Introducción a la seguridad en *cloud computing*

PID_00286168

Jordi Guijarro Olivares

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Jordi Guijarro Olivares

Director de innovación en ciberseguridad en i2CAT (http://www.i2cat.net), el Centro de Investigación en Internet. Ingeniero en Informática por la Universitat Oberta de Catalunya (UOC) y Máster en Gestión de las TIC por la Universidad Ramon Llull (URL). Experto en cloud computing y ciberseguridad, ha participado en proyectos de investigación e innovación de la comisión europea del programa Horizon 2020.

jordi.guijarro@i2cat.net

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Jorba Esteve

Primera edición: febrero 2022

Av. Tibidabo, 39-43, 08035 Barcelona
Autoría: Jordi Guijarro Olivares
Producción: FUOC

Índice

1. Introducción a la seguridad en *cloud computing*

El modelo de servicio TI basado en *cloud* y el constante aumento de las amenazas informáticas implican un cambio en el concepto de seguridad informática en las organizaciones, especialmente en la importancia estratégica que tiene la seguridad en *cloud computing*. Estamos involucrados en una transformación de paradigmas en las tecnologías de la información y comunicación (TIC) en la que la transformación digital basada en modelos *cloud* es la tónica general. El crecimiento del *cloud* incorpora de manera nativa a la web, este crecimiento deriva en grandes retos para la seguridad informática.

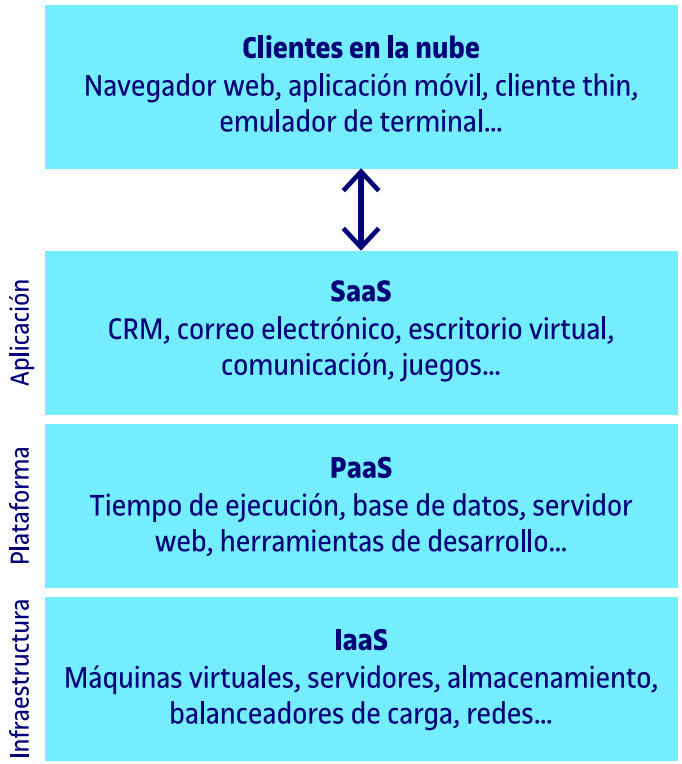
El cibercrimen es desarrollado por organizaciones internacionales que tienen como objetivo perjudicar a empresas y entidades gubernamentales. Por este motivo, las organizaciones necesitan tratar la seguridad en el *cloud* de una manera estructurada. En el momento en el que una organización decide confiar sus datos sensibles, como la información de sus clientes, la organización ha de controlar en todo momento:

- La localización de la información;
- al proveedor y modelo del servicio *cloud*, y
- los niveles de servicio respecto a la integridad y la disponibilidad de los datos.

Además, hay que tener en cuenta el plan de continuidad de negocio, es decir, si este proveedor presenta vulnerabilidades en sus sistemas de seguridad, cuáles serían los potenciales riesgos en el negocio.

La gran mayoría de proveedores de *cloud* aseguran que la seguridad, en última instancia, es responsabilidad del cliente. AWS, RackSpace, Google y otros solo se responsabilizan de sus centros de datos e infraestructura, su seguridad está certificada por las máximas autoridades en la materia. En particular, AWS lo denomina «entorno de responsabilidad compartida». Como usuarios de diferentes servicios *cloud* somos responsables de los datos que alojamos en servidores y bases de datos de los proveedores de *cloud*. Recordemos entonces que la seguridad no solo es importante, sino que debemos trabajar en esta.

Figura 1. Modelos de servicio del *cloud computing*



Los **proveedores de plataforma como servicio (PaaS)** se encargan de la seguridad de la capa de infraestructura y plataforma, mientras que el cliente debe encargarse de la seguridad en la capa de aplicación.

En el caso de los **proveedores infraestructura como servicio (IaaS)** se encargan de la seguridad de la capa de infraestructura, mientras que el cliente debe encargarse de las otras dos.

En la capa de plataforma debemos usar todas las medidas necesarias para mantener nuestros servidores, bases de datos y copias de seguridad accesibles solo a personal autorizado, usando el principio de menor privilegio, otorgando a cada uno el mínimo privilegio necesario para realizar su trabajo.

Los analistas y programadores deben ocuparse de la capa de aplicación, no tiene mucho sentido blindar los datos y servidores si la aplicación permite accesos no legítimos a los datos o a funciones críticas de los servidores.

El *cloud computing* es una revolución en el mundo de las TIC. Posee en su desarrollo una atractiva perspectiva para las organizaciones, grandes o pequeñas, respecto a un mejor aprovechamiento de los recursos internos y a un modelo de gestión optimizado.

Este nuevo modelo ofrece a las organizaciones la posibilidad de tener un foco más claro en sus negocios a partir del momento en el que las tecnologías de la información pasan a ser tratadas como un suministro más de sus cadenas

productivas, y como en todo nuevo concepto el aspecto de la seguridad informática es siempre uno de los puntos más importantes, y que hay que tener en cuenta especialmente en momentos de intensa transformación.

En este apartado dotaremos al estudiante de la visión de los principales riesgos: como la fuga de información o las credenciales comprometidas y la suplantación en la autenticación, así como los principales patrones y la mitigación proactiva de amenazas mediante los procedimientos operativos de seguridad para el control de proveedores.

1.1. Garantías para los clientes en *cloud computing*

Los clientes en la 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. 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.

Ejemplos de riesgos

Algunos ejemplos de los riesgos a los que se enfrentan el cliente y el proveedor son los ataques distribuidos de denegación de servicio (o DDoS).

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 estas garantías.

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

- evaluar el riesgo de utilizar servicios en la nube;
- comparar las ofertas de los distintos proveedores en la nube;
- obtener garantías de los proveedores en la nube seleccionados, y
- reducir la carga del riesgo con respecto a los proveedores en la nube.

