GUÍA DE SEGURIDAD

DE ÁREAS CRÍTICAS PARA LA COMPUTACIÓN EN LA NUBE v4.0

CSA ES cloud security alliance® Spain Chapter

CSA AR cloud security alliance® Argentina Chapter

CSA PE cloud security alliance® Peru Chapter

CSA CL cloud security alliance® Chile Chapter

Versión Preliminar

CSA cloud security alliance®

La ubicación permanente y oficial de la versión 4 de la “Guía de Seguridad de Áreas Críticas para la Computación en la Nube” de Cloud Security Alliance está en https://cloudsecurityalliance.org/download/securityguidance-v4/.

Guía Oficial de Estudio para el CCSK Certificate of Cloud Security Knowledge

Contenido

PROLOGO

Bienvenido a la cuarta versión de la *Guía de Seguridad de Áreas Críticas para la Computación en la Nube* de Cloud Security Alliance (CSA). El aumento de la computación en la nube como una tecnología en constante evolución trae consigo una serie de oportunidades y desafíos. Con este documento, nuestro objetivo es proporcionar tanto orientación como inspiración para respaldar los objetivos comerciales, mientras se gestionan y mitigan los riesgos asociados con la adopción de la tecnología de computación en la nube.

Cloud Security Alliance promueve la implementación de buenas prácticas para proporcionar seguridad en el ámbito de la computación en la nube y ha elaborado una hoja de ruta práctica y ejecutable para organizaciones que buscan adoptar el paradigma de la nube. La cuarta versión de la *Guía de Seguridad de Áreas Críticas para la Computación en la Nube* se basa en iteraciones previas de la guía de seguridad, en investigación dedicada y participación pública de los miembros de Cloud Security Alliance, grupos de trabajo y expertos de la industria dentro de nuestra comunidad. Esta versión incorpora avances en la nube, seguridad y tecnologías de soporte; refleja las prácticas de seguridad en la nube del mundo real; integra los últimos proyectos de investigación de Cloud Security Alliance; y ofrece orientación para tecnologías relacionadas.

El avance hacia la computación en la nube segura requiere la participación activa de un amplio conjunto de partes interesadas distribuidas a nivel mundial. CSA reúne a esta comunidad diversa de asociaciones industriales, capítulos internacionales, grupos de trabajo e individuos. Estamos profundamente agradecidos a todos los que contribuyeron a este lanzamiento.

Por favor visite cloudsecurityalliance.com si está interesado en trabajar con nosotros en identificar y promover las mejores prácticas para garantizar un entorno de computación en la nube seguro.

Atentamente,

Luciano (J.R.) Santos
Vicepresidente Ejecutivo de Investigación
Cloud Security Alliance

AGRADECIMIENTOS

De la traducción al Castellano:

Realizada por los siguientes capítulos del CSA:

CSA-ES: Capítulo Español del CSA: http://www.ismsforum.es/csa
CSA-CH: Capítulo Chileno del CSA: https://www.linkedin.com/groups/3350633/profile
CSA-PE: Capítulo Peruano del CSA: https://www.linkedin.com/groups/3720349/profile
CSA-AR: Capítulo Argentino del CSA: https://chapters.cloudsecurityalliance.org/argentina/

Editores / revisores de la edición en Castellano:

Mariano J. Benito, GMV
Ricardo Urbina, CSA Capítulo Chileno
Jorge Laredo, HPE
Diego Bueno, CSA Capítulo España

Equipo de traducción de la edición en Castellano:

Antonio Sanz, S2 Grupo
Fernando Iglesias, CSA Capítulo España
María Jesús Casado, CSA Capítulo España
Alexei Morales, CSA Capítulo Chile
Carlos Samaniego, CSA Capítulo Chile
Edson Vittoriano, CSA Capítulo Chile
Juan José Cuellar, Wom
Manuel Caldas, Telefónica
Gerardo Guzmán, Banco de Crédito del Perú
Jorge Rojas, AGN Consultores
Leonardo Rosso, CSA Capítulo Argentina
Luciano Moreira, CSA Capítulo Argentina

Equipo CSA de coordinación traducción:

Ryan Bergsma, CSA
Marina Bregou, CSA

Autores Principales

Rich Mogull
James Arlen
Francoise Gilbert
Adrian Lane
David Mortman
Gunnar Peterson
Mike Rothman

Editores

John Moltz
Dan Moren
Evan Scoboria

Staff de CSA

Jim Reavis
Luciano (J.R.) Santos
Hillary Baron
Ryan Bergsma
Daniele Catteddu
Victor Chin
Frank Guanco
Stephen Lumpe (Design)
John Yeoh

Colaboradores

En nombre de la Junta de Directores de CSA y del Equipo Ejecutivo de CSA, nos gustaría agradecer a todas las personas que contribuyeron con su tiempo y comentarios a esta versión de la *Guía de Seguridad de Áreas Críticas para la Computación en la Nube* de CSA. Valoramos sus contribuciones voluntarias y creemos que la dedicación de voluntarios como ustedes continuará liderando Cloud Security Alliance en el futuro.

CARTA DEL DIRECTOR EJECUTIVO (CEO)

Estoy emocionado con esta última contribución a la base de conocimiento de la comunidad de las mejores prácticas de seguridad en la nube que comenzó con el documento de orientación inicial de Cloud Security Alliance publicado en abril de 2009. Esperamos que estudie cuidadosamente los problemas y recomendaciones aquí resumidos, compare con su propia experiencia y nos brinde su opinión. Un gran agradecimiento a todos los que participaron en esta investigación.

