Un proveedor en nube tiene potencial para reasignar recursos de manera dinámica para el filtrado, la catalogación de tráfico, la codificación, etc., con vistas a incrementar el apoyo a las medidas defensivas (por ejemplo, frente a los ataques distribuidos de denegación de servicio (DDoS)) cuando un ataque está produciéndose o puede producirse. Cuando esta capacidad de reasignación dinámica de recursos se combina con métodos adecuados de optimización de recursos, el proveedor en nube puede limitar las posibles consecuencias de determinados ataques sobre la disponibilidad de los recursos que utilizan los servicios alojados legítimamente, así como reducir el impacto del incremento de uso de los recursos por la defensa de seguridad para hacer frente a dichos ataques. Sin embargo, para lograr este efecto, el proveedor debe aplicar una coordinación adecuada de la autonomía para la defensa de seguridad y para la gestión y optimización de los recursos.

La capacidad de escalar dinámicamente los recursos defensivos bajo demanda posee ventajas evidentes con respecto a la resistencia a los fallos. Además, cuanto mayor sea la escalada de los distintos tipos de recursos individuales de manera granular —sin escalar la totalidad de los recursos del sistema—, más barato será responder a los picos repentinos (no maliciosos) de demanda.

AUDITORÍA Y RECOGIDA DE PRUEBAS

La OFERTA de la IaaS apoya la clonación de máquinas virtuales bajo demanda. En caso de supuesto incumplimiento de la seguridad, el cliente puede tomar una imagen de una máquina virtual activa —o de los componentes virtuales de la misma— para llevar a cabo un análisis forense fuera de línea, lo cual reduce el tiempo de espera para la realización el análisis. Con el almacenamiento a libre disposición, es posible crear clones múltiples y poner en paralelo actividades de análisis y así reducir el tiempo dedicado a la investigación. De este modo se mejora el análisis *ex post* de los incidentes de seguridad y se incrementa la probabilidad de localizar a los atacantes y de solucionar las deficiencias. Sin embargo, se presupone que el cliente tiene acceso a expertos forenses bien formados (lo que no constituye un servicio en nube estándar en el momento de redactar este documento).

También puede aportar un almacenamiento de registros más rentable a la vez que permite una actividad de registro más amplia sin afectar al rendimiento. El almacenamiento en nube de pago por uso aporta transparencia a sus gastos de almacenamiento de auditoría y facilita el proceso de ajuste a los requisitos futuros de los registros de auditoría. De este modo se incrementa la eficacia del proceso de identificación de incidentes de seguridad a medida que se producen (7).

ACTUALIZACIONES Y OPCIONES POR DEFECTO MÁS PUNTUALES, EFECTIVAS Y EFICACES

Las imágenes por defecto de las máquinas virtuales y los módulos de software utilizados por los clientes pueden ser reforzados y actualizados previamente con los últimos parches y configuraciones de seguridad, conforme a procesos ajustados; las API del servicio en nube de la IaaS también permiten tomar imágenes de la infraestructura virtual de manera frecuente y comparada con un punto inicial (por ejemplo, para garantizar que las normas del cortafuegos de software no se han modificado) (8). Las actualizaciones pueden aplicarse con mucha más rapidez en una plataforma homogénea que en los sistemas tradiciones de los clientes, que se apoyan en el modelo de parches. Por último, en los modelos de PaaS y SaaS, es más probable que las aplicaciones se hayan reforzado para ejecutarse fuera del entorno empresarial, lo cual hace más probable que sean más portátiles y robustas que el software empresarial equivalente (si lo hay). También es más probable que se sean actualizadas periódicamente y que sean parcheadas de manera centralizada, minimizando la ventana de vulnerabilidad.

LA AUDITORÍA Y LOS ACUERDOS DE NIVEL DE SERVICIO OBLIGAN A GESTIONAR MEJOR EL RIESGO

La necesidad de cuantificar las sanciones de los distintos escenarios de riesgo en los Acuerdos de nivel de servicio y la posible repercusión de los incumplimientos de la seguridad sobre el renombre (véase Seguridad como diferenciador de mercado) motivan una auditoría interna y unos procedimientos de

evaluación del riesgo más minuciosos que los que se llevarían a cabo en condiciones normales. La frecuencia de las auditorías impuestas a los proveedores en nube tiende a exponer los riesgos que, de otro modo, no habrían sido identificados, con lo que tiene el mismo efecto positivo.

BENEFICIOS DE LA CONCENTRACIÓN DE RECURSOS

Aunque sin duda la concentración de recursos tiene desventajas para la seguridad (véase Riesgos), posee el beneficio evidente de abaratar la perimetrización y el control de acceso físicos (por recurso unitario) y permite una aplicación más sencilla y económica de una política de seguridad exhaustiva y un control sobre la gestión de datos, la administración de parches, la gestión de incidentes y los procesos de mantenimiento. Obviamente, la medida en que este ahorro se transmite a los clientes varía.

2. EVALUACIÓN DE RIESGOS

ESCENARIOS DE USO

Para los fines de la presente evaluación de riesgo de la computación en nube, hemos analizado tres escenarios de uso:

- Una perspectiva de las PYME sobre la computación en nube
- La repercusión de la computación en nube sobre la resistencia a los fallos del servicio
- Computación en nube y «Administración electrónica» («eHealth»).

En aras de la brevedad, decidimos publicar la versión íntegra del escenario de uso de las PYME (véase el ANEXO II) y un resumen de los escenarios de resistencia a los fallos y de «eHealth» (véase el ANEXO III).

Esta selección se basa en el argumento de que se prevé que en Europa, el mercado en nube tenga un gran impacto sobre los nuevos negocios y puestas en marcha, así como en la evolución de los modelos de negocio actuales. Dado que la industria de la EU se compone principalmente de PYME (el 99 % de las compañías, según fuentes comunitarias (9)), tiene sentido centrarse en las PYME. No obstante, hemos incluido varios riesgos y recomendaciones que se aplican de manera específica a los gobiernos y a las empresas más grandes.

El escenario de las PYME se basa en los resultados de la encuesta «An SME perspective on Cloud Computing» (que pueden consultarse aquí), y NO pretende ser una hoja de ruta para las compañías que están considerando, planificando o ejecutando inversiones y proyectos de computación en nube.

Se utilizó como caso de uso una compañía de tamaño mediano para garantizar que la evaluación tuviera un elevado nivel de TI y complejidad jurídica y empresarial. El objetivo era exponer toda la información posible sobre riesgos a la seguridad. Algunos de estos riesgos son específicos de las pequeñas y medianas empresas, mientras que otros son riesgos generales a los que es probable que las microempresas o pequeñas empresas se enfrenten durante la migración a un enfoque de computación en nube.

La pretensión NO era que el escenario fuera totalmente realista para cualquier cliente o proveedor en nube, sino que es probable que todos los elementos del escenario se den en muchas organizaciones en un futuro cercano.

PROCESO DE EVALUACIÓN DEL RIESGO

El nivel de riesgo se estima basándose en la probabilidad de un escenario de incidentes, comparado con el impacto negativo estimado. La probabilidad de que se produzca un escenario de incidentes se obtiene mediante una amenaza que explota la vulnerabilidad con una probabilidad concreta.

La probabilidad de cada escenario de incidentes y el impacto sobre el negocio se determinó consultando al grupo de expertos que contribuyó al presente informe y utilizando su experiencia colectiva. En los casos en los que se consideró que no era posible proporcionar una estimación fundada de la probabilidad de un evento, el valor es n/a. En muchos casos, la estimación de la probabilidad depende en gran medida del modelo de nube o arquitectura que se está considerando.

A continuación puede verse el nivel de riesgo como función del impacto sobre el negocio y la probabilidad del escenario de incidentes. El riesgo resultante se mide en una escala de 0 a 8 que puede evaluarse con respecto a los criterios de aceptación del riesgo. Esta escala de riesgo también puede compararse con una sencilla clasificación general de riesgos:

- Riesgo bajo: 0-2
- Riesgo medio: 3-5
- Riesgo alto: 6-8

	Probabilidad del escenario de incidentes	Muy baja (Muy improbable)	Leve (Improbable)	Media (Posible)	Alta (Probable)	Muy alta (Frecuente)
Impacto	Muy bajo	0	1	2	3	4
	Leve	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
Impacto	Muy alto	4	5	6	7	8

Hemos basado la estimación de los niveles de riesgo en norma ISO/IEC 27005:2008 (10).

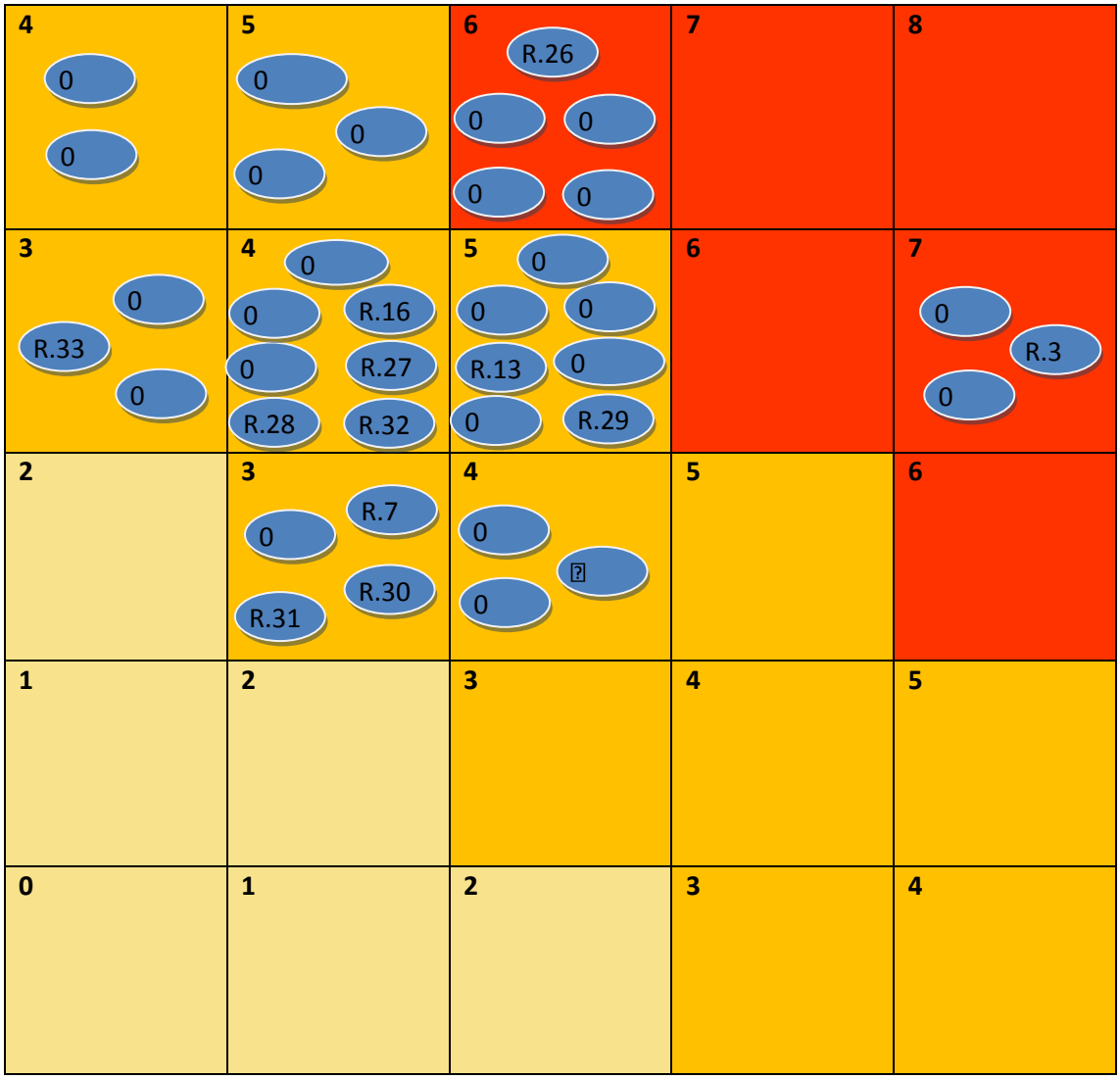
3. RIESGOS

Cabe señalar los siguientes puntos en relación con las siguientes descripciones de riesgos:

- Los riesgos siempre deben entenderse vinculados a las oportunidades de negocio en general y a la actitud hacia el riesgo (en ocasiones el riesgo se ve compensado por la oportunidad).
- Los servicios en nube no sólo tratan de la conveniencia del almacenamiento al que puede accederse desde múltiples dispositivos, sino que incluyen ventajas importantes como una comunicación más conveniente y una colaboración instantánea entre múltiples puntos. Por lo tanto, el análisis comparativo no sólo debe comparar los riesgos de almacenar datos en distintas ubicaciones (en las instalaciones o en la nube), sino también los riesgos que surgen cuando los datos almacenados en las instalaciones (por ejemplo, una hoja de cálculo) se envían por correo electrónico a otras personas para que realicen sus contribuciones, frente a las cuestiones de seguridad de una hoja de cálculo almacenada en la nube y abierta para que dichas personas colaboren. Por lo tanto, los riesgos del uso de la computación en nube deben compararse con los riesgos derivados de mantener las soluciones tradicionales, como los modelos de sobremesa.
- En numerosas ocasiones, el nivel de riesgo variará considerablemente en función del tipo de arquitectura de nube que se esté considerando.
- El cliente en nube puede transferir el riesgo al proveedor en nube, y los riesgos deben considerarse con respecto a la rentabilidad proporcionada por los servicios. Sin embargo, *no todos los riesgos pueden ser transferidos*: Si un riesgo provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños.
- El análisis de riesgo incluido en el presente documento se aplica a la tecnología en nube. No se aplica a ninguna compañía u oferta concreta de computación en nube. El objetivo del presente documento no es sustituir a una evaluación de riesgo organizativa de un proyecto concreto.
- El nivel de riesgos se expresa desde la perspectiva del cliente en nube. Cuando se considera el punto de vista del proveedor en nube, se indica explícitamente.

El siguiente cuadro muestra la distribución de los impactos y probabilidades del riesgo:

IMPACTO



DE LA PROBABILIDAD

FIGURA 2: DISTRIBUCIÓN DE RIESGOS

Los riesgos identificados en la evaluación se clasifican de acuerdo con tres categorías:

- política y organizativa
- técnica

- legal.

Cada riesgo se presenta en cuadros que incluyen:

- el nivel de probabilidad
- el grado de impacto
- referencias a vulnerabilidades
- referencias a los activos afectados
- el nivel de riesgo.

Además, *en los casos representativos*, hemos añadido una probabilidad comparativa y una celda de impacto para comparar los riesgos de la computación en nube y en los enfoques estándar de TI. No hemos incluido el riesgo comparativo, puesto que se asume que todos los riesgos seleccionados son mayores.

RIESGOS POLÍTICOS Y ORGANIZATIVOS

R.1 VINCULACIÓN

Probabilidad	ALTA	Comparativa: Más alta
Impacto	MEDIO	Comparativa: Igual
Vulnerabilidades	. Falta de tecnologías y soluciones estándar . Selección de proveedores insuficiente Ausencia de redundancia **DE SUMINISTRADOR** . Falta de integridad y transparencia en los términos de uso	
Activos afectados	A1. Renombre de la compañía A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	**ALTO**	

La oferta actual en cuanto a herramientas, procedimientos o formatos de datos normalizados o interfaces de servicio que puedan garantizar la portabilidad del servicio y de los datos es escasa (aunque existen algunas iniciativas, por ejemplo, véase (58)). Por este motivo, la migración del cliente

de un proveedor a otro o la migración de datos y servicios desde un entorno de tecnologías de la información interno o al mismo puede ser muy compleja. Además, los proveedores en nube pueden tener un incentivo para impedir (directa o indirectamente) la portabilidad de los datos o los servicios de sus clientes.

Esta dependencia potencial de la prestación del servicio de un proveedor en nube concreto, en función de los compromisos del mismo, puede generar un fracaso catastrófico del negocio si el proveedor en nube va a la quiebra (véase R.5) y la ruta de migración de la aplicación y el contenido a otro proveedor es demasiado costosa (en términos económicos o temporales) o no se proporciona una alerta suficiente (no hay alerta temprana).

La adquisición del proveedor en nube (R.6) también puede tener un efecto similar, puesto que aumenta la probabilidad de que se produzcan cambios repentinos en la política del proveedor y acuerdos no vinculantes como los términos de uso (TdU).
Es importante entender que el grado y la naturaleza de la vinculación varían en función del tipo de nube:

Vinculación SaaS

- Los datos del cliente suelen almacenarse en un esquema de base de datos de uso diseñado por el proveedor del SaaS. La mayoría de proveedores de SaaS ofrecen llamadas API para leer (y, por tanto, «exportar») registros de datos. No obstante, si el proveedor no ofrece una aplicación comercial con una rutina de «exportación» de datos, el cliente tendrá que desarrollar un programa que extraiga sus datos y los escriba en el archivo, dejándolos listos para importarlos a otro proveedor. Cabe señalar que hay pocos acuerdos formales sobre la estructura de los registros comerciales (por ejemplo, los campos de un registro de cliente en un proveedor de SaaS pueden ser distintos en otro proveedor), aunque existen formatos de archivo subyacentes comunes para la importación y la exportación de datos, por ejemplo, XML. Por lo general, el nuevo proveedor puede ayudar en esta tarea por una suma negociable. Sin embargo, si los datos deben volver a la empresa, el cliente tendrá que escribir rutinas de importación que se ocupan de las comparaciones de datos necesarias, a menos que el proveedor en nube ofrezca esta rutina. Dado que los clientes evaluarán este aspecto antes de tomar decisiones importantes sobre la migración, redunda en el interés comercial a largo plazo de los proveedores en nube hacer la portabilidad lo más fácil, completa y rentable posible.

- La vinculación de la aplicación es la forma más evidente de vinculación (aunque no es específica de los servicios en nube). Los proveedores de SaaS suelen desarrollar una aplicación

personalizada a medida de las necesidades de su mercado objetivo. Los clientes de SaaS que poseen una amplia base de usuarios pueden contraer gastos de conmutación muy elevados a la hora de migrar a otro proveedor de SaaS, puesto que la experiencia del usuario final se ve afectada (por ejemplo, es necesario realizar un reciclaje de formación). Si el cliente ha desarrollado programas para interactuar con las API de los proveedores directamente (por ejemplo, para integrarse con otras aplicaciones), éstos también deberán ser reescritos para tener en cuenta la API del nuevo proveedor.

Vinculación PaaS

La vinculación PaaS se produce tanto en el nivel de API (es decir, llamadas específicas de la API a la plataforma) como a nivel de componente. Por ejemplo, el proveedor de PaaS puede ofrecer un almacenamiento de datos secundario de gran eficacia. El cliente no sólo debe desarrollar un código utilizando las API personalizadas que ofrece el proveedor, sino que también debe codificar las rutinas de acceso a los datos para compatibilizarlas con el almacenamiento de datos secundario. Este código no tiene por qué ser portátil entre proveedores de PaaS, incluso si se ofrece una API con un alto grado de compatibilidad, ya que el modelo de acceso a datos puede ser diferente (por ejemplo, relacional frente a «*hashing*» (codificación)).

- La vinculación PaaS en el nivel de API se produce cuando distintos proveedores ofrecen distintas API.
- La vinculación PaaS se produce en el nivel de ejecución, puesto que las ejecuciones estándar suelen estar muy personalizadas, a fin de operar de modo seguro en el entorno en nube. Por ejemplo, una ejecución Java puede sufrir la eliminación o la modificación de llamadas «peligrosas» por motivos de seguridad. Corresponde a los desarrolladores del cliente entender y tener en cuenta estas diferencias.
- La PaaS también es objeto de vinculación de datos, del mismo modo que el SaaS, pero en este caso, el cliente es el único responsable de crear rutinas de exportación compatibles.

Vinculación IaaS

La vinculación IaaS varía en función de los servicios de infraestructura específicos que se consumen. Por ejemplo, un cliente que utiliza almacenamiento en nube no se verá afectado por formatos de máquina virtual no compatibles.

- Los proveedores de computación IaaS suelen ofrecer máquinas virtuales basadas en hipervisor. Los metadatos de VM y software se agrupan juntos por motivos de portabilidad (suele hacerse

únicamente dentro de la nube del proveedor). La migración entre proveedores es no trivial hasta que se adoptan normas abiertas, como el formato abierto de virtualización (OVF) (11).

- Las ofertas de los proveedores de almacenamiento IaaS incluyen desde sencillos almacenajes de datos basados en valores/claves hasta almacenajes basados en archivos mejorados por políticas. Los conjuntos de características varían de forma considerable, y en consecuencia, también lo hace la semántica del almacenamiento. Sin embargo, la dependencia del grado de aplicación de las características específicas de la política (por ejemplo, los controles de acceso) puede limitar la selección de proveedor por parte del cliente.
- La vinculación de datos constituye la preocupación obvia con respecto a los servicios de almacenamiento IaaS. A medida que los clientes en nube empujan más datos para ser almacenados en la nube, la vinculación de los datos aumenta a menos que el proveedor en nube permita la portabilidad de los datos.

Una característica común a todos los proveedores es que ofrecen la posibilidad de un escenario de «pánico bancario» para el proveedor en nube. Para este escenario, en caso de producirse una crisis de confianza en la situación financiera del proveedor en nube, tiene lugar una salida en masa y una retirada de contenido por orden de llegada. Entonces, en una situación en la que el proveedor limita la cantidad de «contenido» (código de aplicación y datos) que puede «retirarse» durante un período de tiempo dado, algunos clientes nunca podrán recuperar sus datos y sus aplicaciones.

R.2 PÉRDIDA DE GOBERNANZA

Probabilidad	MUY ALTA	Comparativa: Más alta
Impacto	MUY ALTO (depende de la organización) (IaaS MUY ALTA, SaaS Bajo)	Comparativa: Igual
Vulnerabilidades	□. Funciones y responsabilidades confusas □. Aplicación deficiente de las definiciones de funciones □. sincronización de las responsabilidades o las obligaciones contractuales externas a la nube □ Cláusulas SLA con compromisos en conflicto para con diferentes partes □. Auditoría o certificación no disponible para los clientes□. Aplicaciones inter-nube que crean dependencia oculta □. Falta de tecnologías y soluciones estándar □. Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto □. Ausencia de un acuerdo de depósito de fuentes	

	□. Falta de control en el proceso de evaluación de vulnerabilidad □. Sistemas de certificación no adaptados a las infraestructuras de nube □. Falta de información sobre jurisdicciones □. Falta de integridad y transparencia en los términos de uso □ Propiedad de los activos confusa
Activos afectados	A1. Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	**ALTO**

Al utilizar las infraestructuras de nube, el cliente necesariamente cede el control de una serie de cuestiones que pueden influir en la seguridad al proveedor en nube. Por ejemplo, los TdU pueden prohibir el escaneado de puertos, la evaluación de vulnerabilidades y las pruebas de penetración. Además, pueden surgir conflictos entre los procedimientos de refuerzo del cliente y el entorno en nube (véase R.20). Por otra parte, puede ocurrir que los Acuerdos de nivel de servicio no incluyan la prestación de dichos servicios por parte del proveedor en nube, dejando así una laguna en las defensas de seguridad.

Asimismo, el proveedor en nube puede subcontratar o externalizar servicios a terceros (proveedores desconocidos) que podrían no ofrecer las mismas garantías (como la prestación del servicio de manera legal) ofrecidas por el proveedor en nube, o que se produzcan cambios en el control del proveedor en nube de modo que provoquen una modificación de los términos y condiciones de sus servicios.

La pérdida de gobernanza y control podría repercutir gravemente sobre la estrategia de la organización, y por tanto, sobre la capacidad de cumplir su misión y sus objetivos. La pérdida de control y gobernanza podría generar la imposibilidad de cumplir los requisitos en materia de seguridad, la falta de confidencialidad, integridad y disponibilidad de los datos y el deterioro del rendimiento y de la calidad del servicio, por no mencionar la introducción de desafíos de cumplimiento (véase R.3).

R.3 Desafíos de cumplimiento

Probabilidad	MUY ALTA (depende de la PCI, SOX)	Comparativa: Más alta
Impacto	ALTO	Comparativa: Igual
Vulnerabilidades	. Auditoría o certificación no disponible para los clientes . Falta de tecnologías y soluciones estándar Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto Sistemas de certificación no adaptados a las infraestructuras de nube . Falta de información sobre jurisdicciones . Falta de integridad y transparencia en los términos de uso	
Activos afectados	A20 Certificación	
Riesgo	**ALTO**	

Determinadas organizaciones que migran a la nube han realizado inversiones considerables para alcanzar la certificación, bien para lograr una ventaja competitiva o para ajustarse a los requisitos normativos o reglamentarios del sector (por ejemplo, la norma PCI DSS). Esta inversión puede verse amenazada por la migración a la nube:

- si el proveedor en nube no puede demostrar su propio cumplimiento de los requisitos pertinentes;
- si el proveedor en nube no permite que el cliente en nube lleve a cabo la auditoría.

En determinados casos, también significa que el uso de una infraestructura pública de nube implica que no pueden alcanzarse determinados niveles de cumplimiento, y por ello los servicios de alojamiento en nube no pueden utilizarse para los servicios que los necesitan. Por ejemplo, EC2 afirma que los clientes estarán presionados para alcanzar el cumplimiento PCI en su plataforma. Por este motivo, los servicios alojados en EC2 no pueden utilizarse para gestionar transacciones con tarjeta de crédito.

R.4 PÉRDIDA DEL RENOMBRE EMPRESARIAL A RAÍZ DE ACTIVIDADES DE PRESTACIÓN CONJUNTA

Probabilidad	BAJA
Impacto	ALTO
Vulnerabilidades	□. Ausencia de aislamiento de los recursos □. Falta de aislamiento de la reputación □. Vulnerabilidades del hipervisor
Activos afectados	A1. Renombre de la compañía A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	**MEDIO**

Los recursos compartidos implican la posibilidad de que las actividades maliciosas de un prestador puedan afectar al renombre de otro. Por ejemplo, el spam, el escaneado de puertos o la prestación de contenido malicioso de la infraestructura en nube puede ocasionar:

- el bloqueo de un rango de direcciones IP, incluidos el atacante y otros proveedores de infraestructura inocentes:
- la confiscación de los recursos debido a las actividades de vecindad (orden judicial de vecindad).

El impacto puede traducirse en una entrega deficiente del servicio y en la pérdida de datos, así como en problemas para el renombre de la organización.

R.5 ERROR O CANCELACIÓN DEL SERVICIO EN NUBE

Probabilidad	N/A	
Impacto	MUY ALTO	Comparativa: Más alta
Vulnerabilidades	□. Selección de proveedores insuficiente □ Ausencia de redundancia de suministrador □. Falta de integridad y transparencia en los términos de uso	

Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	**MEDIO**

Como en cualquier mercado nuevo de TI, la presión de la competencia, una estrategia de negocios inapropiada, la falta de apoyo financiero, etc., pueden provocar el cierre de algunos proveedores o, como mínimo, obligarles a reestructurar su oferta de cartera de servicios. Dicho de otro modo, es posible que a corto o medio plazo finalicen algunos servicios de computación en nube.
El impacto de esta amenaza para el cliente en nube es sencillo de entender, ya que puede dar lugar a una pérdida o al deterioro del rendimiento y de la calidad del servicio, así como a una pérdida de la inversión.