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

1.2. Primeras recomendaciones legales

La mayoría de las cuestiones legales asociadas a la computación en nube se suelen 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 a 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.

2. Ámbito, responsabilidades y modelos de seguridad en la nube

Puede sonar simplista, pero la seguridad en la nube y el cumplimiento incluyen todo lo que un equipo de seguridad es responsable hoy en día, solo que en la nube. Todos los dominios de seguridad tradicionales permanecen, pero la naturaleza de los riesgos, roles y responsabilidades, y la implementación de los controles, cambian, a menudo dramáticamente.

Aunque el alcance general de la seguridad y el cumplimiento no cambian, las piezas de las que en particular cualquier actor de la nube es responsable de hacer ciertamente sí cambian. Piénsalo de esta manera: La computación en la nube es un modelo de tecnología compartida donde las diferentes organizaciones son responsables, frecuentemente, de implementar y administrar las diferentes partes de la pila. Como resultado, las responsabilidades de seguridad también se distribuyen en la pila, y por lo tanto a través de las organizaciones involucradas.

Esto se conoce comúnmente como el **modelo de responsabilidad compartida**. Piensa en ello como una matriz de responsabilidad que depende del proveedor de servicios en la nube en particular y la característica/producto, el modelo de servicio y el modelo de implementación.

En un nivel alto, la responsabilidad de seguridad se correlaciona con el grado de control que tiene un actor dado sobre la arquitectura en pila:

- **Software como servicio**. El proveedor de servicios en la nube es responsable de casi toda la seguridad, ya que el usuario de servicios en la nube solo puede acceder y administrar su uso de la aplicación, y no puede alterar el funcionamiento de la aplicación. Por ejemplo, un proveedor de SaaS es responsable de la seguridad del perímetro, el registro/monitoreo/auditoría y la seguridad de la aplicación, mientras que el consumidor solo puede administrar la autorización y los derechos.

- **Plataforma como servicio**. El proveedor de servicios en la nube es responsable de la seguridad de la plataforma, mientras que el consumidor es responsable de todo lo que implementa en la plataforma, incluida la forma en la que configuran las características de seguridad ofrecidas. Las responsabilidades se dividen de manera más pareja. Por ejemplo, cuando se utiliza una base de datos como servicio, el proveedor gestiona la seguridad, los parches y la configuración central, mientras que el usuario de servicios en la nube es responsable de todo lo demás, incluidas las funciones

de seguridad de la base de datos, las cuentas de administración o incluso los métodos de autenticación.

- **Infraestructura como servicio**. Al igual que PaaS, el proveedor es responsable de la seguridad de base, mientras que el usuario de servicios en la nube es responsable de todo lo que construye en la infraestructura. A diferencia de PaaS, esto otorga mucha más responsabilidad al cliente. Por ejemplo, es probable que el proveedor de IaaS controle su perímetro en busca de ataques, pero el consumidor es totalmente responsable de cómo definen e implementan su seguridad de red virtual, según las herramientas disponibles en el servicio.

Figura 2. Modelos de responsabilidad

Estas funciones se complican aún más cuando se utilizan *cloud brokers* u otros intermediarios y socios. La consideración de seguridad más importante es saber exactamente quién es responsable de qué, en cualquier proyecto en la nube. Es menos importante si un proveedor de servicios en la nube en particular ofrece un control de seguridad específico, siempre y cuando sepa exactamente qué ofrecen y cómo funciona. Puede llenar los vacíos con sus propios controles o elegir un proveedor diferente, si no puede cerrar la brecha de controles. Su capacidad para hacer esto es muy alta para IaaS, y menos para SaaS.

Esta es la esencia de la relación de seguridad entre un proveedor de servicios en la nube y el consumidor. ¿Qué hace el proveedor? ¿Qué necesita hacer el consumidor? ¿El proveedor de servicios en la nube permite al consumidor hacer lo que necesita? ¿Qué está garantizado en los contratos y en el acuerdo de nivel de servicio, y qué implica la documentación y los detalles de la tecnología?

Este modelo de responsabilidad compartida se correlaciona directamente con **dos recomendaciones**:

1) Los proveedores de servicios en la nube deben documentar claramente sus controles internos de seguridad y las características de seguridad del cliente para que el usuario de servicios en la nube pueda tomar una decisión informada. Los proveedores también deben diseñar e implementar adecuadamente esos controles.

2) Los usuarios de servicios en la nube deben, para cualquier proyecto dado en la nube, crear una matriz de responsabilidades para documentar quién está implementando qué controles y cómo. Esto también debería alinearse con los estándares de cumplimiento necesarios.

A modo de ejemplo, la Cloud Security Alliance proporciona **dos herramientas** para ayudar a cumplir estos requisitos:

1) El **cuestionario de iniciativa de evaluaciones de consenso (CAIQ)**. Una plantilla estándar para que los proveedores de servicios en la nube documenten sus controles de seguridad y cumplimiento.

2) La **matriz de controles de la nube (CCM)**, que enumera los controles de seguridad en la nube y los mapea en múltiples estándares de seguridad y cumplimiento. La CCM también se puede usar para documentar las responsabilidades de seguridad. Ambos documentos necesitarán ajustes para requisitos específicos de organización y proyecto, pero proporcionan una plantilla de inicio completa y pueden ser especialmente útiles para garantizar que se cumplan los requisitos de cumplimiento.

Enlaces recomendados

Puede consultarse el cuestionario de iniciativa de evaluaciones de consenso (CAIQ) aquí.

Puede consultarse la matriz de controles de la nube (CCM) aquí.

3. Modelos de seguridad en la nube

Los modelos de seguridad en la nube son herramientas para ayudar a orientar las decisiones de seguridad. El término *modelo* se puede utilizar de forma un poco nebulosa, por lo que para nuestros propósitos se descompone en los siguientes **tipos**:

- Los modelos o *frameworks* conceptuales incluyen visualizaciones y descripciones utilizadas para explicar conceptos y principios de seguridad en la nube, como el modelo lógico de CSA.

- Modelos de control o marcos de trabajo que categorizan y detallan controles de seguridad en la nube específicos o categorías de controles, como la CCM de CSA.

- Las arquitecturas de referencia son plantillas para implementar la seguridad en la nube, generalmente generalizadas (por ejemplo, una arquitectura de referencia de seguridad IaaS). Pueden ser muy abstractos, bordeando lo conceptual, o bastante detallados, bajando hasta controles y funciones específicos.