Recientemente, tuve la oportunidad de pasar un día con uno de los expertos de la industria que ayudó a fundar Cloud Security Alliance. Me comentó que, en gran parte, CSA ha completado su misión inicial, que era probar que la computación en la nube podría protegerse y proporcionar las herramientas necesarias para ese fin. CSA no solo ayudó a hacer de la computación en la nube una opción segura y creíble para la tecnología de la información, sino que hoy la computación en la nube se ha convertido en la opción predeterminada para TI y está reconvirtiendo el mundo empresarial moderno de manera muy profunda.

El rotundo éxito de la computación en la nube y el rol de CSA en liderar el ecosistema de la nube de confianza traen consigo aún mayores desafíos y urgencias en nuestra misión renovada. La nube ahora se está convirtiendo en el *back-end* para todas las formas de informática, incluido el omnipresente *Internet of Things*. La computación en la nube es la base de la industria de la seguridad de la información. Las nuevas formas de organizar el cómputo, como los contendedores y *DevOps* son inseparables de la nube y aceleran nuestra revolución.

En Cloud Security Alliance, nos comprometemos a proporcionarle el conocimiento de seguridad esencial que necesita para este entorno de TI de rápida evolución y permanecer a la vanguardia de las tendencias de protección y confianza de nueva generación. Damos la bienvenida a su participación en nuestra comunidad.

Atentamente,

Jim Reavis
Cofundador y Director Ejecutivo
Cloud Security Alliance

Dominio 1 Conceptos y Arquitecturas de la Computación en la Nube

1.0 Introducción

Este dominio proporciona el marco conceptual para el resto de la Guía de Seguridad de Cloud Security Alliance. Describe y define la computación en la nube, establece nuestra terminología básica, y detalla la lógica general y el marco arquitectónico utilizados en el resto del documento.

Existen muchas formas diferentes de ver la computación en la nube: es una tecnología, una colección de tecnologías, un modelo operativo, un modelo de negocio, solo por nombrar algunos. Es, en esencia, *transformador* y *disruptivo*. También está creciendo muy, muy rápido y no muestra signos de desaceleración. Mientras que los modelos de referencia que incluimos en la primera versión de esta Guía son todavía relativamente precisos, ciertamente no están ya completos. Incluso esta actualización posiblemente no cubra todas las posibles evoluciones en los próximos años.

La computación en la nube ofrece inmensos beneficios potenciales en *agilidad*, *flexibilidad* y *economía*. Las organizaciones pueden moverse más rápido (ya que no tienen que comprar y aprovisionar hardware, y todo está definido por software), reducir el tiempo de inactividad (gracias a la elasticidad inherente y a otras características de la nube), y ahorrar dinero (debido a la reducción de los gastos de capital y una mejor vinculación entre la demanda y capacidad). También vemos beneficios de *seguridad* ya que los proveedores de la nube tienen importantes incentivos económicos para proteger a los clientes.

Sin embargo, estos beneficios solo aparecen si comprende y adopta *modelos nativos* de la nube y ajusta sus arquitecturas y controles para alinearse con las características y capacidades de las plataformas en la nube. De hecho, tomar una aplicación o activo existente y simplemente moverlo a un proveedor de la nube sin ningún cambio a menudo reducirá la agilidad, la resistencia e incluso la seguridad, todo ello mientras se incrementan los costos.

El objetivo de este dominio es construir la base en la que el resto del documento y sus recomendaciones se fundamentan. La intención es proporcionar un lenguaje común y la comprensión de la computación en la nube para profesionales de la seguridad, comienza destacando las diferencias entre la nube y la computación tradicional, y ayudar a orientar a los profesionales de seguridad hacia un enfoque de la adopción de la nube nativa que resulten en una mejor seguridad (y esos otros beneficios), en lugar de crear más riesgos.

Este dominio incluye 4 secciones:

- Definición de la computación en la nube
- El modelo lógico de la nube
- Modelo conceptual, arquitectónico y de referencia de la nube
- Alcance, responsabilidades y modelos de seguridad y cumplimiento de la nube

Cloud Security Alliance no se propone crear una nueva taxonomía o modelo de referencia. Nuestro objetivo es refinar y armonizar los modelos existentes – especialmente el trabajo de *NIST Special Publication 800-145*, *ISO/IEC 17788 e ISO/IEC 17789* –, y concentrarse en lo que es más relevante para los profesionales de la seguridad.

1.1 Visión general

1.1.1 Definición de la Computación en la Nube

La computación en la nube es un nuevo modelo operacional y un conjunto de tecnologías para administrar grupos compartidos de recursos informáticos.

Es una tecnología disruptiva que tiene el potencial de mejorar la colaboración, agilidad, escalabilidad y disponibilidad, además de facilitar oportunidades para la reducción de costos a través de una optimización y eficiencia informática. El modelo de la nube contempla un mundo donde los componentes se pueden orquestar rápidamente, aprovisionado, implementado y desmantelado, y escalando hacia arriba o hacia abajo para proporcionar un modelo de asignación y consumo similar a un servicio a pedido.

NIST define la computación en la nube como:

> La computación en la nube es un modelo para permitir un acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo o interacción del proveedor de servicio.

La definición de *ISO/IEC* es muy similar:

> Paradigma para permitir el acceso de red a un conjunto de recursos compartidos, escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda.

Una forma (un poco) más simple de describir la nube es que toma un conjunto de recursos, como procesadores y memoria, y los coloca en un grupo grande de recursos (en este caso, usando virtualización). Los usuarios piden lo que necesitan del grupo de recursos, como 8 CPUs y 16 GB de memoria, y la nube asigna los recursos para el usuario, el cual se conecta y los utiliza a través de la red. Cuando el usuario finaliza su uso, pueden liberar los recursos nuevamente en el grupo para que otro usuario los use.