Además, los errores en los servicios subcontratados al proveedor en nube pueden repercutir considerablemente sobre la capacidad del cliente en nube para cumplir sus funciones y obligaciones para con sus propios clientes. Así, el cliente del proveedor en nube puede estar expuesto a responsabilidad contractual y extracontractual frente a sus clientes, basándose en la negligencia de su proveedor. Los errores del proveedor en nube también pueden derivar en responsabilidad del cliente ante sus empleados.

R.6 ADQUISICIÓN DEL PROVEEDOR EN NUBE

Probabilidad	N/A	
Impacto	MEDIO	Comparativa: Más alta
Vulnerabilidades	□. Falta de integridad y transparencia en los términos de uso	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A4. Datos personales sensibles A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	**MEDIO**	

La adquisición del proveedor en nube puede incrementar la probabilidad de que se produzca un cambio estratégico y puede amenazar los acuerdos no vinculantes (por ejemplo, las interfaces de software, las inversiones de seguridad y los controles de seguridad no incluidos en el contrato). Ello podría impedir el cumplimiento de los requisitos en materia de seguridad. El impacto final podría ser perjudicial para activos cruciales como: el renombre de la organización, la confianza del cliente o paciente y la experiencia y fidelidad del cliente.

R.7 FALLO EN LA CADENA DE SUMINISTRO

Probabilidad	BAJA	Comparativa: Más alta
Impacto	MEDIO	Comparativa: Más alta
Vulnerabilidades	□. Falta de integridad y transparencia en los términos de uso □. Aplicaciones inter-nube que crean dependencia oculta □. Selección de proveedores insuficiente □. Ausencia de redundancia de suministrador	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	**LEVE**	

Un proveedor de computación en nube puede subcontratar determinadas tareas especializadas de su cadena «de producción» a terceros. En esta situación, el nivel de seguridad del proveedor en nube puede estar supeditado al nivel de seguridad de cada enlace y al grado de dependencia de terceros del proveedor en nube. Cualquier interrupción o corrupción de la cadena, así como la falta de coordinación de las responsabilidades entre las partes implicadas puede ocasionar: la no disponibilidad de los servicios, la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos, las pérdidas económicas y de renombre debidas a la incapacidad de cumplir las demandas del cliente, el incumplimiento de los Acuerdos de nivel de servicio, el fallo en el servicio de conexión en cascada, etc. Un ejemplo importante a este respecto es la existencia de una dependencia crítica de un servicio de gestión de identidad o de un inicio de sesión único de un tercero. En este caso, la interrupción del servicio del tercero o de la conexión del proveedor en nube al servicio o las deficiencias de sus

procedimientos de seguridad pueden poner en entredicho la disponibilidad o la confidencialidad de un cliente en nube, o de hecho, de toda la oferta en nube.

En general, la falta de transparencia en el contrato puede suponer un problema para la totalidad del sistema. Si un proveedor no declara los servicios básicos de TI que están subcontratados —no es realista que los proveedores indiquen los contratistas utilizados, puesto que estos pueden cambiar con frecuencia—, el cliente no está en situación de evaluar de manera adecuada el riesgo al que se enfrenta. Esta falta de transparencia puede reducir el nivel de confianza en el proveedor.

RIESGOS TÉCNICOS

R.8 AGOTAMIENTO DE RECURSOS (PRESTACIÓN EXCESIVA O INSUFICIENTE)

Probabilidad	**A**. Incapacidad para proporcionar capacidad adicional a un cliente: MEDIA	Comparativa: N/A
	B. Incapacidad para proporcionar el nivel de capacidad actual pactado: LEVE	Comparativa: Más alta
Impacto	**A**. Incapacidad para proporcionar capacidad adicional a un cliente: BAJA/MEDIA (por ejemplo, en Navidad)	Comparativa: N/D
	B. Incapacidad para proporcionar el nivel de capacidad actual pactado: ALTA	Comparativa: la misma
Vulnerabilidades	□. Modelado inadecuado del uso de recursos □. Provisión de recursos e inversiones en infraestructura inadecuadas □. ausencia de políticas de limitación de recursos □. Ausencia de redundancia de suministrador	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A10. Prestación del servicio A11. Control del acceso/autenticación/autorización (raíz/admin frente a otros)	
Riesgo	**MEDIO**	

Los servicios en nube son servicios bajo demanda [véase Computación en nube: definición operativa Por tanto, existe un nivel de riesgo calculado en la asignación de todos los recursos de un servicio en nube, puesto que los recursos se asignan en función de las proyecciones estadísticas. Un modelado poco apropiado de la utilización de recursos —los algoritmos de asignación de recursos comunes son vulnerables a la distorsión de la imparcialidad— o un aprovisionamiento de recursos e inversiones en infraestructura inadecuados puede dar lugar, desde la perspectiva del proveedor en nube, a:

- La no disponibilidad del servicio: los fallos en determinados escenarios de aplicación muy específicos que utilizan un recurso concreto de manera muy intensiva (es decir, simulación o procesamiento de números intensivo de memoria/CPU (por ejemplo, la previsión de precios de las existencias;)
- Poner en peligro el control del acceso: en ocasiones puede ser posible forzar el sistema para que se «abra en fallo» en caso de agotamiento de los recursos. [Ref.: CWE-400: Consumo de recursos incontrolado – Agotamiento de recursos (12)];
- Pérdidas económicas y de renombre: debidas a la incapacidad de hacer frente a la demanda de los clientes.
- Las consecuencias contrarias de una estimación imprecisa de las necesidades en términos de recursos puede dar lugar a:
- Sobredimensionamiento de la infraestructura: prestación excesiva que genera pérdidas económicas y pérdida de rentabilidad.

Desde la perspectiva del cliente en nube, una selección de proveedores deficiente y una falta de redundancia en el suministrador puede dar lugar a:

- La no disponibilidad del servicio: errores en la entrega (o rendimiento deficiente) de los servicios, tanto en tiempo real como en tiempo no real.
- Poner en peligro el sistema de control del acceso: comprometer la confidencialidad y la integridad de los datos;
- Pérdidas económicas y de renombre: a raíz de la incapacidad de hacer frente a la demanda de los clientes, incumplimiento del Acuerdo de nivel de servicio, error en el servicio de conexión en cascada, etc.

Nota: este riesgo también puede derivarse de un ataque DDoS (véase R. R. 15) y del mal funcionamiento de las aplicaciones debido a una compartimentación deficiente de la aplicación en algunos sistema de los proveedores en nube.

R.9 FALLO DE AISLAMIENTO

Probabilidad	BAJA (Nube privada) MEDIA (Nube pública)	Comparativa: Más alta
Impacto	MUY ALTO	Comparativa: Más alta
Vulnerabilidades	. Vulnerabilidades del hipervisor . Ausencia de aislamiento de los recursos . Falta de aislamiento de la reputación Posibilidad de que se realice un análisis interno de la red (en nube) . Posibilidad de que se realicen comprobaciones de corresidencia	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	**ALTO**	

La multiprestación y los recursos compartidos son dos de las características que definen los entornos de la computación en nube. La red, el almacenamiento y la capacidad de computación son compartidos entre múltiples usuarios.

Este tipo de riesgos incluye los errores de los mecanismos que separan el almacenamiento, la memoria, el enrutamiento e incluso el renombre entre distintos arrendatarios de la infraestructura compartida (por ejemplo, los denominados ataques de «guest-hopping», los ataques por inyección SQL que exponen los datos de múltiples clientes almacenados en la misma tabla y los ataques por vía alternativa).

Cabe señalar que la probabilidad de que se produzca este escenario de incidentes depende del modelo de nube considerado; es probable que sea bajo para las nubes privadas y mayor (medio) en el caso de nubes públicas.

El impacto puede ser una pérdida de datos sensibles o valiosos, perjuicios para el renombre e interrupción del servicio para los proveedores en nube y sus clientes.

R.10 MIEMBROS MALICIOSOS DE PROVEEDORES EN NUBE. ABUSO DE FUNCIONES PRIVILEGIADAS

Probabilidad	MEDIA (Más baja que la habitual)	Comparativa: Más baja
Impacto	MUY ALTO (Más alto que el habitual)	Comparativa: Más alta (total) Comparativa: La misma (para un único cliente)
Vulnerabilidades	□. Funciones y responsabilidades confusas □. Aplicación deficiente de las definiciones de funciones □. No aplicación del principio de «need-to-know» □. Vulnerabilidades AAA □. Vulnerabilidades del sistema o del sistema operativo □. Procedimientos de seguridad física inadecuados □. Imposibilidad de procesar datos codificados □. Vulnerabilidades de la aplicación o **GESTIÓN DE PARCHES INSUFICIENTE**	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A4. Datos personales sensibles A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A11. Control del acceso/autenticación/autorización (raíz/admin frente a otros)	
Riesgo	**ALTO**	

Las actividades maliciosas de un iniciado pueden repercutir sobre: la confidencialidad, la integridad y la disponibilidad de todos los tipos de datos, IP, todos los tipos de servicios, y por tanto, indirectamente sobre el renombre de la organización, la confianza del cliente y las experiencias de los empleados. Este aspecto puede considerarse especialmente importante en el caso de la computación en nube, debido a que las arquitecturas en nube necesitan determinadas funciones de alto riesgo. Entre los ejemplos de estas funciones se incluyen los administradores de sistema de los proveedores en nube y los proveedores de servicios de seguridad gestionada que se ocupan de los informes de detección de

intrusiones y de las respuestas a los incidentes. A medida que aumenta el uso de la nube, los empleados de los proveedores en nube se convierten cada vez más en objetivos de las bandas criminales (como ponen de manifiesto los trabajadores de los centros de llamadas del sector de servicios financieros (13), (14)).

R.11 COMPROMISO DE INTERFAZ DE GESTIÓN (MANIPULACIÓN, DISPONIBILIDAD DE LA INFRAESTRUCTURA)

Probabilidad	MEDIA	Comparativa: Más alta
Impacto	MUY ALTO	Comparativa: Más alta
Vulnerabilidades	□. Vulnerabilidades AAA □. Acceso remoto a la interfaz de gestión □. Configuración deficiente □. Vulnerabilidades del sistema o del sistema operativo □. Vulnerabilidades de la aplicación o **GESTIÓN DE PARCHES INSUFICIENTE**	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A14. Interfaz de gestión del servicio en nube	
Riesgo	**MEDIO**	

Las interfaces de gestión de cliente de un proveedor en nube público son accesibles a través de Internet, y canalizan el acceso a conjuntos de recursos más grandes (que los proveedores tradicionales de alojamiento), por lo que plantean un riesgo mayor, especialmente cuando se combinan con el acceso remoto y las vulnerabilidades del navegador de web. Aquí se incluyen las interfaces de cliente que controlan una serie de máquinas virtuales, y lo que es más importante, interfaces de proveedores en nube que controlan el funcionamiento de todo el sistema en nube. Es evidente que los proveedores pueden mitigar este riesgo incrementando la inversión en seguridad.

R.12 INTERCEPTACIÓN DE DATOS EN TRÁNSITO

Probabilidad	MEDIA	Comparativa: Más alta (para determinados datos concretos)
Impacto	ALTO	Comparativa: la misma
Vulnerabilidades	□. Vulnerabilidades AAA □. Vulnerabilidades en la codificación de la comunicación □. Falta o debilidad en la codificación de archivos y datos en tránsito □. Posibilidad de que se realice un análisis interno de la red (en nube) □. Posibilidad de que se realicen comprobaciones de corresidencia □. Falta de integridad y transparencia en los términos de uso	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A4. Datos personales sensibles A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A14. Datos de archivo o copia de seguridad	
Riesgo	**MEDIO**	

Al ser una arquitectura distribuida, la computación en nube implica más datos en tránsito que las infraestructuras tradicionales. Por ejemplo, los datos deben transferirse para sincronizar múltiples imágenes de máquinas distribuidas, imágenes distribuidas entre múltiples máquinas físicas, entre la infraestructura de nube y los clientes remotos de web, etc. Además, la mayor parte del uso del alojamiento de los centros de datos es implementada a través de un entorno de conexión segura de tipo VPN, una práctica que no siempre se sigue en el contexto de la nube

Los programas espía, la falsificación de IP, los ataques con intermediarios (MITM), los ataques por vía alternativa y los ataques en repetición deben considerarse posibles fuentes de amenaza.

Además, en ocasiones, el proveedor en nube no ofrece una cláusula de confidencialidad o de no

divulgación, o si lo hace, dichas cláusulas no ofrecen garantías suficientes de protección de la información secreta y los conocimientos del cliente que circularán por la nube.

R.13 FUGA DE DATOS DURANTE LA CARGA/DESCARGA DENTRO DE LA NUBE

Probabilidad	MEDIA (N/A)
Impacto	ALTO
Vulnerabilidades	□. Vulnerabilidades AAA □. Vulnerabilidades en la codificación de la comunicación □. Posibilidad de que se realice un análisis interno de la red (en nube) □. Posibilidad de que se realicen comprobaciones de corresidencia □. Imposibilidad de procesar datos codificados □. Vulnerabilidades de la aplicación o gestión de parches insuficiente
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A4. Datos personales sensibles A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A10. Credenciales A13. A11. A14. Interfaz de gestión del servicio en nube
Riesgo	**MEDIO**

Este es similar al riesgo anterior, pero se aplica a la transferencia de datos entre el proveedor en nube y el cliente en nube.

R.14 SUPRESIÓN DE DATOS INSEGURA O INEFICAZ

Probabilidad	MEDIA	Comparativa: Más alta

Impacto	Muy alto	Comparativa: Más alta
Vulnerabilidades	□. Limpieza de medios sensibles	
Activos afectados	A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A12. Credenciales	
Riesgo	**MEDIO**	

Cuando se cambia de proveedor, los recursos se escalan de forma descendente, el hardware físico se reubica, etc., y los datos pueden estar disponibles más allá de la vida indicada en la política de seguridad. Puede resultar imposible llevar a cabo los procedimientos especificados por la política de seguridad, puesto que la supresión total de los datos sólo es posible mediante la destrucción de un disco que también almacena datos de otros clientes. Cuando se realiza una solicitud para suprimir un recurso en nube, en ocasiones el proceso no elimina definitivamente los datos (al igual que con la mayoría de sistemas operativos). Si se requiere una supresión total de los datos, es necesario seguir procedimientos especiales, y puede que la API estándar no soporte esta función (o no pueda realizarse de ningún modo).
Si se utiliza una codificación satisfactoria, el nivel de riesgo puede considerarse inferior.

R.15 DISTRIBUCIÓN DE DENEGACIÓN DE SERVICIO (DDOS)

Probabilidad	Cliente: MEDIA	Comparativa: Más baja
	Proveedor: LEVE	Comparativa: N/A
Impacto	Cliente: ALTO	Comparativa: Más alta
	Proveedor: MUY ALTO	Comparativa: Más baja
Vulnerabilidades	□. Configuración deficiente □ Vulnerabilidades del sistema o del sistema operativo □. Recursos de filtrado inadecuados o mal configurados	
Activos afectados	A1. Renombre de la compañía A2. Confianza del cliente A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A14. Interfaz de gestión del servicio en nube A16.Red (conexiones, etc.)	
Riesgo	**MEDIO**	

R.16 DENEGACIÓN ECONÓMICA DE SERVICIO (EDOS)

Probabilidad	BAJA
Impacto	ALTO
Vulnerabilidades	□. Vulnerabilidades AAA □. Vulnerabilidades del alta de usuarios □ Vulnerabilidades de la baja de usuarios □.. Acceso remoto a la interfaz de gestión □. ausencia de políticas de limitación de recursos
Activos afectados	A1. Renombre de la compañía A2. Confianza del cliente A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	**MEDIO**

Existen distintos escenarios en los que los recursos del cliente en nube pueden ser utilizados por terceros de forma maliciosa, ocasionando repercusiones de índole económica:

- Usurpación de identidad: Un atacante utiliza una cuenta y los recursos del cliente para su propio beneficio o para perjudicar económicamente al cliente.
- El cliente en nube no ha delimitado de forma efectiva el uso de los recursos abonados y sufre cargas inesperadas en dichos recursos a través de acciones no maliciosas.
- Un atacante utiliza un canal público para acabar con los recursos medidos del cliente – por ejemplo, si el cliente paga por solicitud de HTTP, un ataque DDoS puede tener este efecto.

La EdoS destruye los recursos económicos; el peor escenario sería la quiebra del cliente o un impacto económico grave. NOTA: el activo general DINERO no se menciona en la lista.

R.17 PÉRDIDA DE LAS CLAVES DE CODIFICACIÓN

Probabilidad	BAJA	Comparativa: N/A
Impacto	ALTO	Comparativa: Más alta
Vulnerabilidades	□. Procedimientos insuficientes de gestión de claves □. Generación de claves: Baja entropía para la generación de números aleatorios	
Activos afectados	A4. Datos personales sensibles	

	A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A12. Credenciales
Riesgo	**MEDIO**

Aquí se incluye la divulgación de las claves secretas (SSL, codificación de archivos, claves privadas del cliente, etc.) o las contraseñas a las partes maliciosas, la pérdida o corrupción de dichas claves o su uso indebido para la autenticación y el no repudio (firma digital).

R.18 REALIZACIÓN DE ESCANEADOS O DETECCIONES MALICIOSAS

Probabilidad	MEDIA	Comparativa: Más baja
Impacto	MEDIO	Comparativa: Más baja
Vulnerabilidades	□. Posibilidad de que se realice un análisis interno de la red (en nube) □ Posibilidad de que se realicen comprobaciones de corresidencia	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	**MEDIO**	

El escaneado o la detección maliciosa, así como el mapeo de redes, son amenazas indirectas a los activos en cuestión. Pueden utilizarse para recabar información en el contexto de un intento de piratería. Uno de los posibles resultados podría ser la pérdida de la confidencialidad, integridad y disponibilidad de los servicios y datos.

R.19 MOTOR DE SERVICIO DE COMPROMISO

Probabilidad	BAJA
Impacto	MUY ALTO
Vulnerabilidades	□. Vulnerabilidades del hipervisor

	□ Ausencia de aislamiento de los recursos
Activos afectados	A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	MEDIO

Cada arquitectura de nube descansa en una plataforma altamente especializada: el motor de servicio que se sitúa por encima de los recursos físicos de hardware y gestiona los recursos del cliente con distintos niveles de abstracción. Por ejemplo, en las nubes IaaS, este componente del software puede ser el hipervisor. Este motor de servicio está desarrollado y soportado por los distribuidores de la plataforma en nube y la comunidad de código abierto en algunos casos. Los proveedores de computación en nube pueden personalizarlo todavía más.

Como cualquier otra capa de software, el código del motor de servicio puede tener vulnerabilidades, y es proclive a sufrir ataques o errores inesperados. Un atacante puede poner en peligro el motor de servicio accediendo a él sin autorización desde dentro de una máquina virtual (nubes IaaS), el entorno de ejecución (nubes PaaS), el conjunto de la aplicación (nubes SaaS) o a través de sus API.

El acceso no autorizado al motor de servicio puede servir para escapar al aislamiento entre distintos entornos de cliente (*jailbreak*) y acceder a los datos contenidos en los mismos, controlarlos y modificar la información almacenada dentro de los mismos de forma transparente (sin que haya una interacción directa con la aplicación dentro del entorno del cliente) o reducir los recursos asignados a los mismos, ocasionando una denegación de servicio.

R.20 CONFLICTOS ENTRE LOS PROCEDIMIENTOS DE REFUERZO DEL CLIENTE Y EL ENTORNO DE LA NUBE

Probabilidad	BAJA
Impacto	MEDIO
Vulnerabilidades	□.. Falta de integridad y transparencia en los términos de uso □. □.. Funciones y responsabilidades confusas
Activos afectados	A4. Datos personales sensibles

	A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos
Riesgo	BAJO

Los proveedores en nube deben delimitar claramente las responsabilidades de modo que se dispongan las medidas mínimas que los clientes deben adoptar. La incapacidad de los clientes de asegurar sus entornos de forma apropiada puede generar una vulnerabilidad para la plataforma de nube si el proveedor en nube no ha tomado las medidas necesarias para crear aislamiento. Los proveedores en nube deben articular de manera adicional sus mecanismos de aislamiento y ofrecer las mejores directrices prácticas para ayudar a los clientes a asegurar sus recursos.

Los clientes deben ser conscientes de sus responsabilidades y asumirlas, ya que de no hacerlo, sus datos y sus recursos correrán un mayor riesgo. En algunos casos, los clientes en nube no han asumido correctamente que el proveedor en nube era responsable de las actividades necesarias para garantizar la seguridad de los datos y que las estaba llevando a cabo. Esta hipótesis del cliente y/o la falta de una articulación clara por parte del proveedor en nube generan riesgos innecesarios para los datos del cliente. Es imperativo que los clientes en nube identifiquen sus responsabilidades y cumplan con ellas.

A raíz precisamente de su naturaleza, los proveedores en nube se encargan de proporcionar un entorno de multiprestación, ya sea a través de la virtualización de un servidor o de la red común que comparten los clientes. Es inevitable que la ubicación conjunta de muchos clientes genere conflictos para el proveedor en nube, ya que los requisitos de seguridad en la comunicación de los clientes normalmente difieren en función del cliente.

Si un cliente quiere que el cortafuegos de red bloquee todo el tráfico excepto la línea de comandos segura (SSH) pero otro cliente está gestionando una granja de servidores web y necesita permiso para el tráfico HTTP y HTTPS, ¿quién gana? Los clientes que poseen requisitos de cumplimiento divergentes y de competencia plantean el mismo tipo de cuestiones. Este tipo de reto empeora a medida que aumenta el número de clientes y la disparidad de sus requisitos. Por tanto, los proveedores en nube deben estar en situación de abordar estos retos mediante la tecnología, la política y la transparencia (si procede).

RIESGOS LEGALES

R.21 ÓRDENES JUDICIALES Y DESCUBRIMIENTO ELECTRÓNICO

Probabilidad	ALTA
Impacto	MEDIO
Vulnerabilidades	. Ausencia de aislamiento de los recursos Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto Falta de información sobre jurisdicciones
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	ALTO

En caso de confiscación de hardware físico a raíz de una orden judicial de las fuerzas policiales o de demandas civiles (15), la centralización del almacenamiento y el hecho de que varios clientes compartan el hardware físico implica que hay un número mayor de clientes que corren el riesgo de que sus datos se revelen a partes no deseadas (16), (17) y (18).
Al mismo tiempo, podría ser imposible que las fuerzas de una única nación confiscaran «una nube», a la vista de los avances pendientes en torno a la migración de hipervisor a larga distancia.

R.22 RIESGO DERIVADO DEL CAMBIO DE JURISDICCIÓN

Probabilidad	MUY ALTA
Impacto	ALTO
Vulnerabilidades	. Falta de información sobre jurisdicciones . Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto
Activos afectados	A1. A10Renombre de la compañía

	A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	ALTO

Los datos de los clientes pueden albergarse en múltiples jurisdicciones, algunas de las cuales pueden ser de alto riesgo. Si los centros de datos están ubicados en países de alto riesgo, por ejemplo, aquellos en los que no impera el Estado de derecho cuyo marco jurídico y ejecución de leyes son impredecibles, los Estados policiales autocráticos, los Estados que no respetan los acuerdos internacionales, etc., los sitios podrían ser objeto de incursiones de las autoridades locales y los datos o sistemas podrían ser divulgados o confiscados por la fuerza. Cabe señalar que, a este respecto, no queremos dar a entender que todas las medidas para el cumplimiento de la ley mediante órdenes judiciales sean inaceptables, sino simplemente que algunas pueden serlo, y que, en ocasiones, las confiscaciones legítimas de hardware (que parecen ser inusuales) pueden afectar a otros clientes que no son objeto de las actuaciones represivas, dependiendo del modo en que estén almacenados los datos (19) y (20).

R.23 RIESGOS DE LA PROTECCIÓN DE DATOS

Probabilidad	ALTA
Impacto	ALTO
Vulnerabilidades	□ Falta de información sobre jurisdicciones □. Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	ALTO

La computación en nube plantea varios riesgos relativos a la protección de datos tanto para clientes en nube como para proveedores en nube.

- En algunos casos, puede ser difícil para el cliente en nube (en su función de controlador de datos) comprobar de manera eficaz el procesamiento de datos que lleva a cabo el proveedor

en nube, y en consecuencia, tener la certeza de que los datos se gestionan de conformidad con la ley. Tiene que quedar claro que el cliente en nube será el principal responsable del procesamiento de los datos personales, incluso cuando dicho procesamiento lo realice el proveedor en nube en su papel de procesador externo. El incumplimiento de la legislación en materia de protección de datos puede dar lugar a la imposición de sanciones administrativas, civiles e incluso penales, que varían en función del país, al controlador de datos. Este problema se ve exacerbado en los casos de transferencias múltiples de datos, por ejemplo, entre nubes federadas. Por otra parte, algunos proveedores en nube sí proporcionan información sobre sus prácticas de procesamiento de datos. Otros también ofrecen resúmenes de certificación sobre sus actividades de procesamiento y seguridad de datos y los controles de datos a que se someten, por ejemplo, los proveedores que poseen certificación SAS 70.

- Pueden producirse infracciones de la seguridad de los datos que el proveedor en nube no notifique al controlador.
- El cliente en nube puede perder el control de los datos procesados por el proveedor en nube. Este problema aumenta en los casos de transferencias múltiples de datos (por ejemplo, entre nubes federadas).
- El proveedor en nube puede recibir datos que no hayan sido recabados legalmente por su cliente (el controlador).

R.24 RIESGOS RELATIVOS A LA LICENCIA

Probabilidad	MEDIA	Comparativa: Más alta
Impacto	MEDIO	Comparativa: Más alta
Vulnerabilidades	□. Falta de integridad y transparencia en los términos de uso	
Activos afectados	A1. A10Renombre de la compañía A9. Prestación del servicio – servicios en tiempo real A20. Certificación	
Riesgo	MEDIO	

Las condiciones de la licencia, como los acuerdos por puesto, y las comprobaciones de las licencias en línea pueden no ser factibles en un entorno de nube. Por ejemplo, si el software se carga por instancia cada vez que una máquina nueva es instanciada, los gastos de licencia para el cliente en nube podrían aumentar exponencialmente, a pesar de estar utilizando el mismo número de máquinas durante el mismo período. En el caso de PaaS e IaaS, existe la posibilidad de crear trabajo original en la nube

(nuevas aplicaciones, software, etc.). Al igual que con la propiedad intelectual, si no se encuentra protegido por las cláusulas contractuales apropiadas (véase ANEXO I – Computación en nube – Cuestiones legales clave, Propiedad Intelectual), este trabajo original puede verse amenazado.

RIESGOS NO ESPECÍFICOS DE LA NUBE

Durante el curso de nuestro análisis de riesgo, identificamos las siguientes amenazas no específicas de la computación en nube, pero que deben considerarse detenidamente a la hora de evaluar el riesgo de un sistema típico basado en la nube.

R.25 BRECHAS EN LA RED

Probabilidad	BAJA	Comparativa: la misma
Impacto	MUY ALTO	Comparativa: Más alta
Vulnerabilidades	□.. Configuración deficiente □. Vulnerabilidades del sistema o del sistema operativo □. Ausencia de aislamiento de los recursos □ Software que no es de confianza	
Activos afectados	A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio	
Riesgo	MEDIO	

Es uno de los mayores riesgos. Miles de clientes se ven potencialmente afectados al mismo tiempo.