- Los patrones de diseño son soluciones reutilizables para problemas particulares. En seguridad, un ejemplo es la administración de recursos IaaS. Al igual que con las arquitecturas de referencia, pueden ser más o menos abstractas o específicas, incluso bajar hasta patrones de implementación comunes en plataformas de nube particulares.

Las líneas entre estos modelos a menudo se difuminan y se superponen, según los objetivos del desarrollador del modelo. Incluso agruparlos todos juntos bajo el encabezado «modelo» es probablemente inexacto, pero, dado que vemos los términos usados de manera intercambiable en diferentes fuentes, tiene sentido agruparlos.

La Cloud Security Alliance (CSA) ha revisado y recomienda los siguientes **modelos**:

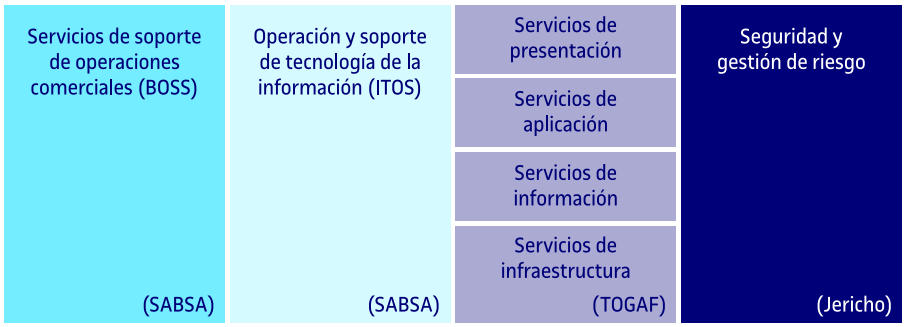
- CSA arquitectura empresarial

- CSA matriz de controles en la nube

- El borrador NIST. La arquitectura de referencia de seguridad de *cloud computing* (NIST Special Publicación 500-299), que incluye modelos conceptuales, arquitecturas de referencia y un marco de control.

- ISO/IEC FDIS 27017. Tecnología de la información, técnicas de seguridad y código de práctica para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.

Figura 3. *Frameworks* de referencia



4. Un modelo simple de proceso de seguridad en la nube

Si bien los detalles de implementación, controles necesarios, procesos específicos y varias arquitecturas de referencia y modelos de diseño varían mucho según el proyecto específico de la nube, existe un **proceso** relativamente sencillo y de alto nivel para administrar la seguridad en la nube:

- identificar los requisitos de seguridad y cumplimiento necesarios y cualquier control existente;
- seleccionar al proveedor de servicios en la nube, servicio y modelos de implementación;
- definir la arquitectura;
- evaluar los controles de seguridad;
- conocer las lagunas de control;
- diseñar e implementar controles para llenar los vacíos, y
- gestionar cambios a lo largo del tiempo.

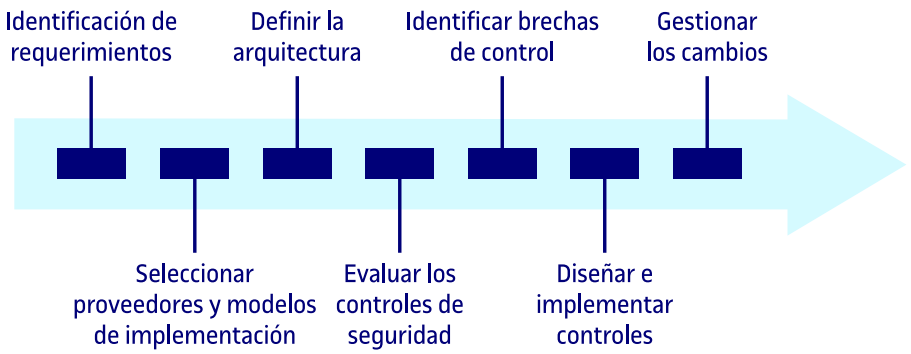
Dado que los diferentes proyectos en la nube, incluso en un solo proveedor, probablemente aprovecharán conjuntos de configuraciones y tecnologías completamente diferentes, cada proyecto debe evaluarse por sus propios méritos.

Evaluación por propios méritos

Por ejemplo, los controles de seguridad para una aplicación implementada en IaaS puro en un proveedor pueden parecer muy diferentes de un proyecto similar que en su lugar usa más PaaS de ese mismo proveedor.

La clave es identificar los requisitos, diseñar la arquitectura e identificar los vacíos en función de las capacidades de la plataforma subyacente de la nube. Es por eso por lo que necesita conocer la arquitectura y el proveedor de servicios en la nube antes de comenzar a traducir los requisitos de seguridad en controles.

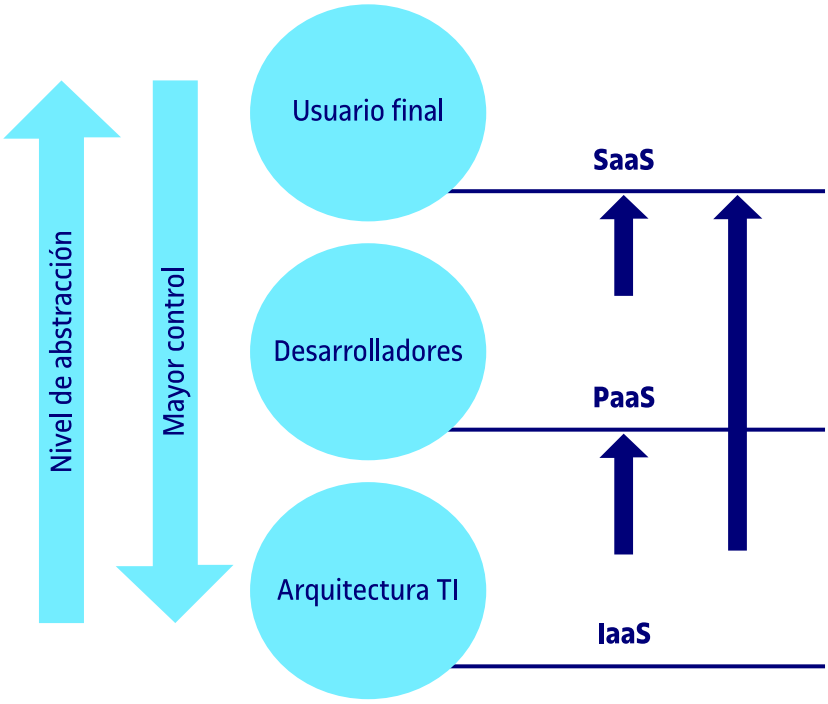
Figura 4. Fases en la adopción



5. Principales riesgos, patrones y mitigación proactiva de amenazas

La naturaleza compartida en los catálogos de servicios en el campo de la computación en la nube introduce la aparición de nuevas brechas de seguridad que pueden amenazar los beneficios obtenidos en el cambio hacia tecnologías basadas en la nube. Organizaciones como la CSA advierten de que es importante considerar que los servicios en la nube por naturaleza permiten a los usuarios omitir las políticas de seguridad de toda la organización utilizando servicios externos. A este fenómeno se le denomina «Shadow IT». De aquí que sea importante establecer nuevos controles para la detección, el control y la concienciación de los riesgos de esta nueva situación.