Una nube puede consistir en casi cualquier recurso informático, desde nuestros ejemplos de "cómputo" de procesadores y memoria hasta redes, almacenamiento y recursos de mayor nivel como bases de datos y aplicaciones. Por ejemplo, suscribirse a una aplicación de gestión de relaciones con clientes para 500 empleados en un servicio compartido por cientos de otras organizaciones es computación en la nube tanto como el lanzamiento de 100 servidores remotos en una nube informática.

> Definición: Un *usuario de la nube* es la persona u organización que solicita y utiliza los recursos, y el proveedor de la nube es la persona u organización que lo entrega. A veces también usamos los términos cliente y consumidor para referirnos al usuario de la nube, y servicio o simplemente nube para describir al proveedor. ***NIST* 500-292** usa el término "actor de nube" y agrega roles para intermediarios en la nube, operadores, y auditores. *ISO/IEC* 17788 utiliza los términos servicio al cliente en la nube, socio de servicios en la nube y proveedor de servicios en la nube.

Las técnicas clave para crear una nube son la abstracción y la orquestación. Extraemos los recursos de la infraestructura física subyacente para crear nuestras agrupaciones, y usamos la orquestación (y la automatización) para coordinar la distribución y la entrega de un conjunto de recursos de dichas agrupaciones al usuario. Como verá, estas dos técnicas crean todas las características esenciales que utilizamos para definir algo como una "nube".

Esta es la diferencia entre la computación en la nube y la virtualización tradicional; la virtualización abstrae los recursos, pero normalmente carece de la orquestación para agruparlos y entregarlos a pedido a los usuarios, en lugar de depender de procesos manuales.

Las nubes son de *múltiple tenencia* por naturaleza. Múltiples grupos de diferentes usuarios comparten el mismo grupo de recursos, pero están *segregados* y *aislados* el uno del otro. La segregación permite que el proveedor de la nube distribuya los recursos a los diferentes grupos, y el aislamiento asegura que no puedan ver o modificar los activos de los demás. La múltiple tenencia no solo se aplica en diferentes organizaciones; también se usa para dividir recursos entre diferentes unidades en una sola empresa u organización.

1.1.2 Modelo de definición

Cloud Security Alliance (CSA) usa el modelo ***NIST* de la computación en la nube** como su estándar para definir la computación en la nube. El CSA también respalda el **modelo *ISO/IEC*** que es más profundo, y además sirve como modelo de referencia. A lo largo de este dominio, haremos referencia a ambos.

La publicación de *NIST* es generalmente bien aceptada, y la guía se alinea con el *NIST Working Definition of Cloud Computing* (*NIST* 800-145) para brindar coherencia y consenso en torno a un lenguaje para enfocarse en casos de uso en lugar de matices semánticos.

Es importante tener en cuenta que esta guía está destinada a ser ampliamente utilizable y aplicable a las organizaciones a nivel mundial. Si bien el *NIST* es una organización gubernamental de los EE. UU., la selección de este modelo de referencia no debe interpretarse como una sugerencia de exclusión de otros puntos de vista o geografías.

NIST define la computación en la nube mediante la descripción de cinco características esenciales, tres modelos de servicios en la nube y cuatro modelos de implementación en la nube. Se resumen de forma visual y se explican en detalle en la página siguiente.

1.1.2.1 Características esenciales

Estas son las características que hacen que una nube sea una nube. Si algo tiene estas características, considérelo computación en la nube. Si carece de alguno de ellos, probable que no sea una nube.

- La *agrupación de recursos* es la característica más fundamental, como se discutió anteriormente. El proveedor abstrae los recursos y los recopila en un grupo, partes de los cuales se pueden asignar a diferentes usuarios (generalmente basados en políticas).
- Los usuarios aprovisionan los recursos del grupo mediante el *autoservicio bajo demanda*. Ellos manejan sus propios recursos, sin tener que hablar con un administrador humano.
- El *amplio acceso a la red* significa que todos los recursos están disponibles en una red, sin necesidad del acceso físico directo; la red no es necesariamente parte del servicio.
- La *elasticidad rápida* permite a los usuarios ampliar o contraer los recursos que utilizan del grupo (aprovisionamiento y *desaprovisionamiento*), a menudo de forma completamente automática. Esto les permite relacionar más estrechamente el consumo de recursos con la demanda (por ejemplo, agregar servidores virtuales cuando la demanda aumenta y luego los apaga cuando baja la demanda).
- *Medidores de servicio* que son proporcionados, para garantizar que los usuarios solo usen lo que se ha asignado, y, si es necesario, cobrar por ello. Aquí es donde viene el término *computación como servicio público* (*utility computing*), ya que los recursos informáticos ahora se pueden consumir como el agua y la electricidad, el cliente solo paga por lo que usa

ISO/IEC 17788 enumera seis características clave, las primeras cinco de las cuales son idénticas a las características del *NIST*. La única adición es *múltiple tenencia*, que es distinta de la agrupación de recursos.