R.26 GESTIÓN DE LA RED (CONGESTIÓN DE LA RED/FALLO EN LA CONEXIÓN/USO NO ÓPTIMO)

Probabilidad	MEDIA	Comparativa: la misma
Impacto	MUY ALTO	Comparativa: Más alta
Vulnerabilidades	□. Configuración deficiente □. Vulnerabilidades del sistema o del sistema operativo □ Ausencia de aislamiento de los recursos □. Software que no es de confianza	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente	

	A3. Fidelidad y experiencia del empleado A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A16. Red (conexiones, etc.)
Riesgo	**ALTO**

R.27 MODIFICACIÓN DEL TRÁFICO DE LA RED

Probabilidad	BAJA
Impacto	ALTO
Vulnerabilidades	□. Vulnerabilidades del alta de usuarios □. Vulnerabilidades de la baja de usuarios □. Vulnerabilidades en la codificación de la comunicación □. Falta de control en el proceso de evaluación de vulnerabilidad
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	MEDIO

R.28 ESCALADA DE PRIVILEGIOS

Probabilidad	BAJA	Comparativa: Más baja
Impacto	ALTO	Comparativa: Más alta (para el proveedor en nube)
Vulnerabilidades	□. Vulnerabilidades AAA □.. Vulnerabilidades del alta de usuarios □. Vulnerabilidades de la baja de usuarios □. Vulnerabilidades del hipervisor □. Funciones y responsabilidades confusas □. Aplicación deficiente de las definiciones de funciones □. No aplicación del principio de «need-to-know»	

	□. Configuración deficiente
Activos afectados	A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A11. Control del acceso/autenticación/autorización (raíz/admin frente a otros) A14. Directorio de usuarios (datos)
Riesgo	MEDIO

R.29 ATAQUES DE INGENIERÍA SOCIAL (SUPLANTACIÓN)

Probabilidad	MEDIA	Comparativa: la misma
Impacto	ALTO	Comparativa: Más alta
Vulnerabilidades	□. Ausencia de conciencia de seguridad □. Vulnerabilidades del alta de usuarios □ Ausencia de aislamiento de los recursos □. Vulnerabilidades en la codificación de la comunicación □ Procedimientos de seguridad física inadecuados	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A3. Fidelidad y experiencia del empleado A4. Datos personales sensibles A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A11. Control del acceso/autenticación/autorización (raíz/admin frente a otros) A14.	
Riesgo	MEDIO	

R.30 PÉRDIDA O COMPROMISO DE LOS REGISTROS OPERATIVOS

Probabilidad	BAJA	Comparativa: Más baja
Impacto	MEDIO	Comparativa: La misma (para el cliente)
Vulnerabilidades	□. Responsabilidad por pérdida de datos □. Vulnerabilidades AAA □. Vulnerabilidades del alta de usuarios □. Vulnerabilidades de la baja de usuarios □. Ausencia de disponibilidad experta □. Vulnerabilidades del sistema o del sistema operativo	
Activos afectados	0. Registros operativos (proveedor en nube y cliente)	
Riesgo	BAJO	

R.31 PÉRDIDA O COMPROMISO DE LOS REGISTROS DE SEGURIDAD (MANIPULACIÓN DE LA INVESTIGACIÓN EXPERTA)

Probabilidad	BAJA	Comparativa: Más baja
Impacto	MEDIO	Comparativa: La misma (para el cliente)
Vulnerabilidades	□. Responsabilidad por pérdida de datos □. Vulnerabilidades AAA □. Vulnerabilidades del alta de usuarios □. Vulnerabilidades de la baja de usuarios □. Ausencia de disponibilidad experta □. Vulnerabilidades del sistema o del sistema operativo	
Activos afectados	0. Registros de seguridad	
Riesgo	BAJO	

R.32 PÉRDIDA O ROBO DE LAS COPIAS DE SEGURIDAD

Probabilidad	BAJA	Comparativa: Más baja
Impacto	ALTO	Comparativa: La misma (para el cliente)
Vulnerabilidades	□. Procedimientos de seguridad física inadecuados □. Vulnerabilidades AAA □. Vulnerabilidades del alta de usuarios □. Vulnerabilidades de la baja de usuarios	

Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A23. Datos de archivo o copia de seguridad
Riesgo	MEDIO

R.33 ACCESO NO AUTORIZADO A LOS LOCALES (INCLUIDO EL ACCESO FÍSICO A LAS MAQUINAS Y OTRAS INSTALACIONES)

Probabilidad	MUY BAJA	Comparativa: Más baja
Impacto	ALTO (para conseguir un impacto muy alto, debe tratarse de un ataque con un objetivo concreto (apuntando a una máquina concreta, etc.); de otro modo, el impacto será alto.	Comparativa: Más alta
Vulnerabilidades	. Procedimientos de seguridad física inadecuados	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A23. Datos de archivo o copia de seguridad	
Riesgo	BAJO	

Dado que los proveedores en nube concentran los recursos en grandes centros de datos, y aunque es probable que los controles del perímetro físico sean más potentes, el impacto de la corrupción de estos controles será mayor.

R.34 ROBO DE EQUIPOS INFORMÁTICOS

Probabilidad	MUY BAJA	Comparativa: Más baja
Impacto	ALTO	Comparativa: Más alta
Vulnerabilidades	.. Procedimientos de seguridad física inadecuados	
Activos afectados	A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A17. Hardware físico	
Riesgo	BAJO	

R.35 CATÁSTROFES NATURALES

Probabilidad	MUY BAJA	Comparativa: Más baja
Impacto	ALTO	Comparativa: Más alta
Vulnerabilidades	. Software que no es de confianza	
Activos afectados	A1. A10Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A8. Datos de recursos humanos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio A23. Datos de archivo o copia de seguridad	
Riesgo	BAJO	

En términos generales, el riesgo de que se produzcan catástrofes naturales es más bajo, en comparación con las infraestructuras tradicionales, ya que los proveedores en nube ofrecen múltiples sitios redundantes y rutas de red por defecto.

4. VULNERABILIDADES

La lista siguiente de vulnerabilidades no es exhaustiva pero, sin embargo, sí resulta suficientemente detallada para el propósito de nuestro análisis. Contiene información sobre vulnerabilidades de seguridad, tanto específicas de la nube como generales.

- **VULNERABILIDADES AAA**

Un sistema pobre de autenticación, autorización y auditoría podría facilitar el acceso no autorizado a recursos, el aumento de privilegios, la imposibilidad de rastrear el uso indebido de recursos y de incidentes de seguridad en general, etc., a través de:

- almacenamiento inseguro de las credenciales de acceso a la nube por parte del cliente:
- funciones disponibles insuficientes;
- credenciales almacenadas en un equipo transitorio.

Además, la nube hace que los ataques de autenticación basados en contraseñas (práctica fraudulenta que utiliza un troyano para robar contraseñas corporativas) tengan un impacto mucho mayor, ya que las aplicaciones corporativas ahora están expuestas en Internet. Por tanto, la autenticación basada en contraseñas llegará a ser insuficiente y será necesaria una autenticación más robusta o de dos factores para acceder a los recursos en nube.

- **VULNERABILIDADES DEL ALTA DE USUARIOS**

- El cliente no puede controlar el proceso de altas.
- La identidad del cliente no se verifica de manera adecuada en el registro.
- Aparecen retrasos en la sincronización entre los componentes del sistema en nube (temporales y del contenido del perfil).
- Se realizan copias múltiples y no sincronizadas de datos de identidad.
- Las credenciales son vulnerables a la intercepción y a la copia.

- **VULNERABILIDADES DE LA BAJA DE USUARIOS**

Las credenciales dadas de baja todavía son válidas debido a un retraso en la descarga de la revocación.

- **ACCESO REMOTO A LA INTERFAZ DE GESTIÓN**

En teoría, esto permite que las vulnerabilidades en equipos terminales comprometan la infraestructura en nube (cliente individual o proveedor en nube), mediante, por ejemplo, una autenticación débil de las respuestas y las solicitudes.

- **VULNERABILIDADES DEL HIPERVISOR**

Los ataques a la capa del hipervisor son muy atractivos: el hipervisor, de hecho, controla totalmente los recursos físicos y los equipos virtuales que se ejecutan sobre él, así que cualquier vulnerabilidad en esta capa es extremadamente crítica. Explotar una vulnerabilidad del hipervisor equivale potencialmente a explotar todos los equipos virtuales. La primera prueba de concepto de un ataque contra un hipervisor desde una capa inferior la ofrecieron King (y otros) en un artículo (21), en el que los autores introducen el concepto de *rootkit* basado en un equipo virtual. Por entonces, habían sido identificadas algunas vulnerabilidades en los hipervisores más populares (por ejemplo, (22) y (23)), que pueden explotarse sin derechos de acceso de administrador, pero en el momento de redactar este documento no se había aportado ninguna solución para cambiar sus resultados.

Un escenario habitual que permite la explotación de una vulnerabilidad del hipervisor es el llamado *«guest to host escape»*, ejemplo del cual es el «*cloudburst*», una vulnerabilidad del VMware descubierta recientemente y documentada en la referencia (24). Otro escenario es el «*VM hopping*»: en el que el atacante accede ilegalmente a un equipo terminal utilizando algún método estándar y entonces, explotando alguna vulnerabilidad del hipervisor, pasa a controlar otros equipos virtuales que estén ejecutándose en el mismo hipervisor. Para más información, véase: *Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments*, (25).

- **AUSENCIA DE AISLAMIENTO DE LOS RECURSOS**

El uso de recursos por un cliente puede afectar al uso de recursos por otro cliente.

Las infraestructuras de computación en nube IaaS dependen mayoritariamente de diseños de arquitectura en los que los recursos físicos se comparten entre múltiples equipos virtuales, y por tanto, múltiples clientes.

Las vulnerabilidades en el modelo de seguridad del hipervisor pueden conducir a un acceso no autorizado a estos recursos compartidos. Por ejemplo, los equipos virtuales del cliente 1 y el cliente 2 tienen sus discos duros virtual guardados en el mismo LUN (número de unidad lógica) compartido dentro de una red de área de almacenamiento (SAN). El cliente 2 puede ser capaz de mapear el disco duro virtual del cliente 1 en su equipo virtual y ver y utilizar los datos que contiene.

Los hipervisores utilizados en nubes IaaS ofrecen API integradas, que el proveedor en nube utiliza para desarrollar una interfaz de gestión de la propiedad, de provisión y de información que está expuesta a sus clientes. Las vulnerabilidades en el modelo de seguridad del hipervisor o en las«interfaces de gestión» pueden llevar a un acceso no autorizado a la información del cliente. Al mismo tiempo, una vulnerabilidad en este nivel puede permitir a un atacante manipular los recursos de una instalación en nube, provocando una denegación de servicio (por ejemplo, apagado de equipos virtuales en ejecución), fuga de datos (por ejemplo, la copia y la transferencia fuera de la nube de equipos virtuales), datos comprometidos (por ejemplo, reemplazo de equipos virtuales con copias modificadas) o daños financiero directos (por ejemplo, réplica y ejecución de numerosas copias de los equipos virtuales).

Además, la falta de controles en la cartografía y la corresidencia de la nube y las vulnerabilidades del canal contrario (véase (26)) pueden plantear graves riesgos al aislamiento de recursos. Por ejemplo, si el uso de recursos no es independiente entre el cliente 1 y el cliente 2, el cliente 1 puede mapear los recursos del cliente 2. Esto puede hacerse, por ejemplo, utilizando una carga controlada de los recursos del cliente 2 al tiempo que se observan los cambios en los patrones de disponibilidad de recursos del cliente 1.

Por último, la falta de herramientas para hacer cumplir un término de servicio (ToS) o un Acuerdo de nivel de servicio (SLA) más específico, como la calidad de servicio (CdS) o los productos de planificación de recursos distribuidos (DRS) podrían permitir a un cliente monopolizar el uso de la nube, con impactos a otros clientes en forma de denegación de servicio o rendimiento pobre.

- **FALTA DE AISLAMIENTO DE LA REPUTACIÓN**

Las actividades de un cliente pueden afectar a la reputación de otro cliente.

- **VULNERABILIDADES EN LA CODIFICACIÓN DE LA COMUNICACIÓN**

Estas vulnerabilidades se refieren a la posibilidad de leer datos en tránsito, por ejemplo, ataques con intermediarios (MITM), autenticación pobre, aceptación de certificados autofirmados, etc.

- **FALTA O DEBILIDAD EN LA CODIFICACIÓN DE ARCHIVOS Y DATOS EN TRÁNSITO**

El no codificar los datos en tránsito, los datos mantenidos en archivos y bases de datos, las imágenes de equipos virtuales sin montar, las imágenes y datos forenses, los registros importantes y otros datos

estáticos pone en riesgo los datos. Por supuesto, el coste de poner en marcha la gestión de claves [□] y los de procesamiento deben ser considerados en relaci? con el riesgo que se genera para la empresa.

- **IMPOSIBILIDAD DE PROCESAR DATOS CODIFICADOS**

La codificación de datos estáticos no es difícil, pero a pesar de los avances recientes en codificación homomórfica (27) no hay indicios de un sistema comercial capaz de mantener esta codificación durante el procesamiento. En un artículo, Craig Gentry considera que realizar una búsqueda de Internet con palabras clave codificadas —una aplicación perfectamente razonable de este algoritmo— incrementaría el tiempo de computación aproximadamente un billón de veces (28). Esto quiere decir que, durante un largo tiempo, los clientes en nube que realicen cualquier actividad diferente a almacenar información en la nube deben confiar en el proveedor en nube.

- **PROCEDIMIENTOS INSUFICIENTES DE GESTIÓN DE CLAVES**

Las infraestructuras de computación en nube requieren la gestión y el almacenamiento de muchos tipos distintos de claves, entre los que, por ejemplo, se incluyen claves de sesión para proteger datos en tránsito (por ejemplo, claves SSL), claves de codificación de archivos, pares de claves para identificar proveedores en nube, pares de claves para identificar clientes, símbolos de autorización y certificados de revocación (29). Debido a que los equipos virtuales no tienen una infraestructura de hardware fija y el contenido basado en nube tiende a estar distribuido geográficamente, es más difícil aplicar controles estándar, como el almacenamiento HSM (módulo de seguridad hardware), en las infraestructuras en nube. Por ejemplo:

- Los HSM tienen necesariamente una fuerte protección física (contra robos, escuchas y falsificaciones). Esto hace que sea muy difícil distribuirlos a lo largo de las múltiples ubicaciones utilizadas en las arquitecturas en nube (es decir, distribuidos geográficamente y con un alto grado de replicación). Las normas de gestión de claves como PKCS#10 y las normas asociadas como PKCS#11 (30) no ofrecen entornos normalizados para interactuar con sistemas distribuidos.

- Las interfaces de gestión de claves accesibles a través de la Internet pública (incluso indirectamente) son más vulnerables, ya que la seguridad se reduce en el canal de comunicación entre el usuario y el almacenamiento de claves de nube y los mecanismos de autenticación remota mutua utilizados.

- Los nuevos equipos virtuales que necesitan autenticarse a ellos mismos deben ser creados con cierto secretismo. La distribución de esos secretos puede presentar problemas de

escalabilidad. La rápida escalada de autoridades de certificación que emiten pares de claves se logra fácilmente si se determinan los recursos por anticipado, pero la escalada dinámica y sin planificar de las autoridades de responsabilidades jerárquicas es difícil de lograr debido al gasto de recursos para crear nuevas autoridades (registro o certificación, autenticando nuevos componentes y distribuyendo nuevas credenciales, etc.).

- La revocación de claves en una arquitectura distribuida también es costosa. La revocación efectiva implica esencialmente que las aplicaciones comprueben el estatus de la clave (un certificado, normalmente) de acuerdo con un límite temporal conocido que determina la ventana de riesgo. Aunque existen mecanismos distribuidos para conseguir esto (véase, por ejemplo, (31) y (32)), constituye un reto asegurar que las diferentes partes de la nube reciban un nivel equivalente de servicio para que se asocien a niveles de riesgo diferentes. Las soluciones centralizadas, como los OCSP, son caras y no reducen necesariamente el riesgo, a no ser que la autoridad de certificación y la lista de revocación de certificados estén estrechamente conectados.

- **GENERACIÓN DE CLAVES: BAJA ENTROPÍA PARA LA GENERACIÓN DE NÚMEROS ALEATORIOS**

La combinación de imágenes de sistema estándar, tecnologías de virtualización y una falta de dispositivos de entrada significa que los sistemas tienen mucha menos entropía que los RNG físicos (véase **Seguridad de la computación en nube** (33)). Ello significa que un atacante en un equipo virtual puede ser capaz de averiguar las claves de codificación generadas en otros equipos virtuales, porque las fuentes de entropía utilizadas para generar números aleatorios pueden ser similares. No es un problema difícil de solucionar, pero si no se toma en consideración durante el diseño del sistema puede tener consecuencias importantes.

- **FALTA DE TECNOLOGÍAS Y SOLUCIONES ESTÁNDAR**

Una falta de medios estándar significa que los datos pueden estar «ligados» a un proveedor. Es un riesgo importante si el proveedor cesa sus operaciones.

Esto puede frenar el uso de servicios de gestión de seguridad y tecnologías de seguridad externa como la gestión federada de la identidad (FIM).

- **AUSENCIA DE UN ACUERDO DE DEPÓSITO DE FUENTES**

La falta de un depósito de fuentes significa que si un proveedor PaaS o SaaS quiebra, sus clientes no están protegidos.

- **MODELADO INADECUADO DEL USO DE RECURSOS**

Los servicios en nube son particularmente vulnerables al agotamiento de recursos debido a que no se provisionan estadísticamente. Aunque muchos proveedores permiten que los clientes reserven recursos con antelación, los algoritmos de provisión de recursos pueden fallar debido a:

- modelado inadecuado del uso de recursos, que puede llevar a un exceso de reserva o de provisión (lo que, a su vez, lleva a un derroche de recursos por parte del proveedor en nube). *Token Bucket* (34), *Fair Queuing* (35) y *Class Based Queuing* (36) son algoritmos reputados de asignación de recursos. Estos algoritmos son vulnerables a distorsiones de equidad; por ejemplo, véase (37).
- fallo de los algoritmos de asignación de recursos debido a eventos extraordinarios (por ejemplo, eventos de noticias remotas para la entrega de contenido).
- fallo de los algoritmos de asignación de recursos que utilizan clasificación de tareas o paquetes debido a que los recursos están clasificados de manera insuficiente.
- fallo en la provisión general de recursos (en oposición a las sobrecargas temporales).

- **FALTA DE CONTROL EN EL PROCESO DE EVALUACIÓN DE VULNERABILIDAD**

Las restricciones al escaneado de puertos y los tests de vulnerabilidad son una vulnerabilidad importante que, en combinación con una condición de uso que haga responsable al cliente de asegurar los elementos de la infraestructura, constituye un problema grave de seguridad.

- **POSIBILIDAD DE QUE SE REALICE UN ANÁLISIS INTERNO DE LA RED (EN NUBE)**

Los clientes en nube pueden llevar a cabo escaneados de puertos y otras pruebas en otros clientes dentro de la red interna.

- **POSIBILIDAD DE QUE SE REALICEN COMPROBACIONES DE CORRESIDENCIA**

Los ataques por vía alternativa que aprovechan una falta de aislamiento de los recursos permiten a los atacantes determinar qué recursos están compartidos por qué clientes.

- **AUSENCIA DE DISPONIBILIDAD EXPERTA**

A pesar de que la nube tiene el potencial de mejorar la disponibilidad experta, muchos proveedores no ofrecen servicios y términos de uso apropiados para permitirlo. Por ejemplo, los proveedores SaaS normalmente no permiten el acceso al registro de IP de los clientes que acceden a contenidos. Los proveedores IaaS pueden no ofrecer servicios expertos como equipos virtuales recientes e imágenes de disco.

- **LIMPIEZA DE MEDIOS SENSIBLES**

La tenencia compartida de recursos de almacenamiento físico significa que puede haber fuga de datos sensibles debido a que bien las políticas de destrucción de datos aplicables al final de un ciclo de vida pueden ser imposibles de aplicar debido a que, por ejemplo, los medios no pueden ser destruidos físicamente porque un disco está todavía en uso por otro propietario o no puede localizarse, bien no hay un procedimiento aplicable.

- **SINCRONIZACIÓN DE LAS RESPONSABILIDADES O LAS OBLIGACIONES CONTRACTUALES EXTERNAS A LA NUBE**

Frecuentemente, los clientes en nube no son conscientes de las responsabilidades que asumen en las condiciones de servicio. Hay una tendencia a atribuir erróneamente al proveedor en nube la responsabilidad de actividades como la codificación de archivos, incluso aunque esté claramente señalado en los términos del contrato entre las dos partes que no se ha asumido ninguna responsabilidad de ese tipo.

- **APLICACIONES INTER-NUBE QUE CREAN DEPENDENCIA OCULTA**

En la cadena de suministro (dependencias intra y extranube) existen dependencias ocultas y la arquitectura del proveedor en nube no ofrece operaciones continuas desde la nube cuando las terceras partes implicadas, subcontratistas o la compañía cliente, han sido separadas del proveedor del servicio y viceversa.

- **CLÁUSULAS SLA CON COMPROMISOS EN CONFLICTO PARA CON DIFERENTES PARTES**

Las cláusulas SLA también pueden estar en conflicto con compromisos enunciados en otras cláusulas o en cláusulas de otros proveedores.

- **CLÁUSULAS SLA QUE CONTIENEN UN RIESGO DE NEGOCIO EXCESIVO**

Los SLA pueden acarrear demasiado riesgo de negocio para un proveedor, dado el riesgo real de fallos técnicos. Desde el punto de vista del cliente, los SLA pueden contener cláusulas que resulten ser perjudiciales; por ejemplo, en el terreno de la propiedad intelectual, un SLA puede especificar que el proveedor en nube posee los derechos de cualquier material almacenado en la infraestructura en nube.

- **AUDITORÍA O CERTIFICACIÓN NO DISPONIBLE PARA LOS CLIENTES**

El proveedor en nube no puede ofrecer ninguna garantía al cliente vía una certificación de auditoría.

Por ejemplo, algunos proveedores en nube están utilizando hipervisores de código abierto o versiones adaptadas de los mismos (por ejemplo, Xen (38)), que no han alcanzado ninguna certificación de criterios comunes (39), lo que constituye un requisito fundamental para algunas organizaciones (por ejemplo, las agencias del Gobierno de EE.UU.).

Por favor tenga en cuenta que no estamos afirmando que exista una correlación directa entre certificación y nivel de vulnerabilidad (dado que no tenemos suficiente información sobre la protección de perfiles y los objetivos de seguridad de los productos certificados).

- **SISTEMAS DE CERTIFICACIÓN NO ADAPTADOS A LAS INFRAESTRUCTURAS DE NUBE**

No existe ningún control específico de nube, lo que quiere decir que las vulnerabilidades de seguridad probablemente pasarán desapercibidas.

- **PROVISIÓN DE RECURSOS E INVERSIONES EN INFRAESTRUCTURA INADECUADAS**

Las inversiones en infraestructura llevan tiempo. Si los modelos predictivos fallan, el servicio del proveedor en nube puede fallar durante un período largo.

- **AUSENCIA DE POLÍTICAS DE LIMITACIÓN DE RECURSOS**

Si no existe un modo flexible y configurable para que el cliente y/o el proveedor en nube establezcan límites sobre los recursos, puede haber problemas cuando el uso de recursos sea impredecible.

- **ALMACENAMIENTO DE DATOS EN JURISDICCIONES MÚLTIPLES Y FALTA DE TRANSPARENCIA SOBRE ESTE PUNTO**

Los servicios de datos en espejo para su entrega a través de redes de proximidad y almacenamiento redundante sin información en tiempo real sobre dónde se almacenan los datos disponible para el consumidor introduce un nivel de vulnerabilidad. Las empresas pueden incumplir las normas inconscientemente, especialmente si no se ofrece información clara sobre la jurisdicción del almacenamiento.

- **FALTA DE INFORMACIÓN SOBRE JURISDICCIONES**

Los datos pueden almacenarse y/o procesarse en jurisdicciones de alto riesgo, donde son vulnerables a la confiscación por medio de una entrada forzada. Si esta información no se encuentra disponible para los clientes en nube, no pueden tomar medidas para evitarlo.

- **FALTA DE INTEGRIDAD Y TRANSPARENCIA EN LOS TÉRMINOS DE USO**

VULNERABILIDADES NO ESPECÍFICAS DE LA NUBE

Durante nuestro análisis de riesgos, hemos identificado las siguientes vulnerabilidades que no son específicas de la computación en nube pero que, sin embargo, deben tenerse muy en cuenta al evaluar un sistema típico planteado en nube.

- **AUSENCIA DE CONCIENCIA DE SEGURIDAD**

Los clientes en nube no son conscientes de los riesgos que podrían afrontar al migrar hacia la nube, en particular aquellos riesgos generados a partir de amenazas específicas de la nube, es decir, pérdida de control, cierre de la empresa proveedora, agotamiento de recursos del proveedor en nube, etc. Esta falta de conciencia también podría afectar al proveedor en nube, que puede no ser consciente de las medidas que debería tomar para mitigar estos riesgos.

- **Falta de procesos de investigación**

Dado que pueden existir funciones de alto privilegio en los proveedores en nube, debido a la escala implicada, la ausencia de, o una inadecuada investigación sobre el perfil de riesgo del personal con dichas funciones es una vulnerabilidad importante.

- **Funciones y responsabilidades confusas**

Estas vulnerabilidades se refieren a la atribución inadecuada de funciones y responsabilidades en la organización del proveedor en nube.

- **Aplicación deficiente de las definiciones de funciones**

En el proveedor en nube, una separación inadecuada de funciones puede conducir a roles excesivamente privilegiados que pueden convertir a los sistemas muy grandes en vulnerables. Por ejemplo, ninguna persona debería tener privilegios de acceso a toda la nube.

- **No aplicación del principio de «need-to-know»**

Éste es un tipo especial de vulnerabilidad relativa a los roles y las responsabilidades. No debería darse un acceso a los datos innecesarios a las partes. De otro modo, ello constituye un riesgo innecesario.

- **Procedimientos de seguridad física inadecuados**

Pueden incluir:

- falta de controles sobre el perímetro físico (tarjeta inteligente de autenticación en la entrada);
- falta de escudo electromagnético para los activos críticos vulnerables a escuchas.

- **Configuración deficiente**

Esta clase de vulnerabilidades incluye: aplicación inadecuada de una línea base de seguridad y procedimientos de aumento de la resistencia a los fallos, error humano y administrador no formado.

- VULNERABILIDADES DEL SISTEMA O DEL SISTEMA OPERATIVO
- SOFTWARE QUE NO ES DE CONFIANZA
- FALTA DE PLAN CONTINUIDAD DEL NEGOCIO Y DE RECUPERACIÓN DE DESASTRES, O PLAN DEFICIENTE Y NO PUESTO A PRUEBA
- FALTA DE INVENTARIO DE ACTIVOS (O INCOMPLETO O INADECUADO)
- FALTA DE PLAN CONTINUIDAD DEL NEGOCIO Y DE RECUPERACIÓN DE DESASTRES, O PLAN DEFICIENTE Y NO PUESTO A PRUEBA
- PROPIEDAD DE LOS ACTIVOS CONFUSA
- IDENTIFICACIÓN INSUFICIENTE DE LOS REQUISITOS DE PROYECTO

Incluye una falta de consideración de los requisitos de seguridad y de cumplimiento legal, falta de implicación del usuario en los sistemas y las aplicaciones, requisitos de negocio confusos o inadecuados, etc.