Figura 5. Modelos y áreas en el cloud computing



En términos generales, en función del tipo de servicio contratado, según va incrementándose el nivel de abstracción disminuye el control que el cliente tiene sobre la infraestructura. Del mismo modo, cuanto mayor control tiene la organización cliente sobre la infraestructura que proporciona el servicio, mayor nivel de seguridad y control puede aplicar sobre esta y, por tanto, sobre la información tratada.

5.1. Amenaza n.º 1: fuga de información

Los entornos en la nube se enfrentan a muchas de las amenazas que ya encontramos en las redes corporativas tradicionales, pero estas se acentúan debido a la gran cantidad de datos almacenados en servidores en la nube y los proveedores se convierten en un objetivo más atractivo. Si hablamos de datos/información, es muy importante tener en cuenta que la gravedad del daño depende en gran medida de la sensibilidad de los datos expuestos. La información financiera expuesta tiende a salir en los titulares de prensa generalista, pero las infracciones que involucran información de salud, secretos comerciales y propiedad intelectual son las más devastadoras.

Cuando ocurre una fuga de datos, las empresas pueden incurrir en multas, o pueden enfrentarse a demandas o incluso a cargos criminales. También se ha de considerar aspectos como las investigaciones de la infracción y las propias notificaciones hacia los clientes que por daños de imagen pueden añadir costes muy significativos. Efectos indirectos, como daños a la marca y la pérdida de negocio, pueden afectar a las organizaciones durante diversos años.

Al final, los proveedores de nube implementan controles de seguridad para proteger sus entornos, pero cabe recordar que, en última instancia, las organizaciones son responsables de proteger sus propios datos dentro de la organización y también en la nube. Es más que recomendable que las organizaciones utilicen mecanismos como la autenticación multifactor y el cifrado de datos para protegerse contra las fugas de información.

5.2. Amenaza n.º 2: credenciales comprometidas y suplantación en la autenticación

Las brechas de datos y otros ataques frecuentemente resultan de un sistema de autenticación «pobre», como permitir contraseñas débiles y una mala administración de claves o certificados. Las organizaciones a menudo luchan con la gestión de identidades a medida que tratan de asignar permisos adecuados a la función de trabajo del usuario. Pero, en algunas ocasiones, la falta de gestión correcta de las bajas provoca que estas no sean efectivas en el momento en el que la función de trabajo cambia o el propio usuario abandona la organización.

Los sistemas de autenticación multifactor, como las contraseñas de un solo uso, la autenticación mediante dispositivos móviles y las tarjetas inteligentes, protegen los servicios en la nube porque dificultan que los atacantes inicien sesión con contraseñas robadas. Existen multitud de ejemplos de organizaciones y servicios de internet, muy conocidos, que han expuesto millones de registros de clientes o usuarios, como resultado de credenciales de usuario robadas. En la mayoría de los casos asociado a fallos en el despliegue de un pro-

ceso de autenticación de tipo multifactor, así que una vez que los atacantes obtienen las credenciales, solo cabe esperar que el proceso que se encarga a la respuesta a incidentes sea efectivo.

Muchos desarrolladores cometen el error de incrustar credenciales y claves criptográficas en el código fuente y dejarlas en repositorios orientados al público como GitHub. Las claves necesitan estar adecuadamente protegidas, y una infraestructura de clave pública bien asegurada es necesaria. También necesitan ser rotados periódicamente para que sea más difícil para los atacantes utilizar claves que han obtenido sin autorización.

Las organizaciones que planean federar la identidad con un proveedor de la nube necesitan entender las medidas de seguridad que el proveedor utiliza para proteger la plataforma de identidad. Centralizar la identidad en un solo repositorio tiene sus riesgos y en cada caso se ha de valorar muy bien la protección y salvaguardas asociadas.

5.3. Amenaza n.º 3: interfaces y API hackeadas

Prácticamente, todos los servicios y aplicaciones en la nube ahora ofrecen API para facilitar tareas de automatización e interoperabilidad. Los equipos de TI utilizan interfaces y API para gestionar e interactuar con servicios en la nube, incluidos aquellos que ofrecen aprovisionamiento en autoservicio, gestión remota, orquestación, monitorización y supervisión en la nube.

La seguridad y la disponibilidad de los servicios en la nube, desde la autenticación y el control de acceso hasta el cifrado y el monitoreo de actividades, dependen de la seguridad de la API. El riesgo aumenta con terceros que dependen de las API y se basan en estas interfaces, ya que las organizaciones pueden necesitar exponer más servicios y credenciales. Las interfaces débiles y las API exponen a las organizaciones a cuestiones de seguridad relacionadas con la confidencialidad, la integridad, la disponibilidad y la rendición de cuentas.

Las API y las interfaces tienden a ser la parte más expuesta de un sistema porque normalmente son accesibles desde internet. Se recomiendan controles adecuados como la «primera línea de defensa y detección». Las aplicaciones y los sistemas de modelado de amenazas, incluidos los flujos de datos y la arquitectura/diseño, se convierten en partes importantes del ciclo de vida del desarrollo. También se recomienda revisiones de código enfocadas a la seguridad y rigurosas pruebas de penetración.

5.4. Amenaza n.º 4: vulnerabilidades

Las vulnerabilidades del sistema, o *bugs* explotables en los programas, no son nuevas, pero se han convertido en un problema mayor con la acentuación de los sistemas de información *multitenant* en el modelo de *cloud computing*. Las organizaciones comparten memoria, bases de datos y otros recursos en estrecha proximidad entre sí, creando nuevas superficies de ataque.

Afortunadamente, los ataques a las vulnerabilidades del sistema pueden ser mitigados con «procesos de TI básicos». Las mejores prácticas incluyen la exploración regular de vulnerabilidades, la administración rápida de parches y un rápido seguimiento de las amenazas informadas.

Es importante considerar que los costes de mitigar las vulnerabilidades del sistema «son relativamente pequeños en comparación con otros gastos de TI». El coste de poner los procesos de TI en el lugar que le corresponde, con el objetivo de controlar, detectar y reparar vulnerabilidades, es pequeño en comparación con el daño potencial. Las organizaciones necesitan parchar lo más rápido posible, preferiblemente como parte de un proceso automatizado y recurrente. Los procesos de control de cambios que tratan los parches de emergencia aseguran que las actividades relacionadas con el mantenimiento del software estén debidamente documentadas y revisadas por los equipos técnicos.