1.1.2.2 Modelos de servicio

El *NIST* define tres modelos de servicio que describen las diferentes categorías fundamentales de servicios en la nube:

- *Software como servicio (SaaS)* es una aplicación completa administrada y alojada por el proveedor. Los usuarios acceden a ella con un navegador web, una aplicación móvil o una aplicación de cliente liviana.
- *Plataforma como Servicio (PaaS)* abstrae y proporciona plataformas de desarrollo de aplicaciones, como bases de datos, plataformas de aplicaciones (por ejemplo, un lugar para ejecutar Python, PHP u otro código), almacenamiento de archivos y colaboración, o incluso procesamiento de aplicaciones propietarias (como aprendizaje de máquina, procesamiento de *Big Data* o acceso directo a interfaces de programación de aplicaciones (*API*) a características de una aplicación SaaS completa). El diferenciador clave es que, con PaaS, no se maneja los servidores, redes u otra infraestructura subyacente.
- *Infraestructura como servicio (IaaS)* ofrece acceso a un conjunto de recursos de infraestructura base de informática, como computación, red o almacenamiento.

A veces los llamamos niveles "SPI".

ISO/IEC utiliza una definición más compleja con *tipos de capacidades de nube* que se correlacionan estrechamente con los niveles *SPI* (aplicación, infraestructura y tipos de capacidad de plataforma). Entonces lo expande a *categorías de servicios en la nube* que son más granulares, como computación como un servicio, Almacenamiento de datos como un Servicio e incluso incluye *IaaS / PaaS / SaaS.*

Estas categorías son algo permeables: algunos servicios en la nube abarcan estos niveles, otros no caen en un solo modelo de servicio. Hablando en términos prácticos, no hay razón para tratar de asignar todo en estas tres amplias categorías, o incluso en las categorías más granulares en el modelo *ISO/IEC*. Esto es simplemente una herramienta descriptiva útil, no un marco rígido.

Ambos enfoques son igualmente válidos, pero dado que el modelo NIST es más conciso y actualmente se usa de manera más amplia, es la definición utilizada predominantemente en la investigación CSA.

1.1.2.3 Modelos de implementación

Tanto el *NIST* como *ISO/IEC* utilizan los mismos cuatro modelos de implementación en la nube. Son cómo las tecnologías se implementan y consumen, y se aplican en toda la gama de modelos de servicio:

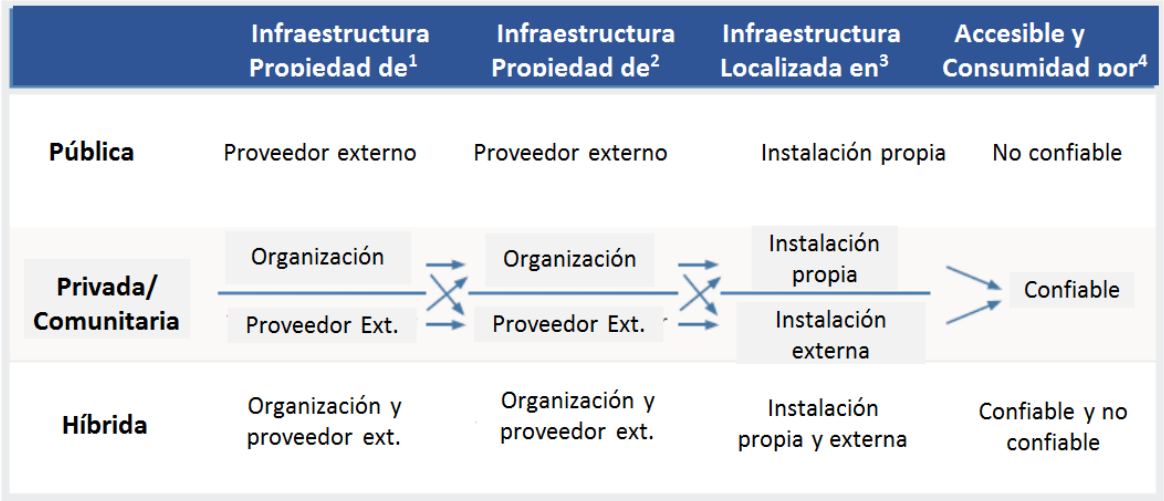
- *Nube pública*. La infraestructura de la nube está disponible para el público en general o un gran grupo de la industria y es propiedad de una organización que vende servicios en la nube.

- *Nube privada*. La infraestructura de la nube se opera únicamente para una sola organización. Puede ser administrado por la organización o por un tercero y puede estar ubicado en sus instalaciones o fuera de su propiedad.

- *Nube comunitaria*. La infraestructura en la nube es compartida por varias organizaciones y soporta a una comunidad específica que tiene inquietudes compartidas (por ejemplo, misión, requisitos de seguridad, política o consideraciones de cumplimiento). Puede ser administrado por las organizaciones o por un tercero y puede estar ubicado en sus instalaciones o fuera de ellas.

- *Nube híbrida.* La infraestructura de la nube es una composición de dos o más nubes (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas por estándares o tecnología patentada que permite la portabilidad de datos y aplicaciones (por ejemplo, proliferación de nubes para equilibrar la carga entre nubes). El término Híbrido también se usa comúnmente para describir un centro de datos que no es de nube y está conectado directamente a un proveedor de la nube.

Los modelos de implementación se definen según el usuario de la nube, es decir, quién usa la nube. Como se muestra en el siguiente diagrama, la organización que posee y administra la nube variará incluso dentro de un único modelo de implementación.