- SELECCIÓN DE PROVEEDORES INSUFICIENTE
- AUSENCIA DE REDUNDANCIA DE SUMINISTRADOR
- VULNERABILIDADES DE LA APLICACIÓN O GESTIÓN DE PARCHES INSUFICIENTE

Esta clase de vulnerabilidades incluye: errores en el código de la aplicación, procedimientos de parcheado conflictivos entre el proveedor y el cliente, aplicación de parches no examinados, vulnerabilidades en los navegadores, etc.

- VULNERABILIDADES EN EL CONSUMO DE RECURSOS
- INCUMPLIMIENTO DEL ACUERDO DE NO DIVULGACIÓN POR EL PROVEEDOR
- RESPONSABILIDAD POR PÉRDIDA DE DATOS
- FALTA DE POLÍTICAS O PROCEDIMIENTOS INSUFICIENTES PARA LA RECOPILACIÓN Y RETENCIÓN DE REGISTROS
- RECURSOS DE FILTRADO INADECUADOS O MAL CONFIGURADOS

5. ACTIF

Activo	Descripción o referencia a elementos descritos anteriormente	Propietario *[interlocutores u organizaciones implicadas]*	Valor percibido *[Escala: MUY BAJO - BAJO - MEDIO - ALTO - MUY ALTO]*
A1. Renombre de la compañía		Cliente en nube	**MUY ALTO**
A2. Confianza del cliente	Incluye buena disposición y puede medirse en función de las reclamaciones	Cliente en nube	**MUY ALTO**
A3. Fidelidad y experiencia del empleado		Cliente en nube	**ALTO**
A4. Propiedad intelectual		Cliente en nube	**ALTO**
A5. Datos personales sensibles	(definidos en la Directiva europea sobre protección de datos)	Proveedor en nube/Cliente en nube	**MUY ALTO** (ya que incluye datos sobre los usuarios del sistema interno de atención)
A6. Datos personales	(definidos en la Directiva europea sobre protección de datos)	Proveedor en nube/Cliente en nube	**MEDIO** (valor operativo) / **ALTO** (valor en caso de pérdida)
A7. Datos personales - críticos	(todos los datos incluidos en la categoría de Datos Personales con arreglo a la Directiva europea sobre protección de datos y que están clasificados como CRÍTICOS por la organización o compañía)	Proveedor en nube/Cliente en nube	**ALTO** (valor operativo) **/ ALTO** (valor en caso de pérdida)

A8. Datos de recursos humanos	Datos pertinentes desde la perspectiva operativa, además de los requisitos relativos a la Protección de datos	Cliente en nube	**ALTO**
A9. Prestación del servicio – servicios en tiempo real	Todos los servicios críticos en cuanto al tiempo y que necesitan un nivel de disponibilidad cercano al 100 %	Proveedor en nube/Cliente en nube	**MUY ALTO**
A10. Prestación del servicio		Proveedor en nube/Cliente en nube	**MEDIO**
A11. Control del acceso/autenticación/autorización (raíz/admin frente a otros)		Proveedor en nube/Cliente en nube	**ALTO**
A12. Credenciales	De los pacientes y del personal que accede al sistema	Cliente en nube	**MUY ALTO**
A13. Directorio de usuarios (datos)	Si no funciona, nadie puede entrar	Cliente en nube	**ALTO**
A14. Interfaz de gestión del servicio en nube	Se tata de la interfaz de gestión (basada en la web, de acceso remoto, etc.) que gestiona todos los servicios que se prestan a través de la nube.	Proveedor en nube/Cliente en nube	**MUY ALTO**
A15. API de la interfaz de		Proveedor en nube/Cliente en	**MEDIO**

gestión		nube/Salud europea	
A16. Red (conexiones, etc.)	Incluye las conexiones dentro y fuera de la nube	Proveedor en nube/Cliente en nube	**ALTO**
A17. Hardware físico		Proveedor en nube/Cliente en nube	**BAJO** (dependiendo de las pérdidas) / **MEDIO** (puede ser grave en caso de robo sin protección)
A18. Edificios físicos		Proveedor en nube/Cliente en nube	**ALTO**
A19. Aplicación del proveedor en nube (código de fuente)		Proveedor en nube/Cliente en nube	**ALTO**
A20. Certificación	ISO, PCI DSS, etc.	Proveedor en nube/Cliente en nube	**ALTO**
A21. Registros operativos (proveedor en nube y cliente)	Aquellos registros utilizados para mantener y optimizar procesos comerciales y con fines de auditoría	Proveedor en nube/Cliente en nube	**MEDIO**
A22. Registros de seguridad	Útiles como pruebas de incumplimiento de la seguridad y forenses	Proveedor en nube/Cliente en nube	**MEDIO**
A23. Datos de archivo o copia de seguridad		Proveedor en nube/Cliente en nube	**MEDIO**

6. RECOMENDACIONES Y MENSAJES CLAVE

La presente sección incluye el conjunto principal de recomendaciones y mensajes clave:

- Un Marco de Aseguración de Información – una lista de comprobación estándar de preguntas que pueden utilizarse para obtener (por parte de los clientes en nube) o prestar (por parte de los proveedores en nube) aseguración
- recomendaciones legales
- Recomendaciones en materia de investigación.

MARCO DE ASEGURACIÓN DE INFORMACIÓN

INTRODUCCIÓN

Una de las recomendaciones más importantes del presente informe es un conjunto de criterios de aseguración diseñados:

1. para evaluar el riesgo de adoptar servicios en nube (comparando los riesgos de mantener una organización y una arquitectura «clásicas» con los riesgos que conlleva la migración a un entorno de computación en nube).

2. para comparar las ofertas de los distintos proveedores en nube.

3. para obtener aseguraciones de proveedores en nube seleccionados. La preparación de cuestionarios de seguridad efectivos para terceros proveedores de servicios constituye un desgaste considerable de recursos para los clientes en nube que es difícil alcanzar sin tener experiencia en arquitecturas específicas de nube.

4. para reducir la carga de la aseguración con respecto a los proveedores en nube. El requisito de la aseguración del Sistema de Información de Red (NIS) introduce un riesgo muy importante específico de las infraestructuras en nube. Muchos proveedores en nube se encuentran con que un gran número de clientes solicita auditorías de su infraestructura y sus políticas. Esto puede generar una carga extremadamente elevada para el personal de seguridad, al tiempo que incrementa el número de personas que pueden acceder a la infraestructura, lo cual aumenta considerablemente el riesgo de ataques derivados de un uso indebido de información crítica de seguridad, robo de datos críticos o sensibles, etc. Los proveedores en nube tendrán que ocuparse de esta cuestión estableciendo un marco claro para gestionar dichas solicitudes.

Esta sección de las recomendaciones propone una serie de preguntas que una organización puede plantear a un proveedor en nube para asegurarse de que está protegiendo suficientemente la información que se les ha confiado.

El objetivo de estas preguntas es proporcionar una línea de base mínima. Por tanto, cualquier organización puede tener requisitos adicionales concretos que no estén incluidos en la línea de base.

Del mismo modo, el presente documento no facilita un formato estándar de respuesta para el proveedor en nube, por lo que las respuestas pueden suministrarse en formato de texto libre. No obstante, se pretende que las preguntas se integren en un marco exhaustivo más detallado que se desarrollará como fase posterior de este trabajo; de este modo se obtendrá un conjunto de respuestas comparable y coherente. Dichas respuestas ofrecerán una métrica cuantificable con respecto a la madurez de la aseguración de información del proveedor.

Se pretende que la mencionada métrica sea coherente frente a otros proveedores que permiten la comparación para organizaciones de usuarios finales.

DIVISIÓN DE RESPONSABILIDADES

La siguiente tabla muestra la distribución de responsabilidades prevista entre cliente y proveedor.

	Cliente	**Proveedor**
Legalidad del contenido	Responsabilidad plena	Responsabilidad del intermediario con excepciones de responsabilidad en virtud de los términos de la Directiva sobre el comercio electrónico (1) y su interpretación[1].
Incidentes de seguridad (incluida la fuga de datos y la utilización de cuentas	Responsabilidad de debida diligencia para lo que es objeto de control en función de las condiciones	Responsabilidad de debida diligencia para lo que es objeto

[1] Véase la definición de servicios de la sociedad de la información que se ofrece en el artículo 2 de la Directiva 98/48/CE y en el artículo 2 de la Directiva 2000/31/CE, en conjunto con las excepciones incluidas en los artículos 12 a 15 de la Directiva 2000/31/CE (Directiva sobre el comercio electrónico).

para lanzar ataques)	contractuales	de control
Estado de la legislación europea en materia de protección de datos	Controlador de datos	Procesador de datos (externo)

DISTRIBUCIÓN DE RESPONSABILIDADES

Con respecto a los incidentes de seguridad, debe haber una definición y un entendimiento claro entre el cliente y el proveedor de funciones y responsabilidades pertinentes en materia de seguridad. Las líneas de dicha distribución varían en gran medida entre las ofertas de SaaS y las de IaaS, y ésta última delega más responsabilidad en el cliente. La siguiente tabla ilustra una distribución de responsabilidad típica y racional. *En cualquier caso, para cada tipo de servicio, el cliente y el proveedor deben definir claramente quién es responsable de todas las cuestiones que se indican en la lista que sigue..* En caso de que se apliquen condiciones estándar de servicio (que no puedan negociarse), los clientes en nube deben verificar el ámbito de sus responsabilidades.

SOFTWARE COMO SERVICIO

Cliente	Proveedor
• Cumplimiento de la ley de protección de datos con respecto a los datos de cliente recabados y procesados • Mantenimiento del sistema de gestión de identidad • Gestión del sistema de gestión de identidad • Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)	• Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.) • Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.) • Gestión de parches del sistema operativo y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor) • Configuración de la plataforma de seguridad (normas del cortafuegos, ajuste de IDS/IPS, etc.)

	• Supervisión de los sistemas • Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes) • Recogida de registros y control de la seguridad

PLATAFORMA COMO SERVICIO

Cliente	Proveedor
• Mantenimiento del sistema de gestión de identidad • Gestión del sistema de gestión de identidad • Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)	• Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.) • Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.) • Gestión de parches del sistema operativo y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor) • Configuración de la plataforma de seguridad (normas del cortafuegos, ajuste de IDS/IPS, etc.) • Supervisión de los sistemas • Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes) • Recogida de registros y control de la seguridad

INFRAESTRUCTURA COMO SERVICIO

Cliente	Proveedor
• Mantenimiento del sistema de gestión de identidad • Gestión del sistema de gestión de identidad • Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas) • Gestión de parches del sistema operativo de invitado y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor) • Configuración de la plataforma de seguridad de invitado (normas del cortafuegos, ajuste de IDS/IPS, etc.) • Supervisión de los sistemas de invitado • Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes) • Recogida de registros y control de la seguridad	• Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.) • Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.) • Sistemas de alojamiento (hipervisor, cortafuegos virtual, etc.)

Si los clientes en nube son responsables de la seguridad de sus Infraestructuras (en IaaS), deben considerar lo siguiente:

Seguridad de la Aplicación en la Infraestructura como servicio

Los proveedores de la aplicación IaaS tratan las aplicaciones de la instancia virtual del cliente como una «caja negra», y por ello se muestran totalmente agnósticos con respecto al funcionamiento y a la gestión de las aplicaciones de un cliente. La totalidad del «paquete» (la aplicación del cliente, la plataforma de aplicación para la ejecución (.Net, Java, Ruby, PHP, etc.)) se ejecuta desde el servidor de los clientes (sobre la infraestructura del proveedor), y son los propios clientes los que lo gestionan. Por este motivo, es de vital importancia señalar que los clientes deben asumir toda la responsabilidad de asegurar sus aplicaciones desplegadas en la nube. A continuación se ofrece una breve lista de comprobación y descripción de las mejores prácticas en cuanto al diseño y a la gestión de aplicaciones seguras:

- Las aplicaciones desplegadas en la nube deben estar diseñadas para el modelo de amenaza de Internet (aunque estén desplegadas como parte de una nube privada virtual (VPC, *virtual private cloud*).
- Deben diseñarse o integrarse con las contramedidas de seguridad estándar para ofrecer protección frente a las vulnerabilidades comunes de la web (véase el top ten de OWASP (40)).
- Los clientes son responsables de la actualización de sus aplicaciones —y, por tanto, deben asegurarse de que disponen de una estrategia de parche (para garantizar que sus aplicaciones son objeto de análisis para identificar programas maliciosos y piratas que intentan identificar vulnerabilidades que les permitan un acceso no autorizado a los datos de los clientes almacenados en la nube)—.
- Los clientes no deben plantearse el uso de aplicaciones personalizadas de autenticación, autorización y contabilización (AAA), ya que éstas pueden debilitarse si no se implementan de forma adecuada.

En resumen: las aplicaciones empresariales distribuidas en nube deben ejecutarse aplicándose múltiples controles para asegurar el alojamiento (y la red - véase la sección anterior), el acceso del usuario y los controles del nivel de aplicación (véase los manuales OWASP (41) relativos a la seguridad del diseño de la aplicación en línea/web). También debe tenerse en cuenta que muchos distribuidores dominantes, como Microsoft, Oracle, Sun, etc., publican documentación exhaustiva sobre el modo de asegurar la configuración de sus productos.

Metodología

Las secciones clave del presente documento se basan en las amplias clases de control incluidas en las normas ISO 27001/2 (42), (43) y BS25999 (44). Los detalles que aparecen en estas secciones se extraen

de ambas normas, así como de las mejores prácticas exigidas por el sector. Durante todo el proceso, hemos seleccionado únicamente los controles pertinentes para los proveedores en nube y los terceros subcontratistas.

El marco detallado, cuya publicación está prevista para 2010, pretende incluir normas adicionales como NIST SP 800-53 (45).

ADVERTENCIA

Las distintas preguntas detalladas en la siguiente sección representan una selección de controles habituales. No pretende ser una lista exhaustiva, y del mismo modo, también puede ocurrir que determinadas preguntas no se apliquen a implementaciones concretas. En consecuencia, esta lista debe utilizarse como línea de base para los controles habituales, y deben obtenerse detalles adicionales cuando sea necesario.

También cabe señalar que, aunque es posible transferir muchos de los riesgos a un proveedor aprovisionado externamente, es raro que se considere el verdadero coste de la transferencia del riesgo. Por ejemplo, un incidente de seguridad que ocasiona la divulgación no autorizada de datos del cliente puede generar pérdidas económicas para el proveedor; no obstante, la publicidad negativa y la pérdida de confianza del consumidor, así como las posibles sanciones reglamentarias (PCI-DSS) afectarían al cliente final. Este tipo de escenario subraya la importancia de distinguir el riesgo del riesgo comercial. Es posible transferir el riesgo comercial, pero el riesgo en última instancia siempre repercute sobre el cliente final.

Cualquier respuesta a los resultados de una evaluación de riesgo —en concreto, la cantidad y el tipo de inversión en la mitigación— debe decidirse analizando el deseo de riesgo de la organización y las oportunidades y el ahorro económico que se perderán al seguir cualquier estrategia concreta de mitigación de riesgos.

Los clientes en nube también deben llevar a cabo sus propios análisis de riesgo específicos para su contexto. En la siguiente dirección pueden encontrarse algunas metodologías de evaluación de riesgos y gestión del riesgo: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

A medida que el entorno comercial y regulador evoluciona y surgen nuevos riesgos, la evaluación de riesgos deberá convertirse en una actividad periódica en lugar de ser un evento aislado.

NOTA PARA LOS GOBIERNOS

Los siguientes controles están dirigidos principalmente a las PYME que evalúan a los proveedores en nube. También pueden resultar útiles para los gobiernos con las siguientes condiciones. *Las características de la nube utilizada deben considerarse detenidamente en conexión con el sistema de clasificación de información utilizado por cualquier organismo gubernamental.*

- El uso de nubes públicas —incluso si obtienen respuestas favorables en el siguiente cuestionario— se recomienda únicamente para las clases de datos con la aseguración más baja.

- Para clases de datos con una aseguración más alta, la lista de comprobaciones propuesta en el presente informe es válida, pero debe complementarse con comprobaciones adicionales. El presente informe no tiene por objeto abarcar dichos controles, pero a continuación se ofrecen ejemplos de cuestiones que deben incluirse:

    - ¿Ofrece el proveedor información transparente y un control total sobre la ubicación física actual de todos los datos? A menudo, la aseguración alta de los datos se ve restringida por la ubicación.
    - ¿Soporta el proveedor el sistema de clasificación de datos utilizado?
    - ¿Qué garantías ofrece el proveedor de que los recurso del cliente están totalmente aislados (es decir, no se comparten máquinas físicas)?
    - Si se asume que los clientes no comparten máquinas físicas, ¿en qué medida se suprime por completo el almacenamiento, la memoria y otros rastros de datos antes de reubicar las máquinas?
    - ¿Soporta el proveedor o incluso solicita la autenticación del símbolo físico de base 2 para el acceso del cliente?
    - ¿Posee el proveedor la certificación ISO 27001/2? ¿Cuál es el ámbito de aplicación de dicha certificación?
    - Los productos utilizados por el proveedor, ¿están sujetos a criterios comunes de certificación? ¿A qué nivel? ¿Qué perfil de protección y objetivo de seguridad se establece para el producto?

REQUISITOS DE ASEGURACIÓN DE LA INFORMACIÓN

SEGURIDAD DEL PERSONAL

La mayoría de preguntas relativas al personal serán similares a las que le plantearía a su propio personal de TI o a otro personal encargado de sus tareas de TI. Al igual que con la mayoría de evaluaciones, existe un equilibrio entre los riesgos y el coste.

- ¿Qué políticas y procedimientos aplica a la hora de contratar a sus administradores de TI o a otras personas que tienen acceso al sistema? Entre ellas deben incluirse:
    - comprobaciones antes de la contratación (identidad, nacionalidad o estado, historial de empleo y referencias, condenas penales e inhabilitación (para personal ejecutivo en cargos privilegiados)).
- ¿Existen distintas políticas en función del lugar donde se almacenan los datos o de las aplicaciones que se ejecutan?
    - Por ejemplo, las políticas de contratación de una región pueden ser distintas de las que se aplican en otra región.
    - Las prácticas deben mantener la coherencia entre regiones.
    - Puede ocurrir que se almacenen datos sensibles en una región concreta con personal adecuado.
- ¿Qué programa de educación en materia de seguridad ejecuta usted para todo el personal?
- ¿Existe un proceso de evaluación continua?
    - ¿Con qué frecuencia se aplica?
    - Entrevistas adicionales
    - Acceso de seguridad y revisión de privilegios
    - Revisión de políticas y procedimientos.

ASEGURACIÓN DE LA CADENA DE SUMINISTRO

Las siguientes preguntas se aplican a las situaciones en las que el proveedor en nube subcontrata determinadas operaciones que son clave para la seguridad de la operación para terceros (por ejemplo, un proveedor SaaS que subcontrata la plataforma subyacente a un tercero, un proveedor en nube que

subcontrata los servicios de seguridad a un proveedor de servicios de seguridad gestionada, uso de un proveedor externo para la gestión de la identidad en los sistemas operativos, etc.). También incluye a terceros que tengan acceso físico o remoto a la infraestructura del proveedor en nube. Se asume que la totalidad de este cuestionario puede aplicarse de manera recursiva a proveedores de servicios en nube (terceros o de orden n).

- Defina los servicios que están subcontratados en su cadena de suministro de entrega de servicios que sean clave para la seguridad (incluida la disponibilidad) de sus operaciones.
- Describa los procedimientos que se utilizan para asegurar a los terceros que acceden a su infraestructura (física y/o lógica).
    - ¿Realiza auditorías sobre sus subcontratistas? ¿Con qué frecuencia?
- ¿Existen disposiciones de Acuerdos de nivel de servicio garantizadas por los contratistas cuya exigencia es inferior a los Acuerdos de nivel de servicio que ofrece a sus clientes? Si no las hay, ¿aplica redundancia al proveedor?
- ¿Qué medidas se adoptan para garantizar el cumplimiento y el mantenimiento de los niveles de servicio de terceros?
- ¿Puede confirmar el proveedor en nube que se aplican controles y política de seguridad (de manera contractual) a sus terceros proveedores?

SEGURIDAD OPERATIVA

Se espera que cualquier acuerdo comercial con proveedores externos incluya niveles de servicio para todos los servicios de red. No obstante, además de los acuerdos definidos, el cliente final debe asegurarse igualmente de que el proveedor emplea los controles adecuados para subsanar la divulgación no autorizada.

- Describa en detalle su política y sus procedimientos de control de cambio. Aquí también deben incluirse el proceso que se utiliza para volver a evaluar los riesgos derivados de los cambios y aclarar si los resultados se ponen a disposición de los clientes finales.
- Defina la política de acceso remoto.
- ¿Mantiene el proveedor procedimientos documentados de operación con respecto a los sistemas de información?
- ¿Existe un entorno en fases destinado a reducir el riesgo, por ejemplo, desarrollo, prueba y entornos operativos? ¿Están separadas dichas fases?
- Defina los controles de red y de alojamiento utilizados para proteger los sistemas que albergan las aplicaciones y la información para el cliente final. Aquí deben incluirse detalles de la certificación relativa a normas externas (por ejemplo, ISO 27001/2).

- Especifique los controles utilizados para protegerse frente a códigos maliciosos.
- Las configuraciones seguras, ¿se despliegan para permitir únicamente la ejecución de códigos móviles y funcionalidades autorizados (por ejemplo, que ejecuten únicamente comandos específicos)?
- Describa las políticas y los procedimientos para realizar copias de seguridad. Aquí deben incluirse procedimientos para la gestión de los medios extraíbles y métodos para destruir de manera segura los medios que ya no son necesarios. (Dependiendo de sus necesidades empresariales, puede que el cliente quiera aplicar una estrategia independiente con respecto a las copias de seguridad. Esta opción es especialmente útil cuando se necesita un acceso de tiempo crítico a dichas copias.)

Los registros de auditoría se utilizan en caso de producirse un incidente que requiera investigación; también pueden utilizarse en la resolución de problemas. Con estos fines, el cliente final deberá tener garantías de que dicha información está disponible:

- ¿Puede indicar el proveedor la información que se introduce en los registros de auditoría?
  - ¿Durante cuánto tiempo se retienen estos datos?
  - ¿Es posible segmentar los datos de los registros de auditoría para ponerlos a disposición del cliente final y/o de las fuerzas policiales sin poner en peligro a otros clientes manteniendo la admisibilidad de los mismos en los tribunales?
  - ¿Qué controles se emplean para proteger los registros del acceso no autorizado o del vandalismo informático?
  - ¿Qué método se emplea para comprobar y proteger la integridad de los registros de auditoría?
- ¿Cómo se revisan los registros de auditoría? ¿Qué eventos registrados causan la adopción de medidas?
- ¿Qué generador de temporización se utiliza para sincronizar sistemas y ofrecer un servicio preciso de estampación de hora de registro?

ASEGURACIÓN DEL SOFTWARE

- Describa los controles utilizados para proteger la integridad del sistema operativo y las aplicaciones de software utilizadas. Incluya cualquier norma que se siga, por ejemplo, OWASP (46), SANS Checklist (47), SAFECode (48).
- ¿De qué modo valida la adecuación para los fines o la ausencia de riesgos en las nuevas versiones (*backdoors*, troyanos, etc.)? ¿Se revisan dichas versiones antes de utilizarlas?
- ¿Qué prácticas se siguen para mantener la seguridad de las aplicaciones?
- ¿Se someten a pruebas de penetración las nuevas versiones de software para garantizar la ausencia de vulnerabilidades? Si se detectan vulnerabilidades, ¿de qué modo se subsanan?

GESTION DE PARCHES

- Proporcione detalles del procedimiento de gestión de parches que se sigue.
- ¿Puede garantizar que el proceso de gestión de parches abarca todas las capas de las tecnologías de entrega de la nube —red (componentes de la infraestructura, routers y conmutadores, etc.), sistemas operativos de servidores, software de virtualización, subsistemas de seguridad y aplicaciones (cortafuegos, portales antivirus, sistemas de detección de intrusos, etc.)?

CONTROLES DE ARQUITECTURA DE RED

- Describa los controles utilizados para mitigar los ataques distribuidos de denegación de servicio (DDoS).
    - Defensa en profundidad (análisis en profundidad de paquetes, regulación del tráfico, bloqueo deliberado («*black-holing*»), etc.)
    - ¿Posee defensas contra los ataques «internos» (originados en las redes de proveedores en nube) y externos (originados en Internet o en las redes de los clientes)?
- ¿Qué niveles de aislamiento se utilizan?
    - para las máquinas virtuales, las máquinas físicas, la red, el almacenamiento (por ejemplo, redes de área de almacenamiento), redes de gestión y sistemas de soporte de gestión, etc.
- ¿Soporta la arquitectura el funcionamiento continuo desde la nube cuando la compañía se separa del proveedor en nube y viceversa (por ejemplo, si existe una dependencia crítica del sistema LDAP del cliente)?
- ¿Utilizan los proveedores en nube la infraestructura de red virtual (en PVLAN y VLAN con arquitectura de etiquetas 802.1 q (49)) garantizada para el distribuidor y/o normas específicas de mejores prácticas (por ejemplo, se impide la falsificación de IP en MAC, los ataques de envenenamiento ARP, etc. mediante una configuración específica de seguridad?

ARQUITECTURA DE ALOJAMIENTO

- ¿Garantiza el proveedor el refuerzo por defecto de las imágenes virtuales?
- ¿Se protege la imagen virtual reforzada del acceso no autorizado?
- ¿Puede confirmar el proveedor que la imagen virtualizada no contiene las credenciales de autenticación?
- ¿Se ejecuta el cortafuegos de alojamiento únicamente con los mínimos puertos necesarios para soportar los servicios de la instancia virtual?

- ¿Puede ejecutarse un sistema de prevención de intrusiones (ISP) basado en el huésped en la instancia virtual?

PAAS – SEGURIDAD DE LA APLICACIÓN

En términos generales, los proveedores de servicios PaaS son responsables de la seguridad del conjunto de software de la plataforma, y las recomendaciones incluidas en las secciones del presente documento constituyen una buena base para asegurarse de que el proveedor PaaS ha considerado determinados principios de seguridad a la hora de diseñar y gestionar su plataforma PaaS. A menudo resulta complejo obtener información detallada de los proveedores de PaaS sobre el modo exacto en que aseguran sus plataformas; no obstante, las siguientes preguntas, junto con otras secciones de este documento, proporcionar ayuda a la hora de evaluar sus ofertas.

- Solicite información sobre el modo en que las aplicaciones de multiprestación se aíslan unas de otras: se necesita una descripción muy detallada de las medidas de retención y aislamiento.
- ¿Qué garantías ofrece el proveedor de PaaS de que el acceso a sus datos está limitado los usuarios de s empresa y a las aplicaciones que posee?
- La arquitectura de plataforma debería ser la opción clásica de «caja de arena» - ¿garantiza el proveedor que la caja de arena de la plataforma PaaS se somete a controles para detectar nuevos virus y vulnerabilidades?
- Los proveedores de PaaS deben ofrecer un conjunto de características de seguridad (que puedan reutilizarse entre sus clientes). ¿Incluyen dichas características la autenticación de usuarios, el inicio de sesión único, la autorización (gestión de privilegios) y los protocolos SSL/TLS (disponibles a través de las API)?