5.5. Amenaza n.º 5: secuestro de cuentas

La pesca electrónica (*phishing*), el fraude y las explotaciones de código siguen teniendo éxito, y los servicios en la nube agregan una nueva dimensión a la amenaza, debido a que los atacantes pueden interceptar actividad, manipular transacciones y modificar datos. A esto se ha de añadir que los atacantes también pueden utilizar la aplicación en la nube para lanzar otros ataques de manera encadenada.

Las estrategias más comunes en la defensa en profundidad pueden contener los daños ocasionados por una infracción. Las organizaciones deben prohibir el intercambio de credenciales de cuenta entre usuarios y servicios, así como habilitar sistemas de autenticación multifactor cuando estén disponibles. Las cuentas, incluso las de servicio, deben ser monitorizadas para que cada transacción pueda ser rastreada e identificar a un usuario unipersonal si fuere necesario. Una parte de la estrategia es proteger las credenciales de las cuentas de usuario para evitar que estas sean robadas.

5.6. Amenaza n.º 6: intrusos maliciosos

Esta amenaza tiene muchas caras: un empleado o un antiguo empleado, un administrador de sistemas, un cliente o incluso un *partner*. La actividad maliciosa puede venir motivada desde el robo de datos hasta la venganza. En un escenario en la nube, un actor privilegiado puede destruir infraestructuras en-

teras o manipular datos. Los sistemas que dependen únicamente de un proveedor de servicios en la nube, como podrían ser los de cifrado, corren sin duda un mayor riesgo.

Se recomienda que sean las propias organizaciones las que controlen el proceso de cifrado y las claves, segregando las tareas y minimizando el acceso dado a los usuarios. Las actividades de registro, monitorización y auditoría de los propios administradores también son consideradas hoy como críticas.

En entornos de *cloud computing*, es fácil interpretar erróneamente un intento de ataque por parte de un proceso rutinario como actividad «malintencionada» sobre información privilegiada. Un ejemplo sería un administrador que copia accidentalmente una base de datos confidencial de clientes en un servidor accesible públicamente. La formación y la prevención para prevenir tales errores se vuelven aspectos más críticos en la nube, debido a una mayor exposición de los sistemas y servicios.

5.7. Amenaza n.º 7: el parásito APT

La CSA llama acertadamente a las amenazas persistentes avanzadas (APT, por sus siglas en inglés) formas «parásitas» de ataque. Las APT se infiltran en los sistemas para establecerse en un punto de apoyo, y luego exfolian furtivamente los datos y la propiedad intelectual durante un periodo prolongado de tiempo.

Normalmente, las APT se mueven lateralmente a través de la red y se mezclan con el tráfico normal, por lo que son difíciles de detectar. Los principales proveedores de nube aplican técnicas avanzadas para evitar que las APT se infiltren en su infraestructura, pero los clientes deben ser tan diligentes en la detección de compromisos APT en las cuentas de la nube como lo harían en sus sistemas locales.

Entre los puntos de entrada comunes se incluyen la pesca electrónica, los ataques directos, unidades USB precargadas con un programa maligno y redes de terceros comprometidas. En particular, se recomienda entrenar a los usuarios para que reconozcan las técnicas de pesca electrónica o *phishing*.

Los programas de concienciación mantienen a los usuarios en alerta y son menos propensos a ser engañados para que una APT ingrese en la red, además de que los departamentos de TI deben mantenerse informados de los últimos ataques avanzados. Los controles de seguridad avanzados, la gestión de procesos, los planes de respuesta a incidentes y la capacitación del personal de TI conducen a mayores presupuestos de seguridad. Las organizaciones deben sopesar estos costes frente al posible daño económico infligido por los ataques exitosos de APT.

5.8. Amenaza n.º 8: pérdida permanente de datos

A medida que la nube se ha madurado, los informes de pérdida permanente de datos debido al error del proveedor se han vuelto extremadamente raros. Sin embargo, se sabe que los *hackers* maliciosos eliminan de forma permanente los datos de la nube para dañar a las empresas, y los centros de datos en la nube son tan vulnerables a desastres naturales como cualquier instalación.

Los proveedores de nube recomiendan distribuir datos y aplicaciones mediante múltiples zonas para una mayor protección. Las medidas adecuadas de respaldo de datos son esenciales, así como la adhesión a las mejores prácticas en la continuidad del negocio y la recuperación de desastres. La copia de seguridad diaria de datos y el almacenamiento fuera de sitio siguen siendo importantes para los entornos en la nube.

La carga de evitar la pérdida de datos no es todo en el proveedor de servicios en la nube. Si un cliente cifra datos antes de subirlos a la nube, entonces ese cliente debe tener cuidado de proteger la clave de cifrado. Una vez que se pierde la clave, también se pierden los datos.

Las políticas de cumplimiento a menudo estipulan cuánto tiempo las organizaciones deben conservar los registros de auditoría y otros documentos. La pérdida de estos datos puede tener graves consecuencias regulatorias. Las nuevas normas de protección de datos de la UE también tratan la destrucción de datos y la corrupción de datos personales como infracciones de datos que requieren una notificación adecuada. Conozca las reglas para evitar problemas.

5.9. Amenaza n.º 9: inadecuada diligencia

Las organizaciones que abrazan la nube sin entender completamente el entorno y sus riesgos asociados pueden encontrarse con un «incremento de riesgos comerciales, financieros, técnicos, legales y de cumplimiento». El grado del riesgo depende de si la organización está intentando migrar a la nube o fusionarse (o trabajar) con otra compañía en la nube. Por ejemplo, las organizaciones que no examinan un contrato de servicio pueden no ser conscientes de la responsabilidad del proveedor en caso de pérdida de datos o algún tipo de incumplimiento.

Los problemas operacionales y de arquitectura surgen si el equipo de desarrollo de una empresa carece de familiaridad con las tecnologías en la nube, ya que las aplicaciones se despliegan en una nube en particular y no son habituales hoy en día los modelos híbridos o de tipo *multicloud*.

5.10. Amenaza n.º 10: abusos de los servicios en la nube

Los servicios en la nube pueden ser utilizados para apoyar actividades ilegales, como el uso de recursos de computación en la nube para romper una clave de cifrado y lanzar un ataque. Otros ejemplos incluyen el lanzamiento de ataques DDoS, el envío de correos electrónicos de *spam* y *phishing*, y el alojamiento de contenido malicioso.