	Infraestructura Propiedad de[1]	Infraestructura Propiedad de[2]	Infraestructura Localizada en[3]	Accesible y Consumidad por[4]
Pública	Proveedor externo	Proveedor externo	Instalación propia	No confiable
Privada/ Comunitaria	Organización / Proveedor Ext.	Organización / Proveedor Ext.	Instalación propia / Instalación externa	Confiable
Híbrida	Organización y proveedor ext.	Organización y proveedor ext.	Instalación propia y externa	Confiable y no confiable

1 La administración incluye: gobierno, operaciones, seguridad, cumplimiento, etc.

2 La infraestructura implica infraestructura física, como instalaciones, redes informáticas y equipos de almacenamiento

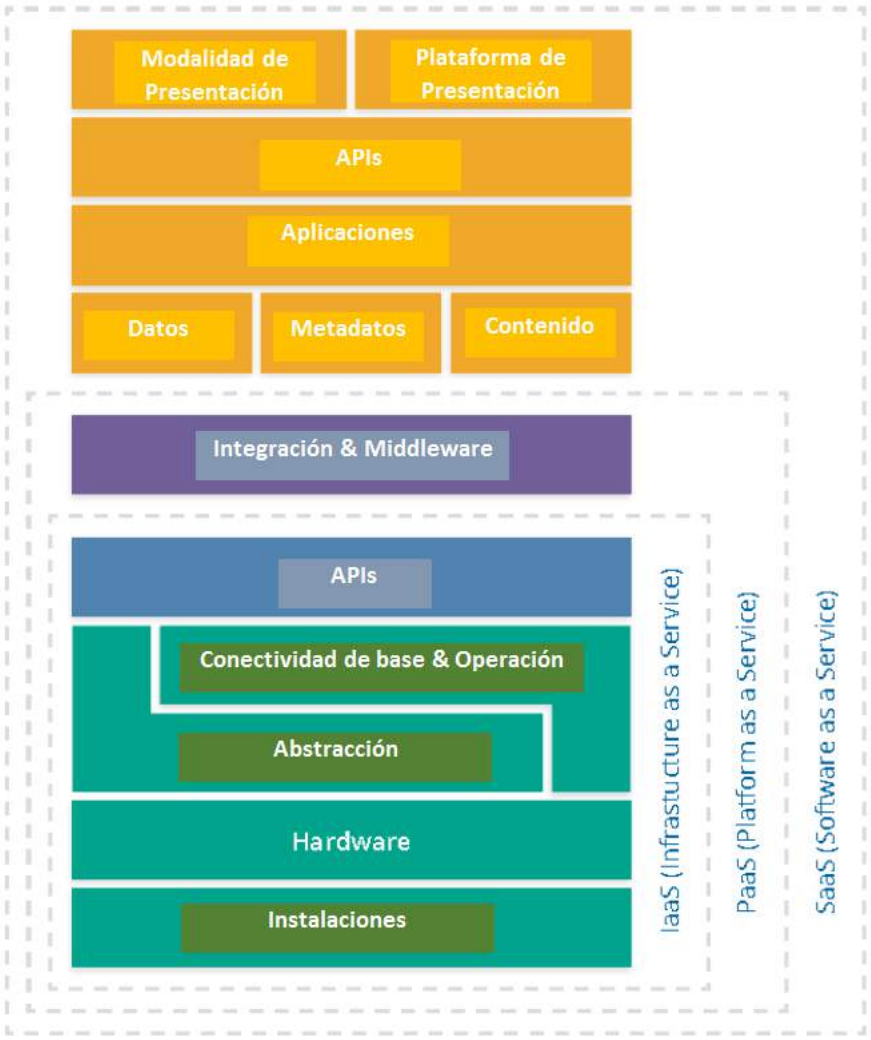
3 La ubicación de la infraestructura es tanto física como relativa al alcance de gestión de una organización y habla de propiedad versus el control

4 Los usuarios de confianza del servicio son aquellos que se consideran parte del alcance legal / contractual / político de una organización, incluidos empleados, contratistas y socios comerciales. Los usuarios que no son de confianza son aquellos que pueden estar autorizados para consumir algunos / todos los servicios, pero no son extensiones lógicas de la organización

1.1.3 Modelos de referencia y arquitectura

En la actualidad, existe una amplia gama de técnicas tecnológicas en constante evolución para la creación de servicios en la nube, lo que hace que cualquier referencia o modelo arquitectónico sea obsoleto desde el principio. El objetivo de esta sección es proporcionar algunos fundamentos para ayudar a los profesionales de seguridad a tomar decisiones informadas, así como una línea de base para comprender modelos más complejos y emergentes. Para un profundo modelo arquitectónico de referencia, nuevamente recomendamos *ISO/IEC* 17789 y *NIST* 500-292, que complementan el modelo de definición *NIST*

Una forma de ver la computación en la nube es como una pila donde el Software como Servicio se basa en la Plataforma como Servicio, que se basa en la Infraestructura como Servicio. Esto no es representativo de todas (o incluso la mayoría) de las implementaciones del mundo real, pero sirve como una referencia útil para iniciar la discusión.