SAAS – SEGURIDAD DE LA APLICACIÓN

El modelo SaaS dispone que sea el proveedor el que gestiona todo el paquete de aplicaciones que se entregan a los usuarios finales. Por tanto, los proveedores de SaaS son los principales responsables de la seguridad de estas aplicaciones. Los clientes suelen ser responsables de los procesos de seguridad operativos (gestión de usuarios y de accesos). No obstante, las siguientes preguntas, junto con otras secciones de este documento, ofrecen ayuda para evaluar las ofertas de dichos proveedores:

- ¿Qué controles administrativos se proporcionan? ¿Pueden utilizarse para asignar privilegios de lectura y escritura a otros usuarios?
- ¿Es el control de acceso del SaaS de grano fino? ¿Puede personalizarse de acuerdo con la política de sus organizaciones?

Suministro de recursos

- En caso de producirse una sobrecarga de recursos (procesamiento, memoria, almacenamiento, red)…
    - ¿Qué información se proporciona sobre la prioridad relativa asignada a su petición en caso de producirse un fallo en el suministro?
    - ¿Hay un plazo establecido con respeto a los niveles de servicio y a los cambios en los requisitos?
- ¿Qué grado de escalada puede alcanzar? ¿Ofrece el proveedor garantías sobre el máximo número de recursos disponibles durante un período mínimo?
- ¿Qué velocidad de escalada puede alcanzar? ¿Ofrece el proveedor garantías sobre la disponibilidad de recursos complementarios durante un período mínimo?
- ¿Qué procesos se aplican para gestionar las tendencias a gran escala en la utilización de recursos(por ejemplo, los efectos de las distintas temporadas)?

Gestión de accesos e identidad

Los siguientes controles se aplican a los sistemas de gestión de los accesos y la identidad del proveedor en nube (los que se encuentran bajo su control):

Autorización

- ¿Tienen las cuentas asociados privilegios para todo el sistema con respecto a la totalidad del sistema de nube? Si es así, ¿para qué operaciones (lectura/escritura/eliminación)?
- ¿Cómo se autentican y se gestionan las cuentas con el máximo grado de privilegio?
- ¿Cómo se autorizan (de manera unilateral o bilateral, y qué cargos de la organización lo hacen) las decisiones más críticas (por ejemplo, el desaprovisionamiento simultáneo de grandes bloques de recursos)?
- ¿Se asignan funciones de alto privilegio a la misma persona? ¿Rompe esta asignación la separación de funciones o las normas de privilegios mínimos?
- ¿Utiliza un control de acceso basado en funciones (RBAC)? ¿Se sigue el principio del privilegio mínimo?
- ¿Qué cambios, si los hay, se aplican a los privilegios y funciones del administrador para permitir un acceso extraordinario en caso de emergencia?
- ¿Existe una función de «administrador» para el cliente? Por ejemplo, ¿tiene el administrador cliente la función de añadir nuevos usuarios (que no le permita cambiar el almacenamiento subyacente)?

SUMINISTRO DE IDENTIDADES

- ¿Qué controles se realizan sobre la identidad de las cuentas de usuario durante el registro? ¿Se sigue alguna norma? Por ejemplo, el Marco de interoperabilidad de «*e-Government*».
- ¿Existen distintos niveles de comprobación de identidad basados en los recursos necesarios?
- ¿Qué procesos se aplican con respecto a las credenciales de desaprovisionamiento?
- ¿Se proporcionan y se retiran las credenciales de manera simultánea en todo el sistema en nube o existen riesgos en su desaprovisionamiento en las múltiples ubicaciones geográficas distribuidas?

GESTIÓN DE DATOS PERSONALES

- ¿Qué controles para proteger y almacenar datos se aplican al directorio de usuarios (por ejemplo, AD, LDAP) y al acceso al mismo?
- ¿Pueden exportarse los datos del directorio de usuarios en formato interoperable?
- ¿Es el *«need-to-know»* la base para acceder a los datos de los clientes en el entorno del proveedor en nube?

GESTIÓN DE CLAVES

Por lo que respecta a las claves que se encuentran bajo el control del proveedor en nube:

- ¿Se aplican controles de seguridad para leer y escribir dichas claves? Por ejemplo, políticas de contraseñas seguras, almacenamiento de claves en un sistema independiente, módulos de seguridad hardware (HSM) para claves del certificado raíz, autenticación mediante tarjeta inteligente, acceso blindado directo al almacenamiento, duración reducida de las claves, etc.
- ¿Se aplican controles de seguridad para utilizar dichas claves para firmar y codificar datos?
- ¿Existen procedimientos aplicables en caso de claves comprometidas? Por ejemplo, listas de revocación de claves.
- ¿Tiene la revocación de claves capacidad para ocuparse de cuestiones simultáneas en múltiples sitios?
- Las imágenes del sistema del cliente ¿están protegidas o codificadas?

CODIFICACIÓN

- La codificación puede utilizarse en múltiples situaciones. ¿Dónde se utiliza?
    - Datos en tránsito
    - Datos estáticos
    - ¿Datos en el procesador o en la memoria?
- ¿Nombres de usuario y contraseñas?
- ¿Existe una política bien definida para lo que debe o no debe codificarse?
- ¿Quién posee las claves de acceso?

- ¿Cómo se protegen las claves?

AUTENTICACIÓN

- ¿Qué formas de autenticación se utilizan para las operaciones que requieren una aseguración elevada? Pueden ser los inicios de gestión para las interfaces de gestión, la creación de claves, el acceso a cuentas de varios usuarios, la configuración del cortafuegos, el acceso remoto, etc.
- ¿Se utiliza la autenticación de dos factores para gestionar componentes críticos de la infraestructura, como cortafuegos, etc.?

ROBO O PELIGRO DE LAS CREDENCIALES

- ¿Ofrece un servicio de detección de anomalías (capacidad para identificar tráfico de IP y comportamiento de usuarios o equipos de soporte inusual y potencialmente malicioso)? Por ejemplo, análisis de intentos fallidos o satisfactorios de inicio de sesión, horarios inusuales, inicios de sesión múltiples, etc.
- ¿Qué disposiciones existen en caso de robo de las credenciales de un cliente (detección, revocación, evidencia de acciones)?

SISTEMAS DE GESTIÓN DE LOS ACCESOS Y LA IDENTIDAD QUE SE OFRECEN AL CLIENTE EN NUBE

Las siguientes preguntas se aplican a los sistemas de gestión de los accesos y la identidad que el proveedor en nube ofrece al cliente en nube para su uso y control:

MARCOS DE GESTIÓN DE LA IDENTIDAD

- ¿Permite el sistema la integración de una infraestructura federada de IdM que sea interoperable para una aseguración elevada (sistemas OTP, si resultan necesarios) y una aseguración reducida (por ejemplo, usuario y contraseña)?
- ¿Puede interoperar el proveedor en nube con terceros proveedores de identidad?
- ¿Hay capacidad para incorporar un inicio de sesión único?

CONTROL DEL ACCESO

- ¿Permite el sistema de credenciales del cliente la separación de funciones y responsabilidades y múltiples dominios (o una clave única para responsabilidades, funciones y dominios múltiples?
- ¿Cómo gestiona el acceso a las imágenes del sistema del cliente? ¿Cómo garantiza que las claves criptográficas y de autenticación no están incluidas en dichas imágenes?

AUTENTICACIÓN

- ¿Cómo se identifica el propio proveedor en nube ante el cliente (existencia de una autenticación mutua)…
    - cuando el cliente envía comandos de API?
    - cuando el cliente entra en la interfaz de gestión?
- ¿Apoya un mecanismo federado de autenticación?

GESTIÓN DE ACTIVOS

Es importante garantizar que el proveedor mantiene una lista actualizada de activos de hardware y software (aplicaciones) que se encuentra bajo el control de los proveedores en nube. De este modo se puede comprobar que todos los sistemas utilizan los controles apropiados y que los sistemas no pueden utilizarse como puerta trasera de entrada a la infraestructura.

- ¿Posee el proveedor un sistema automático para hacer el inventario de todos los activos que facilite una gestión apropiada de los mismos?
- ¿Existe una lista de activos que el cliente haya utilizado durante un período de tiempo concreto?

Las siguientes preguntas se utilizarán cuando el cliente final despliegue datos que requieran protección adicional (es decir, que se consideren sensibles).

- ¿Se clasifican los activos por su grado de sensibilidad y criticidad?
    - En caso afirmativo, ¿utiliza el proveedor una separación apropiada entre sistemas, que incluya distintas clasificaciones, y para un cliente único cuyos sistemas pertenezcan a distintas clasificaciones de seguridad?

DATOS Y PORTABILIDAD DE SERVICIOS

Este bloque de preguntas debe considerarse para poder entender los riesgos asociados a la vinculación del distribuidor.

- ¿Existen procedimientos documentados y API para exportar datos desde la nube?
- ¿Ofrece el distribuidor formatos de exportación interoperables para todos los datos almacenados en la nube?
- En el caso del SaaS, ¿están normalizadas las interfaces API utilizadas?
- ¿Existen disposiciones para la exportación de aplicaciones creadas por el usuario en formato estándar?

- ¿Existen procesos para demostrar que los datos pueden exportarse a otro proveedor en nube —en caso de que el cliente desee cambiar de proveedor, por ejemplo—?
- ¿Puede realizar el cliente su propia extracción de datos para verificar que el formato es universal y puede migrar a otro proveedor en nube?

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La continuidad es un aspecto importante para las organizaciones. Aunque es posible establecer acuerdos de nivel de servicio en los que se estipule la disponibilidad mínima de los sistemas en el tiempo, sigue habiendo varias consideraciones adicionales.

- ¿Mantiene el proveedor un método documentado que describa la repercusión de una interrupción?
    - ¿Cuáles son el Objetivo de Punto de recuperación (RPO) y el Objetivo de Tiempo de recuperación (RTO) para los servicios? Descríbalos en detalle en función de la criticalidad del servicio.
    - ¿Se tratan las actividades de seguridad de la información de manera adecuada en el proceso de restauración?
    - ¿Cuáles son las líneas de comunicación con los clientes finales en caso de interrupción?
    - ¿Están claramente identificadas las responsabilidades y funciones a la hora de solucionar una interrupción?
- ¿Ha clasificado el proveedor las prioridades de la recuperación? ¿Cuál sería nuestra prioridad relativa (la del cliente final) en la restauración? Nota: la respuesta puede ser una categoría (ALTA/MEDIA/BAJA).
- ¿Qué dependencias pertinentes para el proceso de restauración hay? Incluya los proveedores y los socios de subcontratación.
- En caso de que el sitio primario no esté disponible, ¿cuál es la separación mínima para la ubicación del sitio secundario?

GESTIÓN Y RESPUESTA A INCIDENTES

La gestión y respuesta a incidentes forma parte de la gestión de la continuidad del negocio. El objetivo de este proceso es contener el impacto de los eventos inesperados que pueden provocar interrupciones y mantener así un nivel aceptable para la organización.

Para evaluar la capacidad de una organización para minimizar la probabilidad de que se produzca un impacto negativo de un incidente de seguridad de la información o para reducir el mismo, deben plantearse las siguientes preguntas al proveedor en nube:

- ¿Aplica el proveedor un proceso formal para detectar, identificar, analizar y responder a los incidentes?
- ¿Se ha ensayado este proceso para comprobar la eficacia de los procesos de gestión? ¿Garantiza asimismo el proveedor durante el ensayo que todo el personal de la organización de soporte del proveedor en nube conoce los procesos y sus funciones durante la gestión de incidentes (tanto durante el incidente como después del análisis)?
- ¿Cómo se estructuran las capacidades de detección?
    - ¿Cómo puede el cliente en nube notificar al proveedor las anomalías y los eventos relativos a la seguridad?
    - ¿Qué facilidades ofrece el proveedor para que los servicios de gestión de servicios en tiempo real (RTSM) de terceros seleccionados por los clientes intervengan en sus sistemas (si procede) o coordinen las capacidades de respuesta a incidentes en colaboración con el proveedor en nube?
    - ¿Existe un servicio de supervisión de la seguridad en tiempo real (RTSM) en marcha? ¿Se subcontrata el servicio? ¿Qué tipo de parámetros y servicios se supervisan?
    - ¿Suministra (bajo petición) un informe periódico que incluya los incidentes de seguridad (por ejemplo, en función de la definición de ITIL?
    - ¿Durante cuánto tiempo se retienen los registros de seguridad? ¿Están los registros almacenados en un lugar seguro? ¿Quién tiene acceso a los registros?
    - ¿Puede crear el cliente un sistema HIPS/HIDS en la imagen de la máquina virtual? ¿Es posible integrar la información recabada por los sistemas de prevención y detección de intrusiones del cliente en el sistema RTSM del proveedor en nube o de un tercero?
- ¿Cómo se definen los niveles de gravedad?
- ¿Cómo se definen los procedimientos de escalada? ¿Cuándo participa el cliente en nube (si lo hace)?
- ¿Cómo se documentan los incidentes y cómo se recogen las pruebas?
- Al margen de la autenticación, la contabilidad y las auditorías, ¿qué controles adicionales se aplican para impedir (o minimizar el impacto) las actividades maliciosas de los iniciados?
- ¿Ofrece el proveedor al cliente (bajo petición) una imagen constatada de la máquina virtual?

- ¿Recoge el proveedor indicadores y métricas de los incidentes (número de incidentes detectados o notificados al mes, número de incidentes causados por los subcontratistas del proveedor en nube y número total de dichos incidentes, tiempo medio de respuesta y resolución, etc.)?
    - ¿Cuáles de ellos pone el proveedor a disposición del público (NB: no todos los datos relativos a la notificación de incidentes pueden hacerse públicos, puesto que pueden comprometer la confidencialidad y revelar información crítica en materia de seguridad)?
- ¿Con qué frecuencia somete a pruebas el proveedor los planes de continuidad del negocio y de recuperación de desastres?
- ¿Recoge el proveedor datos sobre el grado de satisfacción con respecto a los Acuerdos de nivel de servicio?
- ¿Realiza el proveedor pruebas de asistencia técnica? Por ejemplo:
    - Pruebas de suplantación (la persona al otro lado del teléfono que pide que se restablezca una contraseña, ¿es realmente quien dice ser?) o los denominados ataques de «ingeniería social».
- ¿Realiza el proveedor pruebas de penetración? ¿Con qué frecuencia? ¿Qué elementos se someten a pruebas durante la prueba de penetración, por ejemplo, se prueba el aislamiento de seguridad de cada imagen para garantizar que no pueda saltar contenido de una imagen a otra al tiempo que se obtiene acceso a la infraestructura de alojamiento? Las pruebas también deben comprobar la posibilidad de acceder, a través de la imagen virtual, a los sistemas de soporte y gestión de los proveedores en nube (por ejemplo, los sistemas de control del acceso administrativo y de aprovisionamiento).
- ¿Realiza el proveedor pruebas de vulnerabilidad? ¿Con qué frecuencia?
- ¿Qué proceso se sigue para rectificar las vulnerabilidades (reparaciones en caliente, reconfiguración, actualización a versiones posteriores de software)?

SEGURIDAD FÍSICA

Al igual que con la seguridad del personal, muchas de las cuestiones potenciales se derivan del hecho de que la infraestructura de TI se encuentra bajo el control de un tercero - como la subcontratación tradicional, el efecto que puede tener un incumplimiento de la seguridad física sobre múltiples clientes (organizaciones).

- ¿Qué garantías puede ofrecer al cliente con respecto a la seguridad física de las instalaciones? Ofrezca ejemplos, incluida cualquier norma que se cumpla, por ejemplo, la sección 9 de la norma ISO 27001/2.
    - ¿Quién posee acceso (físico) sin escolta, además del personal de TI autorizado, a la infraestructura de TI?
        - Por ejemplo, limpiadoras, directores, personal de «seguridad física», contratistas, asesores, distribuidores, etc.
    - ¿Con qué frecuencia se revisan los derechos de acceso?
        - ¿Qué período de tiempo es necesario para revocar dichos derechos?
    - ¿Evalúa los riesgos para la seguridad y los perímetros de forma periódica?
        - ¿Con qué frecuencia?
    - ¿Realiza evaluaciones periódicas de los riesgos que incluyan elementos como los edificios adyacentes?
    - ¿Controla o supervisa al personal (incluidos los terceros) que accede a las zonas seguras?
    - ¿Qué políticas o procedimientos aplica a la hora de cargar, descargar e instalar equipos?
    - ¿Se inspeccionan las entregas para identificar riesgos antes de la instalación?
    - ¿Existe un inventario físico actualizado de los elementos que se encuentran en el centro de datos?
    - ¿Los cables de red se extienden por zonas de acceso público?
        - ¿Utiliza cables o conductos blindados?
    - ¿Supervisa frecuentemente las instalaciones para identificar posibles equipos no autorizados?
    - ¿Hay algún equipo que no esté ubicado en el centro de datos?
        - ¿Cómo se protege?
    - ¿Utiliza su personal equipos portátiles (por ejemplo, ordenadores portátiles, teléfonos inteligentes) que pueden acceder al centro de datos?
        - ¿Cómo se protegen dichos equipos?
    - ¿Qué medidas se aplican para controlar las tarjetas de acceso?
    - ¿Qué procesos o procedimientos se aplican para destruir los sistemas o medios obsoletos en caso de ser necesario?
        - ¿se sobrescriben los datos?
        - ¿se destruyen físicamente?
    - ¿Qué procesos de autorización se aplican para el desplazamiento de equipos de un emplazamiento a otro?

        - ¿Cómo se identifica al personal (o a los contratistas) autorizados para llevar a cabo esta tarea?
    - ¿Con que frecuencia se realizan auditorías sobre los equipos para supervisar la posible retirada de equipos no autorizados?
    - ¿Con qué frecuencia se realizan comprobaciones para garantizar que el entorno cumple los requisitos legales y reglamentarios apropiados?

CONTROLES MEDIOAMBIENTALES

- ¿Qué procedimientos o políticas se aplican para garantizar que las cuestiones medioambientales no ocasionan la interrupción del servicio?
- ¿Qué métodos utiliza para impedir los daños derivados de incendios, inundaciones, terremotos, etc.?
    - En caso de producirse una catástrofe, ¿qué medidas adicionales de seguridad se aplican para proteger el acceso físico?
    - ¿Se aplican en los sitios primarios y secundarios?
- ¿Se controla la temperatura y la humedad en el centro de datos?
    - ¿Se supervisa el aire acondicionado?
- ¿Protege sus edificios de los impactos de rayos?
    - ¿Dicha protección incluye las líneas eléctricas y de comunicación?
- ¿Posee generadores autónomos para casos de fallos en el suministro eléctrico?
    - ¿Qué tiempo máximo de funcionamiento poseen?
    - ¿Existe un suministro de combustible suficiente?
    - ¿Existen generadores en caso de fallos?
    - ¿Con qué frecuencia realiza comprobaciones sobre el equipo de alimentación ininterrumpida (UPS)?
    - ¿Con qué frecuencia realiza comprobaciones sobre sus generadores?
    - ¿Posee múltiples proveedores de electricidad?
- ¿Todos los servicios públicos (electricidad, agua, etc.) tienen capacidad para soportar su entorno?

¿Con qué frecuencia se evalúa y se comprueba dicha capacidad?

- ¿Tiene su sistema de aire acondicionado capacidad para soportar su entorno?
    - ¿Con qué frecuencia se somete a pruebas?
- ¿Respeta los plazos de mantenimiento recomendados por los fabricantes?
- ¿Permite únicamente que el personal autorizado realice tareas de mantenimiento o reparaciones en las instalaciones?

  - ¿Cómo comprueba su identidad?
- Cuando el equipo se envía a reparar, ¿se eliminan los datos del mismo en primer lugar?
  - ¿Cómo se lleva a cabo dicha eliminación?

REQUISITOS LEGALES

Los clientes reales y potenciales de los servicios del proveedor en nube deben considerar sus obligaciones respectivas a escala nacional y supranacional con respecto al cumplimiento de los marcos reglamentarios, y garantizar que dichas obligaciones se cumplen de manera adecuada.

Las preguntas legales clave que el cliente debe plantear al proveedor en nube son las siguientes:

- ¿En qué país está ubicado el proveedor en nube?
- ¿Está ubicada la infraestructura del proveedor en nube en el mismo país o en países distintos?
- ¿Utilizará el proveedor en nube otras compañías cuya infraestructura esté ubicada fuera de la del proveedor en nube?
- ¿Dónde estarán ubicados físicamente los datos?
- ¿Se dividirá la jurisdicción de los términos contractuales y de los datos?
- ¿Se subcontratará alguno de los servicios del proveedor en nube?
- ¿Se contratará externamente alguno de los servicios del proveedor en nube?
- ¿Cómo se recogerán, procesarán y transferirán los datos proporcionados por el cliente y los clientes del cliente?
- ¿Qué ocurre con los datos que se envían al proveedor en nube a la finalización del contrato?

RECOMENDACIONES LEGALES

Actualmente, la mayoría de las cuestiones legales asociadas a la computación en nube se resuelven cuando el cliente evalúa los contratos, los TdU, los Acuerdos de licencia de usuario y los Acuerdos de nivel de servicio. Es importante diferenciar el caso de una organización pequeña a mediana, que elegiría entre los distintos contratos que se ofrecen en el mercado, y una organización de mayor tamaño, que podría negociar las cláusulas. En el análisis legal de presente documento, adoptamos la perspectiva de la organización pequeña-a-mediana que puede acceder a distintos contratos, Acuerdos de nivel de servicio, etc., que se ofrecen en el mercado, puesto que se trata del caso más común. Esto se debe a que el modelo de negocios de la computación en nube difiere de la subcontratación: a fin de hacer llegar parte de los beneficios a sus clientes, la computación en nube confía en las economías de escala por proporcionar un servicio básico de bajo coste, en comparación con un servicio hecho a medida de las necesidades del cliente. Sin embargo, las organizaciones de mayor tamaño pueden realizar las mismas consideraciones a la hora de negociar los contratos. Al tiempo que las experiencias pasadas con tecnologías similares de Internet ofrecen directrices que permiten a los clientes y a los

proveedores en nube evaluar los riesgos para la seguridad que se derivan de la computación en nube, es necesario que ambas partes consideren la naturaleza única de la computación en nube a la hora de evaluar estos riesgos.

Aunque hay muchos ámbitos de coincidencia, se recomienda revisar detenidamente determinadas cláusulas estándar del contrato, debido a la naturaleza de la computación en nube. Debe prestarse especial atención a los derechos y obligaciones en lo que respecta a las notificaciones de incumplimiento de los requisitos de seguridad, transferencias de datos, creación de obras derivadas, cambio de control y acceso a los datos por parte de las fuerzas policiales. Debido a que la nube puede utilizarse para subcontratar infraestructura interna crítica, y la interrupción de dicha infraestructura puede provocar consecuencias de gran alcance, debe comprobarse si las limitaciones estándar de la responsabilidad se ajustan a las asignaciones de responsabilidad, habida cuenta del uso de las partes de la nube, o de la asignación de responsabilidades en cuanto a la infraestructura [véase Distribución de responsabilidades].

Hasta que los precedentes legales aclaren las preocupaciones en materia de seguridad de datos específicas de la computación en nube, los clientes y los proveedores en nube deben asegurarse de que las condiciones de su contrato abordan de manera efectiva los riesgos de seguridad.

A continuación se ofrece una lista de ámbitos a los que el cliente debe prestar una atención especial a la hora de evaluar los Acuerdos de nivel de servicio, los TdU, los Acuerdos de licencia de usuario y otros acuerdos relativos a los servicios en nube:

- **Protección de los datos**: debe prestarse atención al seleccionar un procesador que proporcione medidas técnicas de seguridad adecuadas y medidas organizativas que dirijan el procesamiento que tendrá lugar y al garantizar el cumplimiento de dichas medidas.
- **Seguridad de los datos**: debe prestarse atención a las medidas obligatorias relativas a la seguridad de los dato que pueden provocar que o bien el proveedor en nube o bien el cliente se sometan a medidas reguladoras y judiciales si el contrato no aborda dichas obligaciones.
- **Transferencia de datos**: debe prestarse atención a la información que se facilita al cliente con respecto al modo de transferir los datos en la nube propietaria del proveedor en nube, fuera de dicha nube y dentro y fuera del Espacio Económico Europeo.
- **Acceso de las autoridades policiales**: cada país tiene restricciones peculiares y requisitos necesarios para el acceso de las autoridades policiales a los datos. El cliente debe considerar la información que el proveedor pone a su disposición sobre

las jurisdicciones en las que los datos pueden almacenarse procesarse, y evaluar cualquier riesgo derivado de las jurisdicciones aplicables.

- **Confidencialidad y no divulgación**: deben revisarse las funciones y obligaciones asociadas a esta cuestión.
- **Propiedad intelectual**: en el caso de IaaS y PaaS, puede almacenarse la propiedad intelectual, incluidas las obras originales creadas utilizando la infraestructura de nube. El cliente en nube debe asegurarse de que el contrato respeta sus derechos sobre cualquier propiedad intelectual o trabajo original en la medida de lo posible, sin comprometer la calidad del servicio ofrecido (por ejemplo, las copias de seguridad podrían ser un elemento necesario a incluir en una oferta de nivel de servicio satisfactorio).
- **Asignación de riesgos y limitación de la responsabilidad**: a la hora de revisar sus respectivas obligaciones contractuales, las partes deben subrayar las obligaciones que plantean riesgos considerables para las mismas, incluyendo cláusulas de compensación económica u obligaciones de indemnización para la parte que incumpla una obligación contractual. Asimismo, debe evaluarse detenidamente cualquier cláusula estándar que abarque limitaciones de responsabilidad.
- **Cambio de control**: la transparencia relativa a la capacidad continua del proveedor en nube de cumplir sus obligaciones contractuales en caso de producirse un cambio de control, así como cualquier posibilidad de rescindir el contrato.

Las recomendaciones legales expresadas se exponen, por lo general, desde la perspectiva del cliente en nube.

RECOMENDACIONES LEGALES PARA LA COMISIÓN EUROPEA

Recomendamos que la Comisión Europea estudie o aclare lo siguiente:

- Determinadas cuestiones relativas a la Directiva sobre protección de datos personales y a las recomendaciones del grupo de protección de datos del artículo 29 que requieren aclaración. En particular:
- Bajo qué circunstancias puede considerarse al Proveedor en nube como Controlador conjunto;
- La aplicación del apartado 2 del artículo 25 de la Directiva sobre protección de datos al procesamiento de datos en países no pertenecientes al Espacio Económico Europeo durante la transferencia de los datos de un proveedor en nube a otro o en el

seno de la nube de la compañía. [2]

- La repercusión de las transferencias de datos desde y hacia países no pertenecientes al Espacio Económico Europeo, si dichos países no garantizan un nivel de protección adecuado para los datos.
- Si debe volver a analizarse el concepto de «transferencia de datos» a la luz de los avances tecnológicos ocurridos desde la redacción de la Directiva, especialmente en vista del enfoque legal basado en la rendición de cuentas (por ejemplo, según la propuesta incluida en el proyecto Galway (51)).
- Si los proveedores en nube deben estar obligados a notificar a sus clientes los incumplimientos relativos a la seguridad de los datos, y qué información deben transmitir dichos clientes a los clientes finales. Esto también puede ejecutarse mediante cláusulas contractuales, por lo que debe investigarse el medio más eficaz para llevarlo a cabo. Por ejemplo, la legislación sobre la notificación de los incumplimientos podría entrañar dificultades para su cumplimiento, e incluso podría actuar como desincentivo para la transparencia.
- Si es necesario que los Estados miembros aclaren el modo en que las exenciones de responsabilidad de los intermediarios (artículos 12 a 15) de la Directiva sobre comercio electrónico se aplican a los Proveedores en nube.
- Las diferencias entre los Estados miembros con respecto a las leyes que rigen las solicitudes de cumplimiento por parte de varias autoridades públicas en relación con los datos almacenados en la nube, en particular con vistas a evaluar las diferencias del grado de protección frente a las peticiones del gobierno de datos personales almacenados en las instalaciones (domésticas o comerciales) y los datos personales almacenados en la nube.