Los proveedores deben reconocer estos tipos de abuso –como el análisis del tráfico para reconocer los ataques DDoS– y ofrecer herramientas para que los clientes puedan supervisar la salud de sus entornos *cloud*. Los clientes deben asegurarse de que los proveedores ofrezcan un mecanismo para notificar el abuso. Aunque los clientes no pueden ser víctimas directas de acciones maliciosas, el abuso en el servicio en la nube puede resultar en problemas de disponibilidad de servicios y pérdida de datos.

5.11. Amenaza n.º 11: ataques DoS

Los ataques DoS han existido durante años, pero han ganado prominencia gracias a la computación en la nube, ya que a menudo afectan de manera destacada a la disponibilidad. Los sistemas pueden ralentizarse o estar fuera de juego.

> «Experimentar un ataque de denegación de servicio es como estar atrapado en un atasco de tráfico de hora punta; hay una manera de llegar a su destino y no hay nada que pueda hacer al respecto, excepto sentarse y esperar».

Los ataques de DoS consumen grandes cantidades de procesamiento, una factura que el cliente puede finalmente tener que pagar. Aunque los ataques DDoS de gran volumen no son muy comunes, las organizaciones deben ser conscientes de los ataques asimétricos a nivel de aplicación de DoS, que se dirigen a vulnerabilidades de servidor web y otros componentes críticos como las bases de datos.

La norma habitual es que los proveedores de nube tiendan a estar mejor preparados para manejar ataques de DoS que sus clientes. La clave es tener un plan para mitigar el ataque antes de que ocurra, por lo que los administradores tienen acceso a esos recursos cuando los necesitan.

5.12. Amenaza n.º 12: tecnología compartida, peligros compartidos

Las vulnerabilidades en la tecnología compartida suponen una amenaza significativa para la computación en la nube. Los proveedores de servicios en la nube comparten infraestructura, plataformas y aplicaciones, y si surge una

vulnerabilidad en cualquiera de estas capas, afecta a todos. «Una sola vulnerabilidad o mala configuración puede llevar a un compromiso a través de la nube de un proveedor entero».

Si un componente se ve comprometido –digamos, un hipervisor, un componente de plataforma compartida o una aplicación–, expone todo el entorno a un posible compromiso y violación. En definitiva, es más que recomendable una estrategia de defensa en profundidad, incluyendo la autenticación multifactor en todos los *hosts*, sistemas de detección de intrusos basados tanto a nivel de *host* como en red, aplicando el concepto de privilegios mínimos, segmentación de red y parche de recursos compartidos.

6. Control de proveedores. Procedimientos operativos de seguridad

Algunas operaciones del servicio deben ser realizadas de forma conjunta por ambas partes: contratada y contratante, debiendo establecerse los roles, las responsabilidades (capacidad de autorizar y obligación de rendir cuentas) y los protocolos adecuados para llevarlas a cabo.

Cabe destacar las siguientes **actividades**, sin que sean las únicas que procedimentar:

- Mantenimiento y gestión de cambios
- Gestión de incidentes
- Continuidad - recuperación de desastres
- Gestión del personal
- Configuración de seguridad
- Recuperación de datos de copias de seguridad

6.1. Seguimiento del servicio

En los servicios prestados por terceros a la organización, tan importante es el acuerdo contractual con el proveedor de servicios como el seguimiento que hay que realizar del servicio prestado. Para poder tener el control de los servicios, y por tanto también poder exigirle al proveedor el cumplimiento de cualesquiera medidas de seguridad aplicables, es necesaria una **monitorización** de estos.

- La medición del cumplimiento del servicio y el procedimiento para restaurar las desviaciones estipuladas contractualmente.
- El proceso de coordinación para el mantenimiento de los sistemas implicados.
- El proceso de coordinación ante incidentes o desastres.

En cuanto al primer aspecto, y dadas las características de la prestación de servicios en la nube, en ocasiones con aspectos relevantes fuera del control de la organización cliente y también dada su forma de pago, en función del uso, es muy importante reflejar de un modo claro los términos del cumplimiento. Es necesario identificar en el contrato los derechos de la organización cliente para poder monitorizar el funcionamiento del servicio y de este modo comprobar el cumplimiento de las medidas de seguridad, los controles y las políticas que garantizan la integridad, confidencialidad y disponibilidad de los datos, y del

mismo modo poder realizar la comprobación de que el nivel de prestación es el pactado. La definición y el control de los SLA son vitales para poder garantizar el cumplimiento de lo estipulado en el contrato.

La organización debe monitorizar de forma independiente el cumplimiento de los términos establecidos en el contrato, bien a través de controles técnicos propios, bien a través de la revisión y aprobación periódica de los informes de servicio proporcionados por el CSP.

Es necesario ejecutar esta monitorización sobre al menos los siguientes **controles de seguridad y servicio** con independencia de la categoría del sistema:

- Niveles de calidad, disponibilidad y capacidad del servicio ofrecido, incluyendo el cumplimiento de las obligaciones de servicio acordadas y la respuesta ofrecida por el proveedor ante desviaciones significativas.

- Gestión de incidentes de seguridad, incluyendo toda la información necesaria para determinar orígenes, objetivos, riesgos, etc., asociados a cualquier incidente relevante.

- Controles de acceso a los servicios, incluyendo un listado actualizado de usuarios autorizados para utilizar los servicios disponibles, y los privilegios asociados en cada caso.

- Cumplimiento normativo y legislativo entre el prestador y el cliente de los servicios, incluyendo los aspectos de cumplimiento de aplicación sobre el prestador que correspondan en cada caso, como auditorías LOPD, ISO, financieras, etc.

- Situación actualizada de las medidas de protección de la información establecidas por el proveedor, incluyendo aspectos de seguridad física, protección contra software malicioso, seguridad del personal, copias de seguridad, etc.

- Mecanismos de comprobación regular de los controles de seguridad por parte del proveedor y resultados de dichas comprobaciones.

Toda la información de los controles anteriores proporcionada periódicamente por el proveedor de servicios debe incluir de forma obligatoria cualesquiera anomalías o desviaciones significativas producidas durante el periodo, así como las acciones ejecutadas en cada caso como respuesta a estas situaciones susceptibles de introducir riesgos en la organización. Adicionalmente, debemos solicitar al proveedor de servicios la información de auditoría y no conformidades de aplicación en cada caso, para poder verificar que las medidas de seguridad tomadas por este son las correctas y oportunas para solventar desviaciones halladas durante el proceso de auditoría.