1.1.3.1 Infraestructura como servicio (*IaaS*)

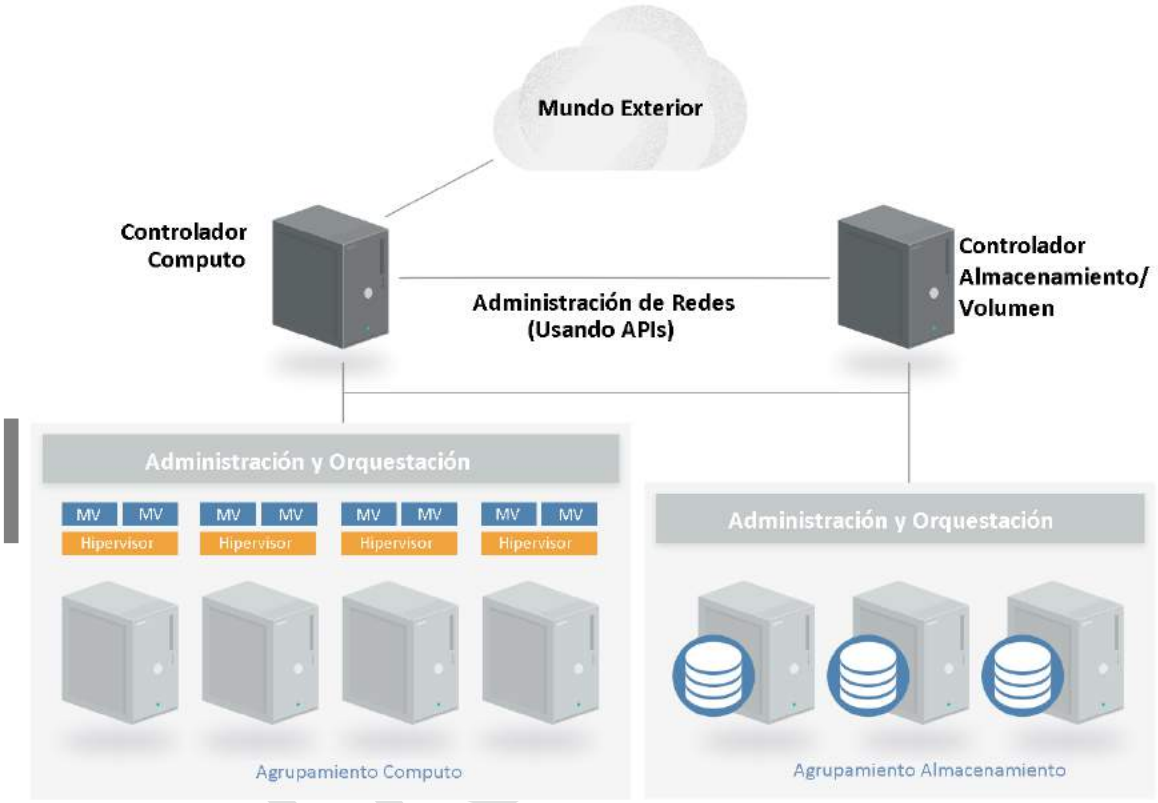
Las instalaciones físicas y la infraestructura de hardware forman la base de *IaaS*. Con la computación en la nube, abstraemos y agrupamos estos recursos, pero en el nivel más básico siempre necesitamos hardware físico, redes y almacenamiento para construir sobre ellos. Estos recursos se agrupan utilizando abstracción y orquestación. La abstracción, a menudo a través de la virtualización, libera los recursos de sus restricciones físicas para permitir la agrupación. Luego, un conjunto de herramientas básicas de conectividad y entrega (orquestación) vinculan estos recursos de abstracción en conjunto, crea los grupos y proporcionan la automatización para entregarlos a los clientes.

Todo esto se facilita mediante el uso de *Interfaces de Programación de Aplicaciones* (*API*). Las *APIs* generalmente son el método de comunicación subyacente para los componentes dentro de una nube, algunos de los cuales (o un conjunto totalmente diferente) están expuestos al usuario de la nube para administrar sus recursos y configuraciones. La mayoría de las *APIs* en la nube actualmente usan *REST* (Transferencia de estado representacional), que se ejecuta sobre el protocolo HTTP, lo que lo hace extremadamente adecuado para los servicios de Internet.

En la mayoría de los casos, esas *APIs* son accesibles de forma remota y se envuelven en una interfaz de usuario basada en web. Esta combinación es el *plano de administración de la nube*, ya que los consumidores lo usan para administrar y configurar los recursos de la nube, como el lanzamiento de máquinas virtuales (instancias) o la configuración de redes virtuales. Desde una perspectiva de seguridad, es la mayor diferencia al proteger la infraestructura física (ya que no puede confiar en el acceso físico como control) y la máxima prioridad cuando se diseña un programa de seguridad en la nube. Si un atacante ingresa en su plano de administración, es posible que tenga acceso remoto completo a toda su implementación en la nube.

Así, *IaaS* consta de una instalación, hardware, una capa de abstracción, una capa de orquestación (conectividad básica y entrega) para unir los recursos abstraídos y *APIs* para administrar de forma remota los recursos y entregarlos a los consumidores.

Aquí hay un ejemplo arquitectónico simplificado de una plataforma de computación *IaaS*:



Este es un diagrama muy simple que muestra los controladores de cómputo y almacenamiento para orquestación, hipervisores para abstracción y la relación entre los agrupamientos de cómputo y almacenamiento. Omite muchos componentes, como el administrador de red.

Una serie de servidores físicos ejecutan cada uno dos componentes: un hipervisor (para virtualización) y el software de administración / orquestación para vincular los servidores y conectarlos al controlador de cómputo. Un cliente solicita una instancia (servidor virtual) de un tamaño particular y el controlador de la nube determina qué servidor tiene la capacidad y asigna una instancia del tamaño solicitado.

Luego, el controlador crea un disco duro virtual solicitando almacenamiento del controlador de almacenamiento, que asigna almacenamiento desde el agrupamiento de almacenamiento y lo

conecta al servidor huésped correspondiente y a la instancia a través de la red (una red dedicada para el tráfico de almacenamiento). Las redes, incluidas las interfaces y direcciones de redes virtuales, también se asignan y conectan a la red virtual necesaria.