El mejor modo de apoyar las normas mínimas de protección de datos y los sistemas de certificación de privacidad basados en conceptos de rendición de cuentas comunes en todo el globo o al menos en todos los Estados miembros.

Pueden consultarse más detalles sobre las cinco cuestiones legales en el ANEXO I.

[2] *La Directiva sobre la privacidad electrónica, revisada en 2009 (http://register.consilium.europa.eu/pdf/es/09/st03/st03674.es09.pdf), exige que los Estados miembros introduzcan un sistema de notificación de incumplimiento de los requisitos de seguridad. Obsérvese que dicho sistema deberá aplicarse a las redes y servicios de comunicaciones electrónica, no a los servicios de la sociedad de la información como los servicios de computación en nube.*

RECOMENDACIONES EN MATERIA DE INVESTIGACIÓN

Recomendamos los siguientes ámbitos prioritarios de investigación a fin de mejorar la seguridad de las tecnologías de computación en nube:

CREACIÓN DE UN CLIMA DE CONFIANZA EN LA NUBE

- Procesos de certificación y normas para las nubes: de manera más general, normas relativas al ciclo de vida de seguridad de la computación en nube que pueden certificarse basándose en disposiciones específicas de nube para las normas de gobernanza - COBIT (52), ITIL (53), etc.;
- Métricas de seguridad en la computación en nube:
- Retorno sobre las inversiones de seguridad (ROSI): las medidas que la computación en nube puede activar para mejorar la precisión del retorno sobre la inversión de seguridad;
- Efectos de las distintas formas de notificación de los incumplimientos relativos a la seguridad;
- Técnicas para aumentar la transparencia a la vez que se mantienen niveles de seguridad apropiados:
  - Etiquetado, por ejemplo, etiquetado de ubicación, de tipos de datos, de política…
  - Privacidad a la hora de conservar los sistemas de procedencia de datos, por ejemplo, rastrear los datos de un extremo a otro a través de los sistemas;
- Confidencialidad integral de los datos en la nube y más allá:
  - Búsqueda codificada (a largo plazo)
  - Sistemas de procesamiento codificados (a largo plazo)
  - Herramientas de confidencialidad y codificación para las aplicaciones sociales en nube
  - Computación en nube de confianza, por ejemplo, secuencias de inicialización confiadas para paquetes de máquinas virtuales;
- Nubes con mayor aseguración, nubes privadas virtuales, etc.;
- Ampliación de la confianza basada en la nube a las aplicaciones y datos basados en el cliente.

PROTECCIÓN DE DATOS EN LOS GRANDES SISTEMAS INTERORGANIZACIONES

Los siguientes ámbitos requieren una investigación adicional con respecto a la computación en nube:

- Destrucción de datos y gestión del ciclo de vida
- Verificación de la integridad de las copias de seguridad y de los archivos almacenados en la nube y su gestión de las versiones
- Mecanismos de recogida de evidencias y expertos
- Gestión de incidentes – seguimiento y localización
- Resolución de conflictos y reglas de prueba

- Diferencias internacionales en la normativa aplicable, incluida la privacidad y la protección de datos
    - Medios legales para favorecer el funcionamiento correcto de las infraestructuras multinacionales de nube
    - Medios automatizados para mitigar los problemas con las distintas jurisdicciones.

INGENIERÍA DE SISTEMAS DE COMPUTACIÓN A GRAN ESCALA

- Seguridad en profundidad en el seno de los sistemas informáticos distribuidos a gran escala;
- Servicios de seguridad en la nube – des-perimetrización de las tecnologías de seguridad y adaptación de tecnologías de control del perímetro de seguridad tradicionales a la nube, por ejemplo, HSM, filtros web, cortafuegos, IDS, etc.;
- Mecanismos de aislamiento de recursos: datos, procesamiento, memoria, registros, etc.;
- Interoperabilidad entre proveedores en nube;
- Portabilidad de VM, datos y configuración de seguridad de VM de un proveedor en nube a otro (para evitar la vinculación a un distribuidor) y mantenimiento del estado y la sesión en las copias de seguridad de VM y en la migración activa a larga distancia de las máquinas virtuales;
- Normalización de interfaces para introducir datos, aplicaciones y sistemas íntegros en la nube, para que cualquier SO pueda desarrollar la correspondiente interfaz de cliente;
- Aprovisionamiento de recursos (ancho de banda y CPU, etc.) y asignación a escala (elasticidad);
- Gestión de seguridad escalable (procedimientos operativos y políticos) en el seno de las plataformas de nube:
    - cumplimiento automático de las políticas de seguridad y protección de datos
    - procesos operativos seguros de proveedores – la aplicación de los procesos de gobernanza;
- Resistencia a los fallos de la computación en nube: cómo mejorar la resistencia a los fallos de una nube:
    - uso de arquitecturas de nube en el ámbito del cliente (redes de proximidad, P2P, etc.)
        - adición de redes de clientes múltiples
        - copias de seguridad y redundancia de cliente;
    - explosión en nube y resistencia a los fallos a escala global en las nubes.

Otra fuente útil de información para obtener recomendaciones en materia de investigación será el informe PROCENT (Prioridades de Investigación sobre Tecnologías de Red Actuales y Emergentes), cuya publicación está prevista para diciembre de 2009. Puede consultarse el siguiente enlace: http://www.enisa.europa.eu/act/res/technologies/procent.

GLOSARIO Y ABREVIATURAS

AAA	Autenticación, autorización y contabilización
AC	Autoridad de certificación
Activo	El objetivo de la protección en un análisis de seguridad
API	Interfaz de programación de aplicaciones – especificación de la interfaz publicada por el proveedor de software
ARP	Protocolo de resolución de direcciones (2)
Ataque por vía alternativa	Cualquier ataque basado en información obtenida de la implementación física de un sistema, por ejemplo, información temporal, consumo de potencia, fugas electromagnéticas o incluso el sonido puede proporcionar una fuente de información adicional que puede utilizarse para romper el sistema.
BS	Norma británica (British Standard)
CC	Criterios comunes
CdS	Calidad de servicio
Confidencialidad	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ISO 17799)
Controlador de datos	La persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que, de manera individual o conjunta, determina los fines y medios del procesamiento de los datos personales; cuando los fines y medios del procesamiento están determinados por la ley o la normativa nacional o comunitaria, el controlador

	o los criterios específicos para su designación pueden estar determinados por la legislación nacional o comunitaria.
Co-residencia	Recursos de hardware o software compartidos por clientes en nube
CRL	Lista de revocación de certificados
CRM	Gestión de la relación con el cliente
DA	Directorio activo
DDoS	Distribución de denegación de servicio
Depósito (Escrow)	Almacenamiento de un recurso por un tercero que puede acceder a dicho recurso cuando se cumplen determinadas condiciones bien definidas
Desaprovisionamiento	Proceso de obligar a retirar un recurso de su uso o prohibir que un conjunto de usuarios haga uso del mismo
Disponibilidad	El porcentaje de tiempo durante el que un sistema puede funcionar
EDoS	Denegación económica de servicio
Escaneado de puertos	Sondeo de un alojamiento en red para determinar los puertos que están abiertos y los servicios que ofrecen
FIM	Gestión de identidad federada
Hipervisor	Software informático o de virtualización de plataforma de hardware que permite la ejecución de múltiples sistemas operativos en un ordenador central de manera simultánea
HSM	Módulo de seguridad hardware

Https	Conexión Http que utiliza TLS o SSL
IDS	Sistema de detección de intrusos
Integridad	Propiedad de los datos que no han sido alterados accidental o maliciosamente durante el almacenamiento o la transmisión
IP	Protocolo de Internet
IPS	Sistema de protección contra intrusos
ISO	Organización Internacional de Normalización
LDAP	Protocolo ligero de acceso a directorios
MAC	Control de acceso al medio (dirección de un nodo de red en un protocolo de IP)
MITM	Ataques con intermediarios
Motor de servicio	Sistema responsable de la entrega de servicios en nube
MSS	Servicios de seguridad gestionada
NIS	Seguridad de las redes y de la información
NIST	National Institute of Standards and Technology (EE.UU.)
No repudio	La propiedad por la que una parte del conflicto no puede repudiar o refutar la validez de una declaración o contrato
Objetivo de seguridad	Documento que especifica los criterios de evaluación de la seguridad para sustanciar las reclamaciones de los distribuidores relativas a las propiedades de seguridad de un producto (término utilizado en Criterios comunes)

OCSP	Protocolo de estado de certificados en línea
Orden judicial	En este contexto, la autoridad legal que confisca las pruebas
OTP	Contraseña de un solo uso (tipo de símbolo de autenticación)
OVF	Formato abierto de virtualización
Perfil de protección	Documento que especifica los criterios de evaluación de la seguridad para sustanciar las reclamaciones de los distribuidores de una familia de productos de sistemas de información concreta (término utilizado en Criterios comunes)
Perimetrización	Control del acceso a un activo o grupo de activos
PN	Proveedor en nube
Prestación	La emisión de un recurso
Procesador de datos	Una persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que procesa datos personales en nombre del controlador.
PV LAN	VLAN privada
RBAC	Control de acceso basado en funciones
Red de proximidad	En este contexto, una red de ordenadores que puede procesar y almacenar dato para ser entregados cerca del destino final
Resiliencia	La capacidad de un sistema para proporcionar y mantener un nivel aceptable de servicio ante fallos (no intencionados, intencionados o derivados de causas naturales)
ROI	Retorno sobre la inversión

ROSI	Retorno sobre la inversión de seguridad
RPO	Objetivo de Punto de recuperación
RTO	Objetivo de Tiempo de recuperación
RTSM	Supervisión de la seguridad en tiempo real
SLA	Acuerdo de nivel de servicio
SO	Sistema operativo
SO de alojamiento	El sistema operativo del proveedor en nube que ejecuta múltiples SO huésped
SO huésped	Un sistema operativo controlado por el cliente en nube que se ejecuta en un entorno virtualizado
SSL	Capa de conexión segura (utilizada para codificar el tráfico entre navegadores y servidores web)
Sujeto de los datos	**P**ersona física identificada o identificable (véase la Directiva UE 95/46/CE) de quien se recogen los datos y/o sobre quien se procesan los datos
TdU	Términos de uso
TLS	Seguridad de la Capa de transporte (utilizada para codificar el tráfico entre navegadores y servidores web)
UPS	Sistema de alimentación ininterrumpida
VLAN	Red de área local virtual
VM	Máquina virtual
VPC	Nube privada virtual
VPN (RED PRIVADA VIRTUAL)	Red privada virtual
Vulnerabilidad	Cualquier circunstancia o evento que puede repercutir de manera negativa sobre un activo

	mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de los datos y/o la denegación de servicio
XML	Lenguaje extensible de marcas

BIBLIOGRAFÍA

1. **IDC** *Cloud Computing 2010 - An IDC Update,* Frank Gens, Robert P Mahowald, Richard L Villars, Sep. 2009 - Doc # TB20090929, 2009

2. — *Western European Software-as-a-Service Forecast,* 2009–2013, David Bradshaw, Apr 2009 - Doc # LT02R9, 2009

3. **Administración General de Servicios de EE.UU. - GSA** [En línea] http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=-24825&P=&contentId=28477&contentType=GSA_BASIC

4. **Consejo de normas de seguridad PCI** [En línea] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

5. **NIST** [En línea] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

6. **Wikipedia** [En línea] http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_nube

7. **Craig Balding** *cloudsecurity.org.* [En línea] http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing/

8. **SUN - Proyecto Kenai** [En línea] http://kenai.com/projects/suncloudapis/pages/HelloCloud#Examining_the_Virtual_Data_Center

9. **CE – Comisión Europea** [En línea] http://ec.europa.eu/enterprise/policies/sme/small-business-act/index_en.htm

10. **ISO/IEC. ISO/IEC 27001:2008** ***Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Anexo E:*** *Enfoques de la evaluación de riesgos de la seguridad de la información,* 2008

11. **Wikipedia** [En línea] http://en.wikipedia.org/wiki/Open_Virtualization_Format

12. **MITRE** [En línea] http://cwe.mitre.org/data/definitions/400.html

13. **BBC** [En línea] http://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/6089736.stm

14. **www.retailresearch.org** [En línea] http://www.retailresearch.org/reports/fightinternalfraud.php

15. **NY Daily News** [En línea] http://www.nydailynews.com/gossip/2009/08/23/2009-08-23_outted_blogger_rosemary_port_blames_model_liskula_cohen_for_skank_stink.html

16. **Enterprise Storage Forum** [En línea] http://www.enterprisestorageforum.com/continuity/news/article.php/3800226

17. **Electronic Discovery Navigator** [En línea] http://www.ediscoverynavigator.com/statutesrules/

18. **Find Law** http://technology.findlaw.com [En línea] http://technology.findlaw.com/articles/01059/011253.html

19. **CBS 11 TV** [En línea] http://cbs11tv.com/local/Core.IP.Networks.2.974706.html

20. **WIRED** *www.wired.com/* [En línea] http://www.wired.com/threatlevel/2009/04/company-caught/

21. **Samuel T King, Peter M Chen, Yi-Min Wang, Chad Verbowsk, Helen J Wang, Jacob R Lorch** *SubVirt: Implementing malware with virtual machines.* 2006

22. **Secunia** [En línea] http://secunia.com/advisories/37081/

23. — [Online] http://secunia.com/advisories/36389/

24. **Kortchinsky, Kostya** *http://www.immunityinc.com* [En línea] http://www.immunityinc.com/documentation/cloudburst-vista.html.

25. **Ormandy, Tavis** [En línea] http://taviso.decsystem.org/virtsec.pdf

26. **Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage** [En línea] http://people.csail.mit.edu/tromer/papers/cloudsec.pdf

27. **Gentry, Craig** [En línea] http://delivery.acm.org/10.1145/1540000/1536440/p169-gentry.pdf?key1=1536440&key2=6166986521&coll=GUIDE&dl=GUIDE&CFID=60359435&CFTOKEN=10086693

28. **Schneier, Bruce** [En línea] http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html

29. **www.spywarewarrior.com** [En línea] http://www.spywarewarrior.com/uiuc/ss/revoke/pgp-revoke.htm

30. **RSA Laboratories, PKCS#11** [En línea] http://www.rsa.com/rsalabs/node.asp?id=2133

31. **Jun Zhou, Mingxing He** [En línea] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4716141

32. **Clulow, Tyler Moore and Jolyon** [En línea] http://people.seas.harvard.edu/~tmoore/ifipsec-pres.pdf

33. **Andrew Bechere, Alex Stamos, Nathan Wilcox** [En línea] http://www.slideshare.net/astamos/cloud-computing-security

34. **Wikipedia** [En linea] http://en.wikipedia.org/wiki/Token_bucket

35. — [En línea] http://en.wikipedia.org/wiki/Fair_queuing

36. — [En linea] http://en.wikipedia.org/wiki/Class-based_queueing

37. **Devera, Martin** [En línea] http://luxik.cdi.cz/~devik/qos/htb/old/htbtheory.htm

38. **Comunidad Xen de código abierto (Open Source Xen Community)** *http://xen.org/* [En línea]

39. **Acuerdo sobre el reconocimiento mutuo de criterios comunes (CCRA)** http://www.commoncriteriaportal.org/ [En línea]

40. **OWASP** [En línea] http://www.owasp.org/index.php/OWASP_Top_Ten_Project

41. — [En línea] http://www.owasp.org/index.php/Category:OWASP_Guide_Project

42. **27001:2005, ISO/IEC *Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información - Requisitos***

43. **27002:2005, ISO/IEC *Tecnología de la información – Técnicas de la seguridad – Código de buenas prácticas para la gestión de la seguridad de la información***

44. **Group, BSI** *BS 25999 Business Continuity*

45. **NIST** *Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems*

46. **OWASP** [En línea] http://www.owasp.org/index.php/Main_Page

47. **SANS Institute** [En línea] http://www.sans.org/reading_room/whitepapers/securecode/a_security_checklist_for_web_application_design_1389?show=1389.php&cat=securecode

48. **Software Assurance Forum for Excellence in Code (SAFECode)** [En línea] http://www.safecode.org

49. **IEEE Standards Association (Asociación de Normas del IEEE)** [En línea] http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

50. **The European Privacy Seal (Sello Europeo de Privacidad)** [En línea] https://www.european-privacy-seal.eu/

51. **EDRI - European Digital Rights** [En línea] http://www.edri.org/edri-gram/number7.2/international-standards-data-protection

52. **ISACA** [En línea] http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/COBIT_Publications/COBIT_Products.htm

53. **Oficina Gubernamental de Comercio (OGC)** [En línea] http://www.itil-officialsite.com/home/home.asp

54. **Luis M. Vaquero, Luis Rodero-Merino, Juan Cáceres, Maik Lindner** *A Break in the Clouds: Towards a Cloud Definition*

55. **Cloud Security Alliance**, Security Guidance for Critical Areas of Focus in Cloud Computing,

Abril 2009, *http://www.cloudsecurityalliance.org/guidance/csaguide.pdf*

56. ***Jericho Forum****, Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Abril 2009, http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf*

57. ***Gartne****r, Assessing the Security Risks of Cloud Computing, June 2008, http://www.gartner.com/DisplayDocument?id=685308*

58. ***Frente de liberación de datos****, Google, http://www.dataliberation.org/*

ANEXO I – COMPUTACIÓN EN NUBE – CUESTIONES LEGALES CLAVE

I. Se han identificado cinco cuestiones legales clave que son comunes a todos los escenarios:

1. protección de datos
   a. disponibilidad e integridad
   b. normas mínimas o garantía
2. confidencialidad
3. propiedad intelectual
4. negligencia profesional
5. servicios de subcontratación y cambios de control.

II. La mayor parte de las cuestiones identificadas en este análisis no son exclusivas de la computación en nube. De hecho, a los clientes de los servicios de computación en nube puede serles de ayuda utilizar el análisis legal aplicado a otros servicios de Internet como base sobre la que realizar su análisis legal de los riesgos de seguridad planteados por la computación en nube. Para evitar repetir análisis previos, nos hemos centrado en los aspectos de seguridad de la computación en nube que creemos que plantean nuevos desafíos legales o cambios materiales en relación con los análisis aplicados a las tecnologías de Internet previas.

III. Creemos que los clientes potenciales de los servicios en nube se mostrarán preocupados sobre cuestiones relativas a la protección de datos. Por ello, en este análisis legal nos hemos centrado en esta cuestión con mayor detalle que en otras.

IV. En tanto que este documento establece cinco cuestiones legales clave, un tema que es constante en todos los escenarios y en todos los debates sobre computación en nube es la necesidad de que los proveedores de computación en nube tengan contratos (y otros acuerdos y declaraciones) muy detallados y específicos de producto, y que los clientes revisen cuidadosamente estos contratos o la documentación relacionada. Las dos partes también deberían prestar mucha atención a los Acuerdos de nivel de servicio (SLA), ya que en los SLA están resueltas, o al menos mitigadas, las consideraciones de numerosas cuestiones legales asociadas con la computación en nube.

V. Antes de entrar en detalles legales, cabe señalar que los clientes de los proveedores en nube pueden diferir en tipología (de entidades privadas a públicas) y tamaño (de PYME a grandes empresas), y, por tanto, en la medida en que están en situación de negociar. Este punto es muy relevante desde el punto de vista legal, ya que la relación entre los proveedores en nube y sus clientes estará regulada mayoritariamente por medio de contratos. Debido a la falta de

regulaciones específicas, las funciones y obligaciones recíprocas se establecerán en el pliego de condiciones generales estándar, elaboradas de manera unilateral por el proveedor en nube y bien aceptadas por los clientes sin modificación (comúnmente), o negociadas en acuerdos específicos.

VI. La siguiente tabla resume las tres posibilidades relativas a la negociación de contratos y acuerdos entre el cliente y el proveedor en nube.

PROVEEDOR EN NUBE	**CLIENTE**
A) Gran empresa – **gran capacidad de negociar cláusulas de contrato**	PYME – **falta o debilidad en la capacidad de negociar cláusulas de contrato**
B) Tanto el cliente como el proveedor tienen **capacidad de negociar cláusulas de contrato**	
C) PYME – **Debilidad en la capacidad de negociar cláusulas de contrato**	Gran empresa o administración pública – **puede negociar cláusulas de contrato**

En función del caso particular (si se trata de A, B o C), la manera de abordar las cuestiones identificadas en *subsección* I puede variar de manera significativa.

VII. Es importante diferenciar entre el caso de una pequeña o mediana organización, que elegirá entre los diferentes contratos ofrecidos en el mercado, y una gran organización, que estará en situación de negociar las cláusulas. Es previsible que el principal beneficio comercial de la computación en nube se derive del hecho de que la computación en nube probablemente sea un servicio básico que podrá adquirirse con poca antelación o en la modalidad de pago por uso (por ejemplo, caso A: gran proveedor en nube – cliente PYME). Se asume una normalización de los servicios y por tanto de las condiciones legales. En consecuencia, en el análisis legal de este documento, tratamos las cuestiones principalmente desde la perspectiva de una PYME que está evaluando diferentes contratos, SLA, etc., que ofrece el mercado.

Sin embargo, puede haber situaciones en las que los servicios de computación en nube se adapten a grandes clientes, es decir, grandes empresas y administraciones públicas (por ejemplo, caso B). Ello implica contratos específicos y adaptados. Es probable que el caso C sea el menos común. En esa situación, habrá algún margen de negociación, como en el caso B. Sin embargo, las organizaciones más grandes pueden utilizar las mismas consideraciones al negociar contratos. Por este motivo, hemos incluido un debate de recomendaciones para la negociación, cuando esta sea posible.

Igualmente, conviene destacar que incluso cuando un cliente no puede negociar diferentes condiciones de un contrato con un proveedor específico, el cliente todavía es *libre de elegir entre las diferentes ofertas del mercado*. *En el caso de una PYME, por tanto, las*

recomendaciones para cláusulas contractuales específicas deben entenderse como preferencias entre ofertas del mercado.

VIII. El siguiente análisis describe y subraya cómo las cinco cuestiones legales clave seleccionadas pueden abordarse en los tres diferentes escenarios de negociación definidos en el párrafo VI.

1. Protección de los datos

Esta sección aborda las cuestiones legales de protección de datos que se plantearán frecuentemente con el uso de un servicio de computación en nube y pretende ofrecer orientaciones basadas en el redactado de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 2009, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[3] (en adelante: la «Directiva sobre protección de datos»). Sin embargo, dado que estas cuestiones estarán directamente gobernadas por la legislación nacional que aplique la Directiva sobre protección de datos, se aconseja a los clientes de los servicios de computación en nube reexaminar estas cuestiones en función de la legislación nacional aplicable.

Glosario

Las siguientes definiciones están establecidas en Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 2009, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante: la «Directiva sobre protección de datos»).

Datos personales se refiere a toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Datos sensibles se refiere a datos personales que revelen el origen racial o étnico, las convicciones religiosas, filosóficas o de otro tipo, las opiniones políticas, la pertenencia a partidos políticos, sindicatos, asociaciones u organizaciones de carácter religioso, filosófico, político o sindical, así como los datos personales relativos a la salud o a la sexualidad.

[3] El texto oficial de la Directiva 95/46/CE y el estado de aplicación puede consultarse en <http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm>

Tratamiento de datos personales (tratamiento) se refiere a cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Responsable del tratamiento se refiere a la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.

Encargado del tratamiento se refiere a la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Definición de las cuestiones

1.1. Teniendo en cuenta que los servicios ofrecidos por los proveedores en nube normalmente consisten en correo electrónico, mensajería, sistemas de sobremesa, gestión de proyectos, gestión de nóminas, contabilidad y finanzas, gestión de las relaciones con los clientes, gestión de ventas, desarrollo de aplicaciones personalizadas, aplicaciones personalizadas, telemedicina y facturación de clientes, se procesarán datos personales (incluidos datos sensibles). Estos datos pueden pertenecer a diferentes personas (interesados), por ejemplo: empleados, clientes, proveedores, pacientes, y, en general, socios comerciales.

1.2 Dado el hecho de que los datos personales se procesan indudablemente, es importante comprender exactamente cuándo se aplica la Directiva sobre Protección de Datos. El artículo 4 indica: ‘1. «1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; b) el responsable del

tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea».

1.3 Del análisis del artículo 4 de la Directiva sobre protección de datos se concluye que:

a) el lugar en que se ubica el responsable del tratamiento es relevante para la aplicación de la Directiva sobre protección de datos;

b) Lo que no es relevante para la aplicación de la Directiva sobre protección de datos es el lugar donde se procesan los datos personales o la residencia del interesado.

1.4 La Directiva sobre protección de datos se aplicará, por tanto, si el responsable del tratamiento está establecido en la UE y si el responsable del tratamiento no está establecido en la UE pero recurre a medios ubicados en la UE para el tratamiento de datos personales (por ejemplo, centros de datos para el almacenamiento y el tratamiento remoto de datos personales situados en el territorio de un Estado miembro, ordenadores, terminales, servidores), salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea[4].

1.5 Tras determinar que se aplica la Directiva sobre protección de datos, la siguiente pregunta es: ¿Quién es el responsable del tratamiento y quién es el encargado del tratamiento? Si el cliente del proveedor en nube determina el propósito y los medios del tratamiento de datos personales, él es el responsable del tratamiento, y si el proveedor en nube trata datos personales en nombre de su cliente él es el encargado

[4] Para obtener orientación adicional sobre la cuestión del establecimiento y el uso de equipos y determinantes para la aplicabilidad de la Directiva de protección de datos, véase el artículo 29, que contiene las opiniones del grupo de trabajo sobre protección de datos relativas a las redes sociales en línea y los motores de búsqueda – respectivamente, la Opinión 5/2009 sobre las redes sociales en línea, y la Opinión 1/2008 sobre las cuestiones relativas a la protección de datos vinculada a los motores de búsqueda, disponibles en la siguiente dirección: <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm>.

externo del tratamiento[5]. De hecho, la clasificación como responsable o encargado del tratamiento es muy diferente en relación con el cumplimiento de tareas y las obligaciones y responsabilidades asociadas. En nuestro análisis, asumimos que el cliente del proveedor en nube es el responsable del tratamiento y que el proveedor en nube es el encargado externo del tratamiento.