6.2. Gestión de cambios

Otro aspecto que tratar en la gestión diaria del servicio es el referente a la **gestión y coordinación del mantenimiento de los sistemas**. En este sentido, se deberá establecer contractualmente de acuerdo con los requisitos mínimos de normativas, como el Esquema Nacional de Seguridad (ENS), la obligación de mantener actualizados los sistemas para garantizar su correcto funcionamiento, así como eliminar las posibles vulnerabilidades que pueden afectar a los sistemas.

Deberá definirse un procedimiento de coordinación en el mantenimiento de sistemas entre ambas partes para prevenir paradas o errores en la prestación del servicio; este procedimiento estará en línea con el proceso de gestión de cambio e incluirá la notificación con suficiente antelación de la realización de mantenimientos por parte del proveedor, identificando los tiempos en los que puede interrumpirse el servicio. La notificación se realizará previa y posteriormente al mantenimiento y tras este se pedirá al cliente conformidad del correcto funcionamiento del servicio.

Por otra parte, siempre que el mantenimiento o actualización implique un cambio mayor o pueda suponer el funcionamiento incorrecto de los sistemas de la organización cliente, el proveedor habilitará previamente un entorno actualizado para que el cliente pueda verificar el correcto funcionamiento de sus sistemas en preproducción. Además, el proveedor deberá informar periódicamente de los mantenimientos y las actualizaciones realizados en los sistemas que albergan los sistemas del cliente.

6.3. Gestión de incidentes

De acuerdo con normativas vigentes y buenas prácticas, el proveedor deberá disponer de un **procedimiento de gestión de incidentes**. Se deberá informar a la organización cliente de:

- El procedimiento de notificación de incidentes.
- La tipología de incidentes incluidos en el servicio.
- Los procedimientos específicos ante incidentes de seguridad.
- Los tiempos de respuesta y resolución de incidentes.
- El mantenimiento y gestión del registro de incidentes.

Deberá definirse un procedimiento de coordinación ante incidentes que puedan afectar a los sistemas del cliente, procedimiento que deberá contemplar los flujos de información y las interacciones entre cliente y proveedor durante la gestión del incidente. A su vez, el proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan los sistemas del cliente.

En los niveles de servicio, en el caso de incidentes que afecten a la información o a los servicios del organismo contratante, el proveedor deberá facilitar toda la información forense necesaria para analizar el incidente y su gestión.

6.4. Respaldo y recuperación de datos

El proveedor deberá disponer de **un procedimiento de copias de respaldo** que garantice la restauración de la información como describe [mp.info.9]. El proveedor deberá informar a la organización cliente de:

- la política de copias de seguridad;
- las medidas de cifrado de información en respaldo;
- el procedimiento de solicitud de restauraciones de respaldo;
- la realización de pruebas de restauración;
- el alcance de los respaldos, y
- el traslado de copias de seguridad (si aplica).

6.5. Continuidad del servicio

De acuerdo con normativas como el Esquema Nacional de Seguridad (ENS) o normas como la ISO27001, los sistemas afectados deberán disponer de **medidas para la continuidad del servicio**. Si bien los niveles de disponibilidad, así como los tiempos de recuperación en la prestación de servicios, se encuentran recogidos contractualmente en los SLA, se deberá solicitar al proveedor evidencia de la existencia de un plan de continuidad de negocio que garantice la restauración de los servicios. El proveedor deberá informar a la organización cliente de:

- la existencia de un plan de continuidad de negocio;
- la evidencia satisfactoria de la ejecución periódica de pruebas de continuidad, y
- el análisis de impacto del servicio proporcionado.

Donde se considerarán los siguientes **aspectos** en función del nivel de disponibilidad requerido:

- Se deberá requerir al proveedor evidencia de la existencia de un plan de continuidad de negocio cuyo alcance incluya los servicios objeto de la prestación.

- Se exigirá constancia de que los tiempos de recuperación identificados en el análisis de impacto están alineados con los criterios definidos en los SLA, en cuanto a tiempo de recuperación del servicio.

- Deberá definirse un procedimiento de coordinación ante incidentes y desastres que puedan afectar a los sistemas del cliente, procedimiento que deberá contemplar los flujos de información y las interacciones entre

cliente y proveedor durante la gestión tanto de incidentes como de desastres.

- A su vez el proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan los sistemas del cliente.

- Se realizarán pruebas periódicas que involucren al organismo y a los diferentes proveedores y subproveedores para validar el correcto funcionamiento de los planes y el cumplimiento de los plazos y servicios mínimos previstos.

6.6. Finalización del servicio

Salvo cuando la parte contratante disponga de una copia actualizada de su información, se deberán establecer los **procedimientos para que la parte contratante recupere la información entregada al proveedor**. En estos procedimientos se deben acotar formatos de datos y tiempos.

Salvo cuando la parte contratante no haya transferido información en claro al proveedor, se deberán establecer **procedimientos para la eliminación de las copias en los equipos del proveedor**. Estos procedimientos deben incluir los mecanismos de borrado y las garantías de que han sido aplicados correctamente. Los tiempos de destrucción de la información deberán tener en cuenta los requisitos legales de retención, si los hubiera.

Los procedimientos anteriores deben tener en el proveedor la parte correspondiente para prolongarlos a posibles terceros proveedores subcontratados.

7. Supervisión y auditoría

La organización cliente, como responsable última de los posibles riesgos que afecten tanto a la información como a los servicios prestados, deberá disponer de un determinado nivel de control sobre tales servicios. En este sentido, y para garantizar el cumplimiento de las medidas de seguridad de aplicación en cada caso, la organización deberá **evaluar la conveniencia de disponer del derecho de auditoría**, con la profundidad correspondiente, sobre el proveedor de servicios o de solicitar a este la siguiente documentación:

- Una declaración de aplicabilidad de las medidas que deben aplicarse.
- Una auditoría que verifique mediante evidencias el cumplimiento de las medidas de seguridad que sean de aplicación de acuerdo con el nivel del sistema.
- Auditorías de cumplimiento de normativa necesaria para satisfacer los requisitos de seguridad de la información del organismo contratante. Por ejemplo, GDPR, SAS70, PCI-DSS, etc.

El proveedor puede disponer de certificaciones o acreditaciones en materia de seguridad. Estas certificaciones pueden simplificar la auditoría completa del servicio prestado, en su condición de evidencias de cumplimiento que debe valorar el equipo auditor.

Ejemplos de certificaciones o acreditaciones

- Auditorías recomendadas por ENISA para proveedores de servicios en la nube [ENISA-CCSL].
- Sistema de gestión de la seguridad de la información (SGSI) [ISO/IEC 27001:2013].
- Sistema de gestión de la continuidad [ISO 22301:2012].
- *Cloud Controls Matrix* [CCM].