El controlador luego envía una copia de la imagen del servidor a la máquina virtual, la inicia y la configura; esto crea una instancia que se ejecuta en una máquina virtual (*VM*), con la red virtual y el almacenamiento configurados correctamente. Una vez que se completa todo este proceso, el controlador de la nube correlaciona la información de metadatos y conectividad y la pone a disposición del consumidor, que ahora puede conectarse a la instancia e iniciar sesión.

1.1.3.2 Plataforma como servicio (*PaaS*)

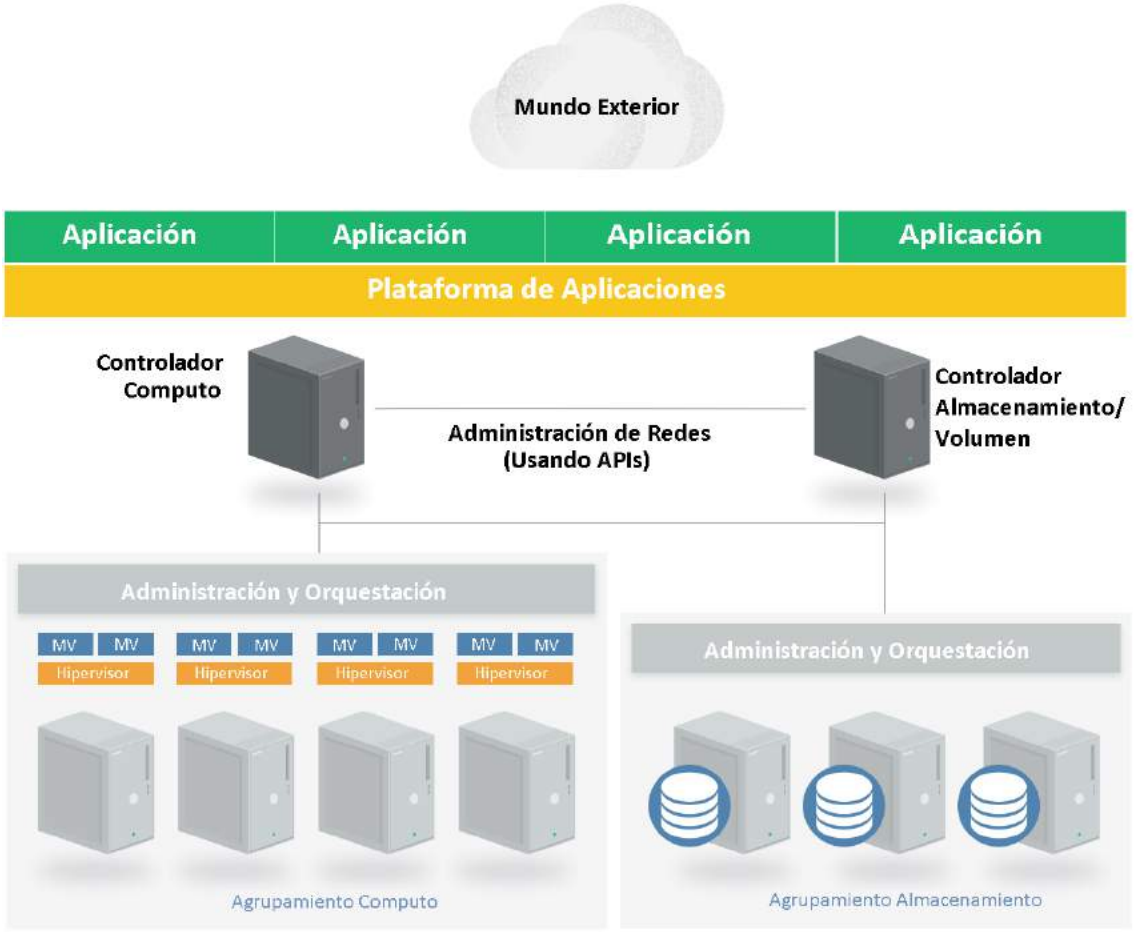
De todos los modelos de servicio, *PaaS* es el más difícil de caracterizar definitivamente debido tanto a la amplia gama de ofertas de *PaaS* como a las muchas formas de crear servicios de *PaaS*. PaaS agrega una capa adicional de integración con marcos de desarrollo de aplicaciones, capacidades de middleware y funciones como bases de datos, mensajería y colas. Estos servicios permiten a los desarrolladores crear aplicaciones en la plataforma con lenguajes de programación y herramientas que son compatibles con la pila.

Una opción, frecuentemente vista en el mundo real e ilustrada en nuestro modelo, es construir una plataforma sobre *IaaS*. Una capa de integración y middleware se basa en *IaaS*, luego es agrupada, orquestada y expuesta a los clientes usando *APIs* como *PaaS*. Por ejemplo, una base de datos como servicio podría construirse mediante la implementación de software de sistema de gestión de bases de datos modificado en instancias que se ejecutan en *IaaS*. El cliente gestiona la base de datos a través de *API* (y una consola web) y accede a ella a través de los protocolos de red de base de datos normales o, de nuevo, a través de *API*.

En *PaaS*, el usuario de la nube solo ve la plataforma, no la infraestructura subyacente. En nuestro ejemplo, la base de datos se expande (o contrae) según sea necesario en función de la utilización, sin que el cliente tenga que administrar servidores individuales, redes, parches, etc.

Otro ejemplo es una plataforma de implementación de aplicaciones. Es un lugar donde los desarrolladores pueden cargar y ejecutar código de aplicación sin administrar los recursos subyacentes. Existen servicios para ejecutar casi cualquier tipo de aplicación en cualquier lenguaje en *PaaS*, liberando a los desarrolladores de la configuración y creación de servidores, manteniéndolos actualizados, o preocupándose por complejidades como la agrupación y el equilibrio de carga.