1.6 Las principales funciones y obligaciones del responsable del tratamiento que establece la Directiva sobre protección de datos son:

a) tratar los datos personales de acuerdo con los principios de equidad, legalidad, finalidad, adecuación, proporcionalidad, necesidad y minimización de datos (artículo 6 de la Directiva sobre protección de datos);

b) Obtener el consentimiento del interesado de forma inequívoca cuando se aplique el punto a) del artículo 7 de la Directiva 95/46[6].

c) llevar a cabo el tratamiento de datos personales tras haber comunicado al interesado la información necesaria (artículo 10 de la Directiva sobre protección de datos);

d) garantizar al interesado los derechos establecidos en el artículo 12 de la Directiva sobre protección de datos —por ejemplo: obtener confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, obtener información de los fines de dichos tratamientos, las categorías de datos a que

[5] Externo porque en el caso concreto, el encargado del tratamiento es un sujeto que no pertenece al ámbito de la organización/compañía del responsable del tratamiento.

[6] *El artículo 7 de la Directiva 95/46 afirma lo siguiente:*
Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:
a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
(f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

se refieran, los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; rectificar, suprimir o bloquear los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva; etc. (artículo 12 de la Directiva sobre protección de datos);

e) aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la pérdida accidental, la alteración, la difusión o el acceso no autorizados, y contra cualquier otro tratamiento ilícito de datos personales (artículo 17 de la Directiva sobre protección de datos);

f) elegir un encargado del tratamiento que ofrezca suficientes garantías respecto a las medidas de seguridad técnica y las medidas organizativas que controlan el tratamiento de datos a ejecutar, y asegurar el cumplimiento de esas medidas.

g) transferir los datos personales a terceros países que no aseguren un adecuado nivel de protección de acuerdo con el artículo 25 (2) de la Directiva sobre protección de datos únicamente si el interesado ha dado su consentimiento previo de forma inequívoca a la transferencia propuesta o con la condición de otros procedimientos aplicables del artículo 26 (por ejemplo, «cláusulas contractuales tipo» o —si los datos se transfieren a los Estados Unidos— «principio de puerto seguro»).

1.7 El responsable del tratamiento (en este análisis, el cliente en nube) debería ofrecer a los interesados (clientes finales del cliente en nube) toda la información obligatoria relativa al tratamiento de datos. Al amparo de la Directiva sobre protección de datos, se exigirá al cliente en nube que informe a sus clientes sobre las circunstancias de la transferencia al proveedor en nube, la calidad del proveedor en nube (es decir, el encargado externo del tratamiento), y los fines de la transferencia. De hecho, la subcontratación de los servicios mencionados anteriormente en 1.1 implica necesariamente la comunicación y transferencia de esos datos a terceros[7], (es decir, los proveedores en nube)[8], que pueden estar ubicados en Europa, pero también en

[7] *Obsérvese que en algunas leyes nacionales (por ejemplo, la ley alemana de protección de datos), los términos «transferencia» y «tercero» se definen como términos jurídicos que conllevan implicaciones legales concretas. El uso de estos términos en el presente documento no es objeto de dichas implicaciones.*

[8] Lamentablemente, no parece haber una definición oficial para la transferencia de datos. Sin embargo, del artículo 4 de la Directiva 95/46/CE podría deducirse que el tránsito de datos a través de los territorios no es relevante desde el punto de vista jurídico. Por ejemplo, si los datos se transfieren del Reino Unido a los Estados

países fuera del Espacio Económico Europeo (terceros países). Estos países pueden no ofrecer un adecuado nivel de protección de los datos personales, según el apartado 2 del artículo 25 de la Directiva sobre protección de datos. Es crucial que las entidades que recogen datos sujetos a la Directiva sobre protección de datos se aseguren de comprender la aplicación de la Directiva al uso y la transferencia de los datos. En este sentido, se aconseja a los responsables del tratamiento que actualmente no están implicados en la computación en nube buscar el consentimiento informado de los interesados para el tratamiento y la transferencia de datos fuera del Espacio Económico Europeo. Se aconseja a aquellos que actualmente trabajan en computación en nube que se aseguren de que se ha conseguido este consentimiento, y de que describe adecuadamente la naturaleza y el alcance del tratamiento y la transferencia. La alternativa sería poder aplicar uno de los procedimientos establecidos en el artículo 26 (por ejemplo, «cláusulas contractuales tipo» o «principio de puerto seguro», si los datos se transfieren a los Estados Unidos y el proveedor en nube participa en un programa de ese tipo). En realidad, esta segunda estrategia presenta algunas ventajas sobre la transferencia de datos basada en el consentimiento del interesado, ya que el interesado puede retirar este consentimiento en cualquier momento

1.8 Se recomienda que la Comisión aclare la aplicación del apartado 2 del artículo 25 de la Directiva cuando se aplica al posible tratamiento de datos en países fuera del Espacio Económico Europeo durante su transferencia desde un proveedor de computación en nube a otro, o dentro de la nube de una empresa, si esa nube está ubicada en jurisdicciones múltiples, una de las cuales se sitúa fuera del Espacio Económico Europeo.

1.9 Todas las partes implicadas en el tratamiento de datos (interesados, responsables del tratamiento y encargados del tratamiento) deben comprender sus derechos y obligaciones respectivas en relación con el tratamiento de datos, tal y como se define en la Directiva sobre protección de datos y en los instrumentos legales relevantes a escala nacional con los que la Directiva se ha aplicado en los distintos Estados miembro de la UE[9]. Además, estas partes también deben comprender el derecho a respetar la vida privada tal y como establece el artículo 8 del Convenio Europeo para la Protección

Unidos, el hecho de que los datos fluyan a través de enlaces de red ejecutados a través de Islandia, Groenlandia y Canadá no parece ser relevante desde el punto de vista legal.

[9] *Véase el estado de aplicación de la Directiva 95/46 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Puede consultarse en: <http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#spain>.*

de los Derechos Humanos y de las Libertades Fundamentales, en los casos en que los países implicados sean firmantes del Convenio o hayan aplicado legislación nacional que lo habilite.

1.10 Para aplicar la Directiva sobre protección de datos de manera adecuada, la disponibilidad e integridad de los datos es clave, lo que dirige el debate hacia las medidas de seguridad de los datos. En este contexto hay algunas concesiones inevitables. Una mayor seguridad de los datos probablemente dará lugar a una reducción de la disponibilidad. El cliente del proveedor en nube, de este modo, tal vez desee revisar las medidas de seguridad que pone en práctica el proveedor en nube y la disponibilidad de los datos que se garantiza. Ha de tenerse en cuenta que en la mayor parte de los países europeos existen requisitos obligatorios de seguridad de los datos. El cliente del proveedor en nube deberá asegurarse de que se cumplen esas medidas. En algunos casos (eHealth y, probablemente, escenarios de resistencia a los fallos en los que se tratan datos sensibles y financieros) el cliente puede incluso desear asegurarse de que se aplican medidas de seguridad de los datos todavía más estrictas en lo que respecta al almacenamiento de datos, la comunicación o la transferencia de datos, la recuperación de pérdida de datos y las transferencias futuras.

1.11 En este punto, debe quedar claro que el cliente —considerado como único responsable del tratamiento de datos— será la entidad responsable del tratamiento de datos personales en relación con los interesados. El cliente también será responsable de estos datos cuando este tratamiento se realice por parte del proveedor en nube en calidad de encargado externo del tratamiento. El incumplimiento de la Directiva sobre protección de datos puede llevar a sanciones administrativas, civiles y también penales, que difieren entre países, para el responsable del tratamiento. Estas sanciones están detalladas en gran medida en los instrumentos legales relevantes mediante los que se aplica la Directiva 95/46 en los diversos Estados miembros.

Gestión de estas cuestiones

1.12 Todas las cuestiones analizadas anteriormente pueden abordarse contractualmente. Además de asegurarse de recoger cualquier dato personal cumpliendo los artículos 7 y 10 de la Directiva sobre protección de datos, es decir, habiendo informado previamente de manera adecuada a los interesados y habiendo obtenido su consentimiento (si se necesita, según el artículo 7), los clientes en nube deberían revisar la presencia de una cláusula de protección de datos en el contrato entre el cliente y el proveedor en nube. Esta cláusula debería establecer las funciones y

obligaciones de las partes pertinentes. El cliente en nube debería tener en cuenta lo siguiente al evaluar esas cláusulas:

a. Teniendo en cuenta que el cliente en nube se clasifica como responsable del tratamiento según las disposiciones de la legislación de la UE sobre protección de datos, y que el cliente es legalmente responsable de la equidad, la legalidad, la finalidad, etc., deberían buscarse cláusulas que apoyen el cumplimiento de los principios de la Directiva sobre protección de datos por parte del cliente.

b. El proveedor en nube debería cooperar con el responsable del tratamiento para asegurar que éste puede garantizar efectivamente los derechos de los interesados de acuerdo con el artículo 12 de la Directiva sobre protección de datos.

c. El proveedor en nube debería poner en práctica medidas de seguridad adecuadas según el artículo 17 y el proveedor en nube debería notificar puntualmente al responsable del tratamiento de cualquier incumplimiento de la seguridad de los datos y cooperar rápidamente para solucionar el problema.

d. Las posibles transferencias de datos personales a terceros países que no garanticen un nivel adecuado de protección de acuerdo con el apartado 2 del artículo 25 de la Directiva sobre protección de datos deberían realizarse bien basándose en un consentimiento previo inequívoco a la transferencia del interesado o bien de acuerdo con otros procedimientos coherentes con el artículo 26 (por ejemplo, «cláusulas contractuales tipo» o «principio de puerto seguro», si los datos se transfieren a los Estados Unidos y el proveedor en nube participa en un programa de ese tipo). Debería tenerse en cuenta que la computación en nube puede consistir en la transferencia de datos. Puede ser difícil tratar esta cuestión contractualmente. Recomendamos que la Comisión Europea trate esta cuestión.

1.13 **Nótese que en el caso A** (véase *Introducción*, párrafo VI), el contrato, incluida la cláusula de protección de datos, será redactado por el proveedor en nube, dada la imposibilidad de negociar cláusulas contractuales entre un gran proveedor y numerosos pequeños clientes. Por tanto, el cliente potencial debería analizar cuidadosamente la disposición, para determinar si la cláusula aporta al cliente suficientes garantías de tratamiento lícito de los datos por parte del proveedor en nube, así como soluciones adecuadas para daños contractuales.

1.14 **En los casos B y C** (véase *Introducción*, párrafo VI), la cláusula de protección de datos estará sujeta a negociación. Además, las medidas de seguridad pueden abordarse en los anexos y en los SLA. Al abordar las cuestiones de seguridad, las partes deberán tener en cuenta que pueden no ser capaces de detallar todas las medidas de seguridad a abordar. Debido a que la seguridad de las TI constituye una carrera continua por hacer frente a cuestiones nuevas, las condiciones del contrato deben poder evolucionar en coherencia.

1.15 En los casos B y C (contratos de alto valor con posibilidad de negociación), también puede ser recomendable para el cliente negociar soluciones adecuadas a los daños contractuales, en caso de que se viole la cláusula de protección de datos. Por último, si la infracción del proveedor en nube es sustancial puede ser incluida en la lista de situaciones que conducen a una resolución unilateral del acuerdo.

1.16 Si el proveedor en nube está en un país fuera del Espacio Económico Europeo y ese país no ofrece un nivel adecuado de protección de datos, es recomendable contar con procedimientos coherentes con el artículo 26 (por ejemplo, «cláusulas contractuales tipo» o «principio de puerto seguro», si los datos se transfieren a los Estados Unidos y el proveedor en nube participa en un programa de ese tipo), en vez de basar la transferencia en el consentimiento del interesado (por el motivo indicado en la *subsección* 1.7). Sin embargo, hay que subrayar que la transferencia de datos dentro del territorio de los Estados miembros no está exenta de problemas. De hecho, a pesar de que los datos personales pueden circular libremente dentro de los Estados miembros, las leyes no son coherentes entre los países. Esta incoherencia puede generar dificultades evidentes en el cumplimiento y por tanto plantear cuestiones sobre la responsabilidad. Recomendamos que la Comisión de pasos hacia la normalización de los requisitos mínimos de protección de datos en Europa. Esto es particularmente importante a la luz del hecho de que la Directiva de protección de datos está siendo revisada actualmente. Además, un sistema de certificación de la protección de datos basado en normas mínimas de protección de datos, que sea común a todos los Estados miembros, puede ser de gran utilidad.

2. Confidencialidad

Definición de las cuestiones

2.1 En los escenarios considerados en este documento también se plantean preocupaciones sobre la confidencialidad. De hecho, en la nube se puede tratar información secreta y de «saber hacer». Cualquier fuga de información causada por una comunicación voluntaria del proveedor en nube o por una infracción de la seguridad de la nube puede poner en riesgo los servicios o la actividad empresarial del cliente. NB: en este contexto es crucial distinguir entre el tratamiento de datos, como el que se realiza en operaciones de computación con esos datos, y el almacenamiento o la transmisión de datos sin alterarlos, ya que el tratamiento en este modo normalmente requiere que los datos no estén codificados.

2.2 Parece oportuno analizar con más detalle el concepto de saber hacer y las posibles formas de protegerlo.

Saber hacer se define como un corpus de información que es secreto, sustancial e identificado de cualquier modo apropiado[10]. El término «secreto» significa que el paquete del saber hacer como un conjunto, o como la configuración precisa y el engranaje de sus componentes, normalmente no es conocido o fácilmente accesible. El término «identificado» significa que el saber hacer se describe o se registra de un modo que posibilita verificar que satisface los criterios de secreto y substancialidad. A estos efectos, «sustancial» significa que el saber hacer incluye información que es importante para el conjunto o para una parte significativa de:

i un proceso productivo, o
ii un producto o servicio, o
iii para el desarrollo del mismo y excluye información trivial.

2.3 No parece haber ninguna reglamentación europea aplicable a esos escenarios. Las regulaciones europeas relativas al saber hacer, expuesto en la definición anterior, se aplican principalmente a licencias y actividades que implican transferencia y explotación de la información.

Gestión de estas cuestiones

[10] *Véase el Reglamento (CE) nº 772/2004 de la Comisión, de 27 de abril de 2004, relativo a la aplicación del apartado 3 del artículo 81 del Tratado a determinadas categorías de acuerdos de transferencia de tecnología.*

2.4 Sin perder de vista los reglamentos, y con vistas a preservar el valor económico del saber hacer y de la información secreta en general, incluidos resultados de investigación e información relativa a proyectos y clientes, recomendamos que los clientes procuren condiciones contractuales que abarquen esta cuestión. De hecho, las funciones y obligaciones de las partes para preservar este valor deberían abordarse específicamente en una «cláusula de confidencialidad/no divulgación». Debería prestarse especial atención a los límites de las responsabilidades de las partes y las funciones relacionadas. Los anexos técnicos pueden ser apartados particularmente efectivos para abordar esta cuestión.

2.5 **En el caso A,** el cliente potencial del proveedor en nube debería analizar cuidadosamente la cláusula de confidencialidad/no divulgación para determinar si el proveedor en nube ofrece suficientes garantías para proteger la información secreta y el saber hacer del cliente que circularán en la nube.

2.6 **En los casos B y C,** recomendamos que las partes negocien una disposición que refleje el daño que una parte puede sufrir si la información confidencial o secreta se divulga. Si la divulgación es sustancial, esta infracción puede incluirse en la lista de casos que permiten a la empresa resolver unilateralmente el acuerdo.

3. Propiedad intelectual

Definición de las cuestiones

3.1 La propiedad intelectual también puede estar en riesgo en los escenarios de computación en nube.

3.2 Aunque una entidad que subcontrata servicios con el proveedor en nube puede proteger y hacer cumplir sus derechos de propiedad intelectual por medio de la legislación pertinente, similar en todos los Estados miembros, una infracción de los derechos de propiedad intelectual puede causar un perjuicio inmediato que nunca se revertirá plenamente en un proceso legal.

3.3 Además, en el caso improbable de que las interacciones entre el cliente y el proveedor en nube —por ejemplo, en la fase de negociación que será posible en los casos B o C— den lugar a resultados conjuntos que puedan ser objeto de derechos de propiedad intelectual (por ejemplo, técnicas para manejar mejor los datos). Por tanto, es acertado determinar quién poseerá esos derechos antes de iniciar las actividades de computación en nube, y determinar también el uso que las partes pueden hacer de los objetos de esos derechos.

Gestión de estas cuestiones

3.4 Los derechos de propiedad intelectual deberían regularse a través de cláusulas contractuales específicas: «Cláusula de propiedad intelectual» y «Cláusula de confidencialidad/no divulgación»[11].

3.5 **En el caso A,** el cliente potencial del proveedor en nube debería evaluar detenidamente el valor de su propiedad intelectual y los riesgos relativos a los servicios de computación en nube. Tras ello, el cliente debería revisar detenidamente las cláusulas relativas a la propiedad intelectual, para determinar si el proveedor en nube ofrece suficientes garantías y ofrece al cliente herramientas apropiadas para proteger su información (por ejemplo, a través de la codificación de los datos), para proteger los activos del cliente. El cliente en nube debería asegurarse de que el contrato respeta sus derechos de propiedad intelectual en la medida de lo posible sin comprometer la calidad del servicio ofrecido (por ejemplo, la creación de copias de respaldo puede ser un elemento necesario de la oferta de un buen nivel de servicio).

3.6 **En los casos B y C,** la «cláusula de propiedad intelectual» debería ser suficientemente detallada como para ofrecer normas para abordar las cuestiones descritas en el párrafo 3.3. Además, es recomendable que el cliente negocie una cláusula en la que se penalice al proveedor en nube si se violan las disposiciones sobre propiedad intelectual. Las infracciones sustanciales por parte del proveedor en nube pueden incluirse en la lista de casos que permiten a la empresa resolver unilateralmente el acuerdo.

4. Negligencia profesional

Definición de las cuestiones

4.1 Los errores en los servicios subcontratados al proveedor en nube pueden tener un impacto considerable en la capacidad del cliente para cumplir sus funciones y obligaciones para con sus propios clientes. El cliente, por tanto, puede estar expuesto a responsabilidades contractuales enrevesadas antes sus clientes por negligencia.

4.2 Los errores del proveedor en nube también pueden derivar en responsabilidad del cliente ante sus empleados. Dado que el cliente está subcontratando tecnología que ofrece, o permite, funciones internas críticas como el correo electrónico, la mensajería,

[11] *Con respecto a la «cláusula de confidencialidad/no divulgación», se aplica el párrafo 2.4 anterior.*

los sistemas de sobremesa, la gestión de proyectos y las nóminas, los errores del proveedor en nube, y la imposibilidad que resulta para los empleados del cliente de acceder a estas funciones o a los datos que se procesan, puede llevar a responsabilidades del cliente ante sus empleados.

4.4 Una cuestión relacionada es si las condiciones del contrato atribuyen responsabilidad al cliente por cualquier actividad ilegal realizada utilizando la cuentas autenticadas por las credenciales del cliente, pero sin que el cliente realmente las realice.

Gestión de estas cuestiones

4.5 **En el caso A,** el cliente debería revisar detenidamente la cláusula de limitación/exclusión (estándar) de responsabilidad a favor del proveedor en nube, para comprobar si es sostenible.

4.6 **En los casos B y C (es decir, en los casos poco frecuentes en los que se negocian contratos de alto valor)** recomendamos que, en la medida de lo posible, el cliente desplace sus responsabilidades en los casos mencionados anteriormente hacia el proveedor en nube, si ello es posible sin incurrir en costes más elevados derivados del desplazamiento de la responsabilidad. Ello puede conseguirse por medio de cláusulas de «limitación de la responsabilidad» y de «indemnización». Las infracciones sustanciales por parte del proveedor en nube pueden incluirse en la lista de casos que permiten al cliente resolver unilateralmente el acuerdo. Debería tenerse en cuenta, sin embargo, que el responsable del tratamiento siempre es legalmente responsable, de acuerdo con las disposiciones de las Directivas sobre protección de datos (1) (1), en lo que respecta a perjuicios a los interesados, independientemente de las cláusulas del contrato.

4.7 Recomendamos que la Comisión Europea ofrezca una aclaración legal sobre cómo se aplican las exenciones de responsabilidad de los intermediarios de la Directiva sobre comercio electrónico a los proveedores en nube.

5. Servicios de subcontratación y cambios de control

Definición de las cuestiones

5.1 Es probable que el acuerdo entre la empresa y el proveedor se defina como un contrato *intuitu personae.* Un contrato *intuitu personae* es aquel en el que una parte escoge contratar con una empresa basándose en cualidades que son únicas de esa empresa. Por ejemplo, un cliente puede elegir un proveedor en nube en particular por

las condiciones que ofrece, su renombre o profesionalidad, o sus habilidades técnicas. Como resultado, el cliente puede ser reacio a que el proveedor en nube subcontrate todos o parte de los servicios que ofrece al cliente.

5.2 El control del proveedor en nube también puede variar, y, como resultado, las condiciones de los servicios prestados por el proveedor en nube pueden variar igualmente.

Gestión de estas cuestiones

5.3 **En el caso A,** recomendamos que el cliente determine si los proveedores en nube subcontratarán los servicios y si el proveedor en nube ofrece alguna garantía relativa al funcionamiento de los servicios subcontratados. Sin embargo, no recomendamos que el cliente intente restringir la subcontratación de servicios por parte del proveedor en nube. También recomendamos que se revise el contrato para determinar cómo comunicará el proveedor en nube al cliente los cambios de control. El cliente debería también considerar si el contrato incluye el derecho a resolver el contrato si se produce un cambio de control.

5.4 **En los casos B y C,** el cliente *puede* elegir si requerirá que la subcontratación de servicios por parte del proveedor en nube esté sujeta a una autorización previa del cliente. Para decidirlo, el cliente necesitará estar informado sobre el tipo de servicios que el proveedor en nube pretende subcontratar y la identidad de la empresa a la que se subcontratarán estos servicios. Incluso si el cliente está de acuerdo con la subcontratación, puede pedir que el proveedor en nube le ofrezca garantías relativas al funcionamiento de los servicios subcontratados. Con el mismo razonamiento, el cliente también puede desear tener la oportunidad de aprobar un cambio de control, o de resolver o renegociar el contrato en el caso de un cambio de control del proveedor en nube. Dichas opciones pueden especificarse cuidadosamente en el contrato entre la empresa y el proveedor en nube por medio de una cláusula de «subcontratación a terceros», una cláusula de «garantías y compensaciones», una cláusula de «cambio de control», o una cláusula de «resolución del acuerdo» —en función del poder de negociación de las partes.

Conclusiones

Todas las cláusulas contractuales de las secciones 1, 2 y 3 son susceptibles de normalización, excepto las sanciones pertinentes, que dependen del poder de negociación de las partes. En la medida en que el contenido de las cláusulas contractuales de las secciones 4 y 5 depende esencialmente del poder de negociación de las partes, estas cláusulas son menos susceptibles de normalización.

ANEXO II – ESCENARIO DE USO DE PYME

UNA PERSPECTIVA DE LAS PYME SOBRE LA COMPUTACIÓN EN NUBE

Evaluación de riesgos de la seguridad de la computación en nube de la ENISA

Este escenario se ha utilizado como base para el análisis de riesgos publicado en el informe.

Limitaciones e hipótesis

Este escenario se basa parcialmente en los resultados del estudio: Una perspectiva de las PYME sobre la Computación en nube [REF]. El escenario NO pretende ser una hoja de ruta para las compañías que están considerando, planificando o ejecutando inversiones y proyectos de computación en nube.
La selección como caso de uso una compañía de tamaño mediano se realizó para garantizar que la evaluación tuviera un elevado nivel de TI y complejidad jurídica y empresarial. El objetivo era exponer toda la información posible sobre riesgos a la seguridad. Algunos de estos riesgos son específicos de las pequeñas y medianas empresas, mientras que otros son riesgos generales a los que todas las microempresas o pequeñas empresas se enfrenten probablemente durante la migración a un entorno de computación en nube.
La pretensión NO es que el escenario sea totalmente realista para una organización individual, sino que es probable que todos los elementos del escenario se den con frecuencia en muchas organizaciones; actualmente no existe ningún proveedor único en el mercado que pueda abarcar la amplitud de los servicios descritos en el escenario, sino que todo los servicios están cubiertos por varios proveedores.
La cesión de las aplicaciones a cada nivel (IaaS, PaaS, SaaS) es arbitraria, y se lleva a cabo únicamente con fines ilustrativos, SIN ánimo de ser una recomendación.

Escenario

La compañía CleanFuture desarrolla su actividad en el sector fotovoltaico. La compañía produce y suministra sistemas integrales fotovoltaicos y solares y piezas clave para los sistemas solares y de calefacción. La compañía se creó en 1999 en Alemania, donde está ubicado el principal centro de producción. Desde entonces, CleanFuture ha crecido a un ritmo rápido, y su volumen de ventas se ha incrementado en un promedio anual del 20 %.

En 2003 se inauguró una sucursal en España, y en 2004 se abrieron nuevas oficinas en Italia. En 2005 se tomó la decisión de reubicar la línea de producción de vidrio solar antirreflectante a Polonia, y en junio de 2006 la fábrica ya estaba produciendo los primeros ejemplares. La compañía también tiene previsto explorar el mercado de los Estados Unidos.

CleanFuture emplea a 93 personas:

- 50 en Alemania (en dos emplazamientos distintos: la sede (incluida la central de producción y el laboratorio) y una sucursal))
- 34 en Polonia
- 5 en España
- 4 en Italia.

La compañía también tiene un número variable de contratistas (entre 10 y 30 agentes provisionales, representantes de ventas, asesores, personas en prácticas, etc.).

A raíz de la presión de la competencia y de la crisis económico-financiera de 2008-2009, CleanFuture inició un debate interno sobre una estrategia de futuro muy cercano para reducir gastos e incrementar la productividad. Los servicios de TI se identificaron como un ámbito crucial en el que había un amplio margen de mejora.
Se analizaron internamente los requisitos de seguridad y TI y se llegó a las siguientes conclusiones:

1. Se necesitan una mayor flexibilidad y escalabilidad para responder a las demandas variables de servicios informáticos (un número variable de empleados durante el año, un numero variable de socios y proveedores, cambios repentinos en la situación del mercado, posible cooperación con un centro de investigación y universidades, posible inauguración de sucursales y ampliación de la fuerza de ventas, etc.).
2. La compañía requiere servicios de TI de gran calidad (en cuanto a efectividad y rendimiento) y un alto nivel de seguridad de la información (en cuanto a disponibilidad, integridad y confidencialidad). No obstante, a fin de proporcionar recursos internos (departamento de TI) con tan elevados niveles de servicio, se necesitan conocimientos específicos combinados con una inversión de capital en hardware, software, soporte informático y seguridad de la información.
3. La continuidad del negocio y las capacidad de recuperación en caso de desastre deben mejorarse.
4. Contar con un banco de pruebas para evaluar nuevas aplicaciones de apoyo al negocio, así como un entorno de cooperación en el que los desarrolladores puedan trabajar junto a los

socios en la búsqueda de nuevas soluciones y proyectos serían elementos cruciales desde la perspectiva de la efectividad empresarial y la capacidad de innovación.

5. Un proyecto de migración de físico a virtual (P2V) proporcionaría información de referencia importante en cuanto a la fiabilidad y la eficiencia de la configuración final.

Los servicios y aplicaciones identificados como afectados por el nuevo enfoque de TI fueron:

- el correo electrónico y el servicio de mensajería
- sistemas de sobremesa (aplicaciones de oficina)
- gestión de proyectos
- nóminas
- CRM y gestión de ventas
- contabilidad y finanzas
- ejecución o alojamiento de aplicaciones personalizadas y desarrollo de aplicaciones personalizadas
- gestión de la identidad.