Tabla 1. Control de medidas de seguridad basadas en la norma ISO 27001 y Cloud Control Matrix (CSA)

Medidas de seguridad		**ISO 2700**			**CCM**	
org	Marco organizativo	nivel	2005	2013	nivel	v3
org. 1	Política de seguridad	1	27001: • 4.2.1 • 5.1 27002: • 5.1.1 • 5.1.2 • 6.1.2 • 6.1.3 • 15.1.1	27001: • 4 • 5.2 • 5.3 27002: • 6.1.1 • 18.1.1	1	GRM-05 GRM-09

8. Recomendaciones

He aquí algunas recomendaciones finales:

- Comprender las diferencias entre la computación en la nube y la infraestructura tradicional o la virtualización, y cómo la abstracción y la automatización afectan a la seguridad.

- Familiarizarse con el modelo NIST para computación en la nube y la arquitectura de referencia CSA.

- Usar herramientas tales como el cuestionario de la iniciativa de evaluaciones de consenso de CSA (CAIQ) para evaluar y comparar proveedores de servicios en la nube.

- Los proveedores de servicios en la nube deben documentar claramente sus características y controles de seguridad y publicarlos utilizando herramientas como CSA CAIQ.

- Usar herramientas como la matriz de controles de nube de CSA para evaluar y documentar los requisitos y controles de cumplimiento y seguridad del proyecto en la nube, así como quién es responsable de cada uno.

- Usar un modelo de proceso de seguridad en la nube para seleccionar a proveedores y arquitecturas de diseño, identificar brechas de control e implementar controles de seguridad y cumplimiento.

9. Caso de uso: COVID-19 y *cloud computing*

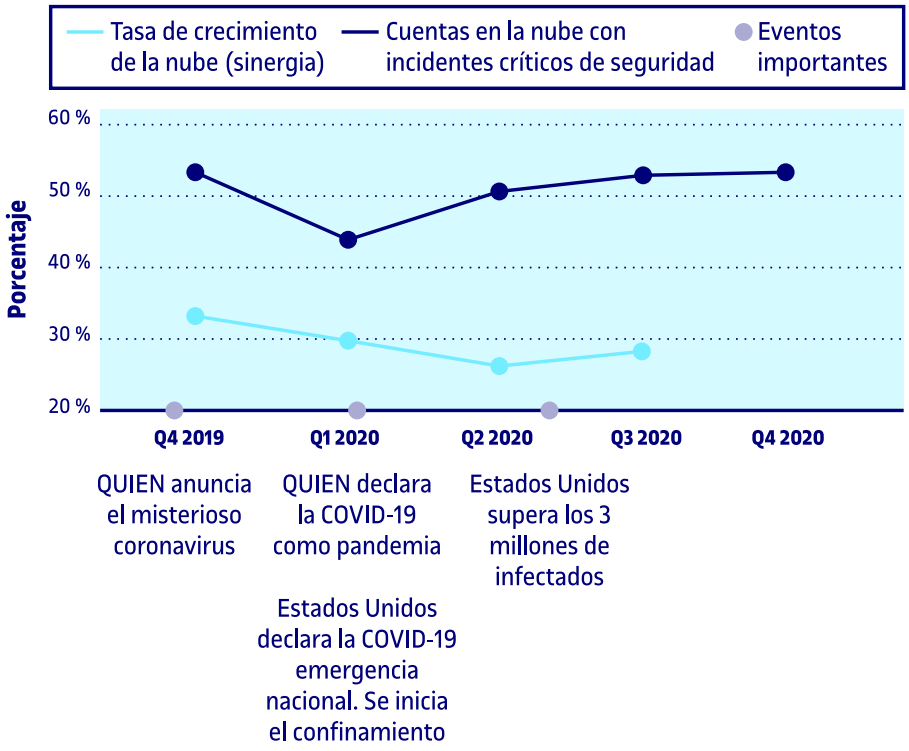
En los primeros días de la pandemia de COVID-19, hubo un rápido aumento en la demanda de servicios en la nube. En cuestión de meses, el porcentaje de empleados que trabajan de forma remota saltó del 20 al 71 %. Además, las empresas escalaron rápidamente su gasto en la nube en el tercer trimestre de 2020 (julio-septiembre), un aumento del 28 % con respecto al mismo trimestre de 2019. El momento es significativo porque la Organización Mundial de la Salud (OMS) declaró la COVID-19 una pandemia en marzo de 2020. En el tercer trimestre de 2020, el trabajo remoto aumentó y las organizaciones aceleraron planes de migración a la nube, de manera que se experimentó un aumento masivo año tras año.

Basándose en un estudio de la Unit42 de Paloalto Networks y utilizando datos extraídos de su gama global de sensores, los investigadores de amenazas en la nube encontraron una correlación entre el aumento del gasto en la nube debido a la COVID-19 y los incidentes de seguridad.

Organizaciones a nivel mundial aumentaron sus cargas de trabajo en la nube en más del 20 % (entre diciembre de 2019 y junio de 2020), lo que implicó una explosión de incidentes de seguridad. La investigación muestra que los programas de seguridad en la nube para organizaciones a nivel mundial todavía están en pañales cuando se trata de automatizar los controles de seguridad (es decir, DevSecOps). Todo esto nos lleva a la conclusión de que el rápido escalado y la complejidad de la nube sin una seguridad automatizada son una combinación con un riesgo multiplicador, siendo más que necesario disponer de controles integrados en todo el proceso de desarrollo.

Es importante tener en cuenta que en investigaciones anteriores encontraron que el 65 % de los incidentes de seguridad divulgados públicamente en la nube fueron el resultado de configuraciones incorrectas del cliente.

Figura 6. Crecimiento de la nube e incidentes de seguridad



Enlace recomendado

Se puede consultar el estudio *Unit 42 Cloud Threat Report, 1H 2021. COVID-19's global impact on security posture* aquí.

Bibliografía

Beck, Kent y otros (2001, febrero). *Manifesto for Agile Software Development* [en línea]. http://agilemanifesto.org

Cunningham, Ward (1992, 26 de marzo). «The WyCash Portfolio Management System».

Guijarro Olivares, Jordi; Caparrós, Joan; Cubero, Lorenzo (2019). *Devops y Seguridad Cloud*. Barcelona: UOC.

Marick, Brian (2003, 22 de agosto). *Agile testing directions: tests and examples* [en línea]. http://www.exampler.com/old-blog/2003/08/22/http://www.exampler.com/old-blog/2003/08/22/

Enlaces recomendados

Additional bookmark (Government of Canada)

CSA - CCSK

DevSecOps: la evolución de la seguridad del software

EUCS - Cloud Services Scheme