El grupo de trabajo interno, apoyado por un asesor externo, propuso las tecnologías de computación en nube como posible solución a las necesidades de CleanFuture.

El siguiente paso fue llevar a cabo un estudio de viabilidad sobre la computación en nube. Se entregó un informe al Consejo de administración de la compañía: «CleanFuture – Un estudio de viabilidad sobre la computación en nube: posible estrategia de implementación e inquietudes de seguridad, legales y empresariales asociadas».
Basándose en el análisis del grupo de trabajo ad-hoc, el informe propone la subcontratación de las aplicaciones y servicios de TI identificados a tres proveedores en nube como mínimo. A largo plazo, los tres proveedores podrían formar lo que se denomina una «federación de nubes», pero de momento se recomienda que, en aras de la sencillez, se utilicen tres proveedores independientes vinculados a través de una solución de «gestión federada de la identidad».

1. Proveedor en nube nº 1: ofrecerá un servicio de alojamiento basado en la nube para el correo electrónico, el servicio de mensajería, los entornos de sobremesa, la gestión de proyectos y las nóminas (un modelo «software como servicio» (SaaS) de computación en nube). Contractualmente, los datos pueden estar ubicados y procesados en distintas ubicaciones de todo el mundo, incluidos Asia, Europa y los Estados Unidos.
2. Proveedor en nube nº 2: ofrecerá una plataforma basada en la nube para el alojamiento de aplicaciones personalizadas, denominada frecuentemente como el modelo «plataforma como servicio» (PaaS) de computación en nube. Esta aplicación personalizada consiste en un

«simulador que ayuda a los clientes a configurar ellos mismos la instalación fotovoltaica, calcular la producción de energía (en función de su ubicación geográfica) y el ROI (dependiendo del incentivo del país en el que se llevará a cabo la instalación).

3. Proveedor en nube nº 3: ofrecerá una infraestructura basada en la nube para los departamentos de recursos humanos, contabilidad y finanzas, CRM y gestión de ventas y desarrollo de aplicaciones personalizadas (el modelo «infraestructura como servicio » (IaaS) de computación en nube).
   A corto plazo (dos años), CleanFuture se ocupará de la continuidad del negocio y de la recuperación en caso de desastre de los datos y servicios subcontratados a los proveedores PaaS e IaaS. Esta medida se llevará a cabo utilizando la infraestructura existente. El proveedor SaaS asume la responsabilidad de los requisitos de continuidad del negocio y las copias de seguridad de los servicios que presta. En ambos casos, el servicio de copia de seguridad lo prestan conjuntamente el proveedor y CleanFuture durante un período de dos años.

El plan estratégico a medio plazo para la recuperación en caso de desastre todavía está por definir. Las dos opciones siguientes deben compararse:

I. para identificar un socio comercial con quien crear una pequeña nube privada y compartir las capacidades y el gasto de una infraestructura de este tipo;
II. para adquirir servicios de recuperación en caso de desastre y continuidad del negocio de cada proveedor en nube.

La decisión se tomará en el plazo de dos años, cuando la actual infraestructura de TI se quede obsoleta. Hasta entonces CleanFuture utilizará su tecnología interna y su alojamiento in situ para sus necesidades de continuidad y recuperación.

Gestión de la identidad

El informe identifica la gestión de la identidad como elemento que afecta a todos los aspectos de la migración. Por motivos de fiabilidad y escalabilidad, CleanFuture NO debe confiar a largo plazo en un directorio interno de compañías para la gestión de cuentas y la autenticación de usuarios. Una solución escalable, resistente a los fallos y válida para el futuro debe proporcionar:

a. un inicio de sesión único
b. un fin de sesión único
c. un directorio de identidad único para todos los servicios
d. una aplicación única para el alta y la baja de identidades
e. la gestión segura de cualquier clave criptográfica utilizada para la autenticación y la firma
f. el cumplimiento de la política de control de accesos (por ejemplo, utilizando XACML). una solución que garantice que TODOS los usuarios (miembros del personal, socios, contratistas) cumplan con los requisitos de línea de base de seguridad de la compañía.

estos requisitos deberán establecerse con arreglo a las características del permiso y el perfil de usuario. Los requisitos mínimos establecidos deben ser: un antivirus y un SO actualizados.

El informe recomienda el cambio a una solución federada de gestión de la identidad que desacople las distintas cuentas necesarias en distintos proveedores de solución de servicios de gestión y alta de identidades. Un breve estudio muestra que son pocas las soluciones de nube existentes que proporcionan las interfaces necesarias para disponer de una solución FIM integral. Esto, a su vez, genera un conjunto de requisitos importantes con respecto a la migración:

1. Los servicios seleccionados deben soportar la autenticación a través de un marco FIM seleccionado (implementación que utilice Liberty/Cardspace + SAML 2.0).
2. Antes de migrar cualquier servicio y aplicación a la nube, CleanFuture debe implementar una solución de inicio de sesión único para todas sus aplicaciones, incluida la autenticación de socios externos.
3. Las propiedades de responsabilidad de cualquier infraestructura de gestión clave deben verificarse detenidamente.
4. Debe definirse una línea de base de clientes de seguridad para todos los clientes que acceden a todos los servicios.

Proyecto	Fase 1 - 2008	Fase 2 - 2009	Fase 3 - 2010	Fase 4 - 2011	Fase 5 - 2012
Migración física a virtual (P2V)	Adopción de una plataforma de visualización dentro de la compañía, realización de una migración física a virtual (P2V) de las siguientes aplicaciones: CRM y Gestión de ventas, Aplicación personalizada, RH	Verificación de la fiabilidad y del rendimiento de la solución de la fase 1 Migración P2V a la siguiente aplicación: Contabilidad y finanzas	Verificación de la fiabilidad y del rendimiento de la solución de la fase 2 Migración a solución FIM SSO y solución de gestión		

		Selección de FIM y soluciones de gestión clave.	clave.		
Migración a la computación en nube: **PROVEEDOR Nº 1 - SaaS**			Selección del proveedor en nube (SaaS) y migración de la siguiente aplicación: Gestión de proyectos*	Migración de las siguientes aplicaciones y servicios: Correo electrónico*, mensajería*, sistemas de sobremesa*, nóminas*	
Migración a la computación en nube: **PROVEEDOR Nº 2 - PaaS**	----		Selección del proveedor en nube (PaaS) y migración de las siguientes aplicaciones: CRM y gestión de ventas	Verificación de la fiabilidad y del rendimiento del Proveedor PaaS Migración de las siguientes aplicaciones: Aplicaciones personalizadas, Contabilidad y finanzas y	Verificación de la fiabilidad y del rendimiento del Proveedor PaaS Migración de la siguiente aplicación: Desarrollo de aplicaciones personalizadas

				RH	
Desarrollo de socio de nube privada para DR y BC			Identificación de socios, definición de los requisitos del proyecto…	Definición de plan ejecutivo…	Activación de la nube privada.

*Obsérvese que estas aplicaciones o servicios se subcontrataron a un proveedor de computación en nube sin realizar ninguna migración interna física a virtual.

Controles de seguridad existentes

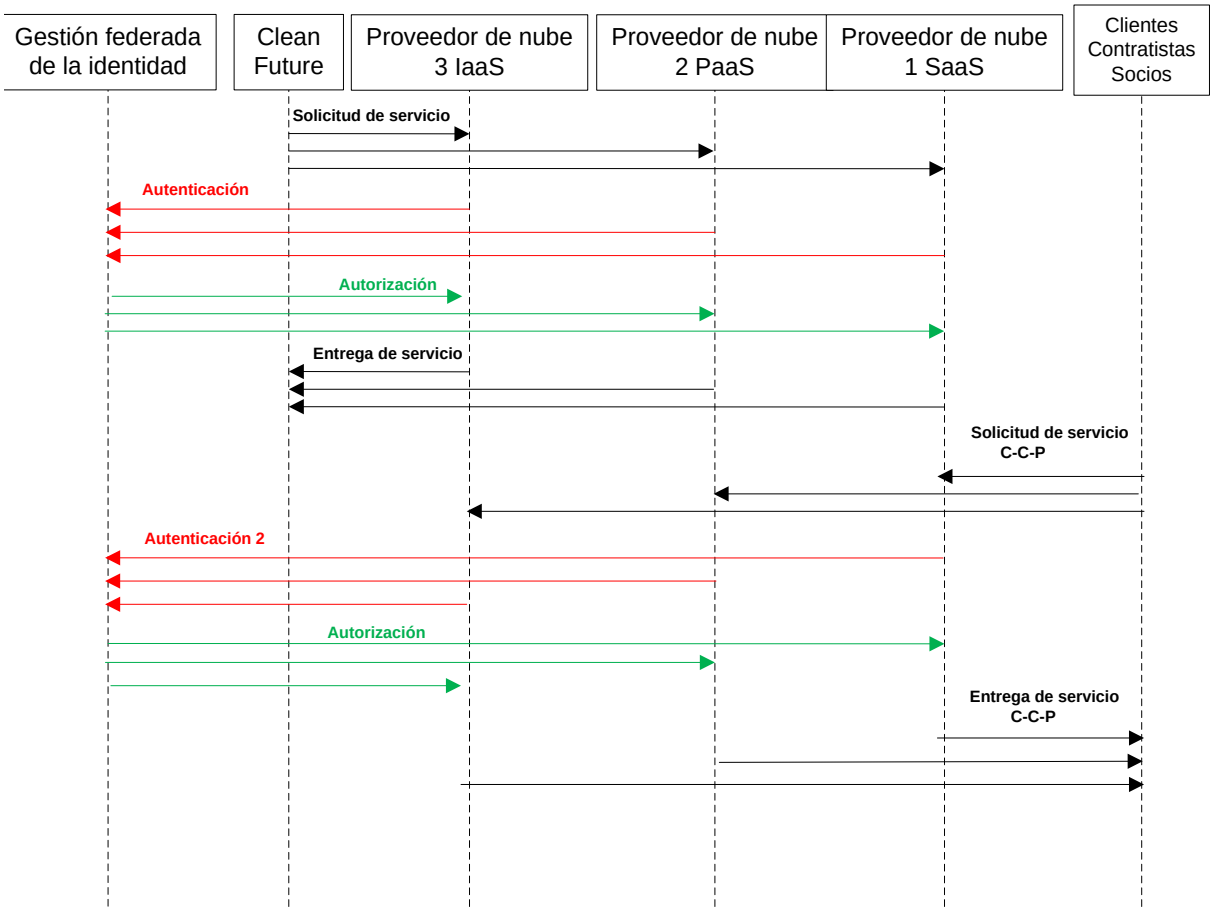
El proveedor nº 1 (SaaS) y el proveedor nº 2 (PaaS) afirman implementar un conjunto de controles de seguridad estándar que incluye:

- cortafuegos
- IDS/IPS (con base en la red y en el alojamiento)
- refuerzo del sistema y pruebas de penetración dentro de la compañía
- gestión de parches e incidentes conforme a ITIL.

No se facilitan detalles adicionales. CleanFuture realizó la selección de los proveedores sobre la base del buen renombre del Proveedor nº 1 y el Proveedor nº 2.
El Proveedor nº 3 (IaaS) ofrece instancias preconfiguradas de VM en distintas configuraciones estándar. Sin embargo, no ofrecen instancias reforzadas previamente por defecto, es decir, el cliente es el único responsable de todas las medidas de seguridad en las instancias VM, incluida la revisión de toda la configuración por defecto.
El Proveedor nº 3 especifica las comprobaciones de fondo realizadas sobre todos los empleados (con ciertas limitaciones determinadas por la legislación local), el control del acceso físico basado en tarjetas inteligentes biométricas y las políticas de control del acceso a datos basados en la premisa *«need-to-know»*.
Todas las conexiones (para IaaS, PaaS, SaaS, IDM, etc.), EXCEPTO las que incluyen clientes (por ejemplo, que usan la aplicación de configuración) están codificadas (bien vía VPN o SSH).
Todos los proveedores cumplen la norma ISO 27001, pero ninguno de ellos declara el ámbito preciso de la certificación.
El Acuerdo de nivel de servicio con cada proveedor incluye una cláusula de notificación de incumplimiento. Todos los proveedores ofrecen prestaciones de notificación de seguridad premium (de pago). Estos informes de pago pueden incluir: incumplimientos fallidos (de los activos del cliente),

ataques contra objetivos específicos (por usuario de compañía, por aplicación concreta, por máquina física específica, ratio de ataques internos comparados con los ataques externos, etc.), tendencias y estadísticas.
El umbral de notificación para los intentos fallidos y la escala de gravedad de los incidentes se personalizan en función de las necesidades específicas del cliente.

Flujo de datos



ANEXO III – OTROS ESCENARIOS DE USO

Aquí puede encontrar un breve resumen de los escenarios de resistencia a los fallos y *eHealth* que utilizamos en nuestro análisis de riesgos.

ESCENARIO DE RESISTENCIA

Este escenario explora el modo en que el uso de la computación en nube afecta a la resistencia a los fallos de los servicios ante:

- incrementos repentinos de la demanda de cliente (por ejemplo, en períodos de crisis financiera)
- ataques de denegación de servicio
- catástrofes naturales localizadas
- uso indebido de la infraestructura como plataforma de ataque
- fugas de datos (iniciados maliciosos o descuidados o ruptura de procesos).

El año es 2012. XK-Ord proporciona comercio electrónico en tiempo real a través de una interfaz de servicio web, junto con soluciones de entrega de contenido en forma de productos hipotéticos que pueden integrarse en portales de adquisición. Entre los casos de uso típicos se encuentran:

- datos de precios en tiempo real y diagramas de artículos en portales de adquisición
- historial de datos para utilizar en análisis y predicciones de precios
- historias de orden e informes de control de existencias para compañías
- conversión de divisas en tiempo real e historial de FX
- informes comerciales antimonopolio actualizados de SOX y UE
- datos financieros para aplicaciones más complejas.

Además, XK-Ord ofrece una plataforma para gestionar los distintos servicios y combinarlos en aplicaciones personalizadas. Habida cuenta de su oferta de servicios, XK-Ord requiere un alto nivel de resistencia a los fallos de:

- latencia – los retrasos en el suministro de datos pueden dar lugar a la pérdida de oportunidades valiosas;
- solicitud de cumplimiento – por ejemplo, gran fiabilidad de:
  - consultas a bases de datos y presentación de resultados
  - cumplimiento del servidor web de las solicitudes de http
  - infraestructura TCP/IP;
- integridad de los datos – los errores en los datos pueden dar lugar a pérdidas económicas;

- confidencialidad e información: los datos tienen valor financiero, y en consecuencia, si se divulgan a clientes que no pagan por dicho servicio, se incurre un pérdida financiera en perjuicio de XK-Ord;
- vulnerabilidades e integridad de la aplicación.

Infraestructura

En 2011, XK-Ord cambió a una infraestructura de nube por motivos de costes, flexibilidad y fiabilidad. XK-Ord utiliza sistemas de CumuloNimbus, un proveedor en nube que ofrece IaaS para la entrega de contenido.

- Los datos se almacenan utilizando un modelo DaaS (base de datos como servicio).
- La gestión de cuentas de cliente de XK-Ord y la CRM, incluida la facturación, están gestionadas por un segundo proveedor en nube, Stratocumulus. Las credenciales son emitidas y verificadas por XK-Ord utilizando este servicio, mientras que el control del acceso al contenido se proporciona a través de los recursos de CumuloNimbus, es decir, Stratocumulus actúa como proveedor federado de identidad y proporciona un inicio de sesión único.
- Los sistemas de I+D y las aplicaciones de sobremesa de oficina, las nóminas y los recursos humanos de XK-Ord se gestionan directamente y se alojan in situ por parte de XK-Ord.

Red

En comparación con el uso de un centro de datos, la infraestructura de los proveedores en nube ofrece mejoras considerables en el ancho de banda total, el procesamiento, las capacidades de almacenamiento y memoria y la capacidad de escalar límites rápidamente. Por ejemplo, los routers ubicados cerca de los emplazamientos de entrega de contenidos utilizan recursos escalables de filtrado de paquetes, inicios de sesión y memoria virtualizada. IPSec se implementa en partes de la red. Estas características mejoran considerablemente a resistencia frente a los ataques DDoS.

Gestión de los recursos

- La entrega de contenido se carga a XK-Ord basándose en solicitudes por HTTP. Los costes se limitan en función de la selección de políticas ofrecidas por CumuloNimbus. Los clientes de XK-Ord reciben los cargos en función del número de solicitudes HTTP a cada servicio, conforme a un sistema diferente.

- El proveedor opera los recursos basándose en una prestación compartida con otros clientes (que no tienen por qué ser similares) en toda la infraestructura. Esto significa que el aislamiento entre los recursos utilizados por los distintos clientes debe ser sólido. XK-Ord posee la opción de abonar una tasa reducida para reservar los recursos de manera anticipada, lo cual aumenta la fiabilidad total para el proveedor del servicio y para XK-Ord.
- El crecimiento a corto plazo dentro de los recursos disponibles es más rápido que en las infraestructuras típicas de tipo distinto a la nube. La integración de más recursos de expansión (es decir, más hardware para el proveedor en nube) es lenta. Las defensas frente a ataques DDoS en particular deben escalar rápidamente, y las implicaciones de gastos uso de recursos deben estar definidas claramente.
- Se utilizan SLA y API estándar para favorecer el movimiento entre nubes.

Servicios de seguridad

XK utiliza un proveedor de servicios de seguridad, BorealisSec, para la supervisión de la seguridad en tiempo real (RTM), la evaluación de vulnerabilidades y la gestión de dispositivos.

- El personal de BorealisSec gestiona los sistemas de XK alojados en Cumulonimbus utilizando una conexión VPN.
- Los registros se recogen en Cumulonimbus y se envían automáticamente a la plataforma SIEM (información de seguridad y gestión de eventos) de BorealisSec a través de la VPN, para ser analizados.

Si se produce un incidente, puede ocurrir que:

- Un administrador de BorealisSec se ocupe del incidente directamente (automática o manualmente) o
- que abran una incidencia con CumuloNimbus para resolver el problema.

En cualquier caso, la respuesta a los incidentes se acordará mediante contrato con XK, en función de la gravedad. Cabe señalar los demás puntos siguientes:

- La evaluación de la vulnerabilidad sólo puede realizarse sobre una instalación de pruebas, puesto que los TdU de Cumulonimbus prohíben las pruebas proactivas de seguridad.
- BorealisSec proporciona informes de cumplimiento y auditoría en la medida en que los TdU de CumuloNimbus lo permiten.
- BorealisSec es responsable de mantener los parches de software fuera del ámbito del proveedor en nube.

SLA: XK-Fin -> clientes

XK-Ord ofrece un Acuerdo de nivel de servicio (SLA) a sus clientes para competir con otras compañías de datos financieros que ofrecen SLA. Cabe señalar que el SLA de XK puede ofrecer niveles de fiabilidad más altos que Cumulonimbus, a pesar de la dependencia entre ambas compañías. Ello puede deberse a que XK está dispuesto a aceptar un nivel de riesgo mayor.

Meta	KPI	Valor	Penalizaciones
Disponibilidad del servicio	Porcentaje de tiempo de actividad al mes	99,99	Reducción del 20 % de la factura por cada factor de 10
Latencia (NB: el tiempo desde el que la bolsa publica los datos)	Tiempo medio de respuesta sobre 100 peticiones en 1 día	1 seg.	Reducción del 5 % de la factura por cada incumplimiento
Administración	Tiempo para responder a la petición en minutos	60 min.	Reducción del 5 % de la factura por cada incumplimiento
Alertas	Minutos para alertar al cliente de un incumplimiento del servicio (sin incluir éste…)	5 min.	Reducción del 5 % de la factura por cada incumplimiento
Tiempo para recuperarse del fallo	Horas	2 horas	Reducción del 5 % de la factura por cada incumplimiento

ESCENARIO DE EHEALTH

Este escenario explora el uso de la computación en nube por parte de los grandes organismos gubernamentales que deben cumplir requisitos reglamentarios rigurosos y son muy sensibles a la percepción negativa del público. Una consideración clave —a la hora de utilizar servicios de nube— es la percepción pública de que puede haberse producido una falta de consideración de cuestiones de privacidad o seguridad. Esto sería especialmente cierto en caso de utilizar servicios en nube «públicos».

EuropeanHealth representa un servicio de salud gubernamental amplio en Europa, *pero no describe ningún servicio de salud nacional concreto. EuropeanHealth* está compuesto de organizaciones públicas y proveedores privados que ofrecen servicios de *eHealth*. Se trata de una organización de

gran tamaño que se extiende en varias ubicaciones y atiende a sesenta millones de ciudadanos. Anes de utilizar cualquier tipo de infraestructura de nube, tenía más de veinte proveedores de servicios de TI y más de cincuenta centros de datos.

Escenario específico

El escenario específico implica una plataforma de eHealth que proporcione cuidados y seguimiento domiciliario de pacientes con enfermedades crónicas. Este proceso general se describe con más detalle como sigue:

1. Un centro de supervisión utiliza una plataforma independiente con base en Internet que despliega sensores en el domicilio para supervisar e interactuar con los pacientes mayores en su casa.
2. Las variables controladas se analizan para detectar anomalías basándose en un perfil. Un centro de supervisión decide cuándo se necesitan servicios más especializados (médicos, enfermeras, etc.).
3. Los pacientes también pueden elegir poner la información a disposición de proveedores de servicios externos de eHealth. Dicha información privada se proporciona a través de una base de datos centralizada.
4. Los servicios se ofrecen a los pacientes mayores en su casa, utilizando una interfaz multimodal que se adapta a las capacidades de los ancianos. Pueden utilizarse personajes digitales y síntesis de voz.

Los datos supervisados se ponen a disposición de médicos y hospitales a través del servicio de registros médicos de pacientes. Puede accederse a la información sobre los pacientes a través del identificador único de pacientes. Este servicio proporciona documentación relativa a los cuidados y al historial médico del paciente.

Gov-cloud

Para entregar estos servicios mediante una infraestructura de nube, EuropeanHealth utiliza ***Gov-Cloud***, un servicio de nube proporcionado por los gobiernos nacionales para los servicios gubernamentales en su conjunto. Se trata de una nube híbrida privada-asociada, puesto que únicamente la utilizan socios fiables y organizaciones gubernamentales que tienen acceso administrativo (por ejemplo, la administración pública y los servicios sanitarios). Utiliza una infraestructura de red dedicada que es físicamente independiente de la Internet pública. Gov-cloud se aloja en múltiples ubicaciones geográficas, pero las máquinas virtuales pueden migrar de un emplazamiento a otro.
Todos los servicios de nuestro escenario concreto ejecutan Gov-Cloud con las propiedades de seguridad que se describen a continuación. Por ejemplo:

- algunos de los servicios que se ejecutan en casa se ejecutan en la nube utilizando IaaS;

- los servicios que se ejecutan en el centro de control se ejecutan en la nube utilizando IaaS;
- los datos supervisados también se almacenan en la nube a través de DaaS (base de datos como servicio).

Gov-Cloud también proporciona un medio de transferir los datos de los pacientes de manera segura (ya que antes esta acción era bastante difícil de ejecutar) utilizando un servicio personalizado de correo electrónico para médicos y enfermeras. Este servicio se suministra a través de terceros, aunque es EuropeanHealth quien lo diseña.

Protección de los datos

Todos los datos recabados por EuropeanHealth deben cumplir los siguientes requisitos:

- Los datos (incluida la información personal sensible) deben codificarse en tránsito y quedarse estáticos cuando corren peligro (por ejemplo, en los dispositivos móviles).
- El procesamiento de datos debe ajustarse a la legislación europea en materia de protección de datos (por ejemplo, definición de «procesador de datos» para todas las operaciones).
- La legislación nacional aplica determinadas restricciones sobre el procesamiento de los datos (por ejemplo, los datos no deben abandonar el país original de recogida en ningún momento).
- La seguridad clínica debe ser enorme en el caso de determinadas aplicaciones; ello significa que la integridad y la disponibilidad deben «garantizarse» en algunas situaciones.
- Los datos sensibles deben destruirse en un momento específico de su ciclo de vida (por ejemplo, destruyendo los discos duros en el final de la vida de los equipos).
- Deben garantizarse controles de seguridad física en los centros de datos en los que se almacenan los datos (algunos de estos controles se incluyen en las presentaciones ISO 27001 de los proveedores).
- El personal ejecutivo recibe responsabilidades especiales con respecto a la confidencialidad de «la información del paciente y el usuario del servicio».

Cumplimiento de leyes, reglamentos y mejores prácticas

- Todos los proveedores deben demostrar que cumplen la norma ISO 27001. NO se les exige la acreditación, pero se verifica el cumplimiento a través de la presentación anual de su sistema de gestión de la seguridad de la información y de los documentos de política asociados.
- Otras certificaciones y acreditaciones ayudan a las organizaciones de EuropeanHealth a seleccionar los proveedores apropiados, por ejemplo, ISO 20000 (gestión del servicio), ISO 9001 (calidad), etc., pero no son un requisito necesario.
- En cuanto a auditoría y cumplimiento de los reglamentos o las normas designadas por el proveedor de servicios, los proveedores de servicios de computación en nube deben

asegurarse de que pueden y quieren permitir el derecho a auditar sus políticas, procesos, sistemas y servicios.

Gobernanza

Gov-Cloud ofrece un conjunto básico de controles de seguridad, y los servicios de gestión o la gestión interna de cada usuario de Gov-Cloud (como EuropeanHealth) ofrece la opción de aplicar controles adicionales. Se utilizan normas de gobernanza, como ITIL.
EuropeanHealth no puede ordenar a los departamentos internos que adopten tecnologías específicas, sino únicamente recomendar dicha adopción. Los departamentos de EuropeanHealth siguen siendo libres para implementar la tecnología que mejor se ajusta a sus necesidades.
EuropeanHealth puede solicitar a las organizaciones participantes que presenten documentación en la que se muestre que sus recomendaciones han sido seguidas, por ejemplo, evidencias de que todos los datos de los ordenadores portátiles están codificados. Para los proveedores externos existen requisitos específicos para que las organizaciones se conecten a la red EuropeanHealth y se mantengan conectadas.

Control del acceso y confirmación de auditoría

EuropeanHealth ofrece el inicio de sesión único (SSO) para aquellas de sus aplicaciones y servicios que utilizan tarjetas inteligentes como símbolos de autenticación. Las organizaciones de EuropeanHealth pueden utilizar muchos otros modos de autenticación o múltiples formas con distintos fines (factor único, dos factores, biométrica, etc.). Los terceros proveedores de Gov-Cloud interactúan con la interfaz de EuropeanHealth PKI mediante tarjetas inteligentes.

Existen requisitos imperativos en términos de auditoría para garantizar que queda claro quién ha accedido a qué datos personales o datos personales sensibles y con qué fin.

Acuerdos de nivel de servicio

Los SLA deben ser contractuales e integrarse dentro de cualquier oferta de servicio en nube a las organizaciones de EuropeanHealth. La clave será probablemente disponibilidad las 24 horas del día los 7 días de la semana (dependiendo del tipo de servicio, aplicación o datos alojados).

- Una preocupación para las organizaciones de EuropeanHealth será la posible pérdida de control que sufrirán (por ejemplo, de infraestructura, de servicios, de datos y prestación, etc.). La capacidad de los proveedores de servicios en nube de demostrar que no hay pérdidas de control será una consideración clave para la decisión.