Este diagrama de arquitectura simplificado muestra una plataforma de aplicación (*PaaS*) que se ejecuta en la parte superior de nuestra arquitectura *IaaS*:



PaaS no necesariamente se debe construir encima de *IaaS*; no hay ninguna razón por la que no pueda ser una arquitectura autónoma diseñada a medida. La característica definitoria es que los consumidores acceden y administran la plataforma, no la infraestructura subyacente (incluida la infraestructura de la nube).

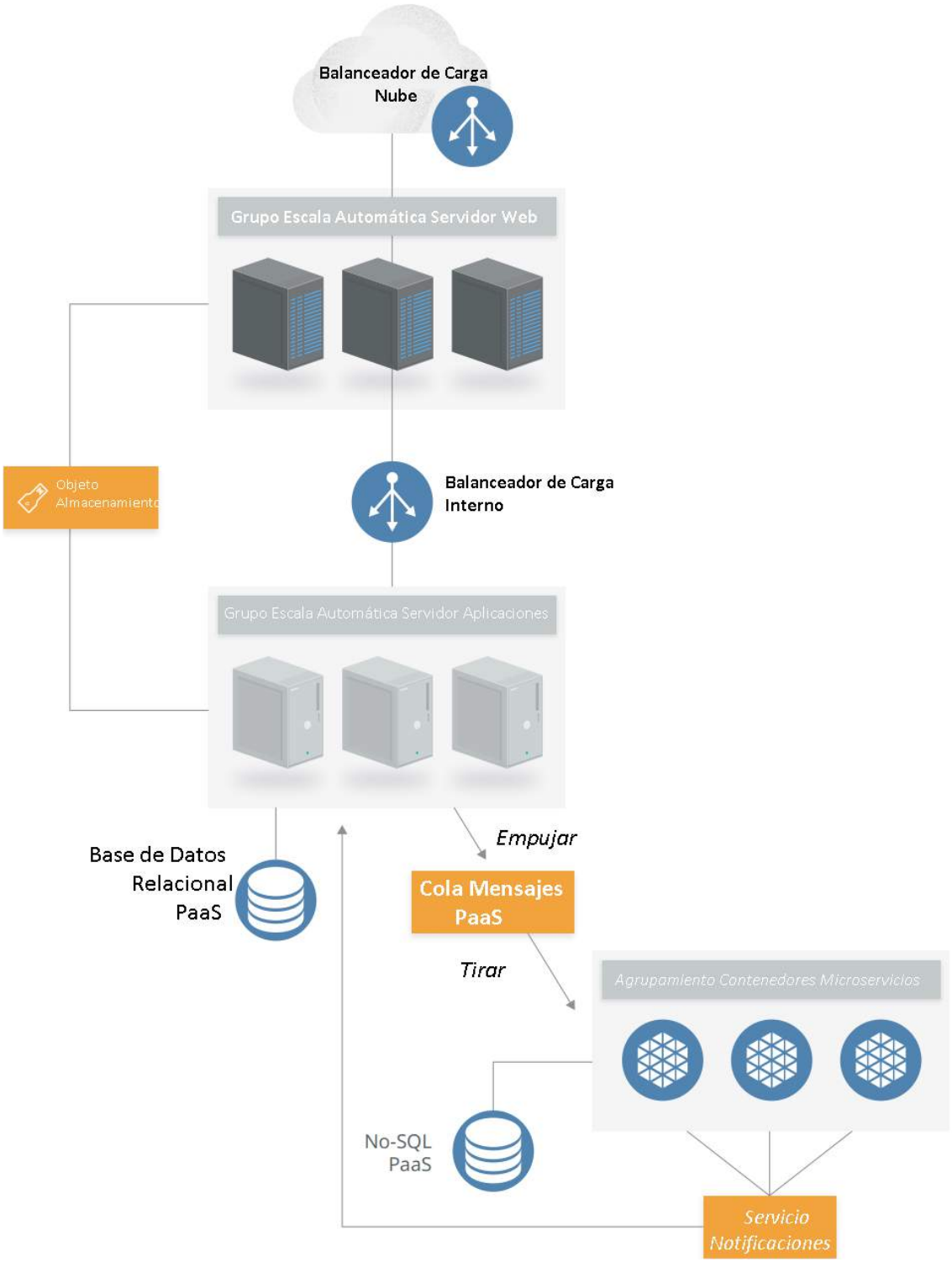
1.1.3.3 Software como servicio (*SaaS*)

Los servicios SaaS son aplicaciones completas para usuarios múltiples, con todas las complejidades arquitectónicas de cualquier plataforma de software grande. Muchos proveedores de *SaaS* se basan en *IaaS* y *PaaS* debido a la mayor agilidad, capacidad de recuperación y (potenciales) beneficios económicos.

La mayoría de las aplicaciones modernas en la nube (*SaaS* u otras) utilizan una combinación de *IaaS* y *PaaS*, a veces a través de diferentes proveedores de la nube. Muchos también tienden a ofrecer *API* públicas para alguna (o toda) la funcionalidad. A menudo necesitan estos para soportar una variedad de clientes, especialmente navegadores web y aplicaciones móviles.

Por lo tanto, todo *SaaS* tiende a tener una capa de aplicación / lógica y almacenamiento de datos, con una *API* en la parte superior. Luego, hay una o más capas de presentación, que a menudo incluyen navegadores web, aplicaciones móviles y acceso público a la *API*.

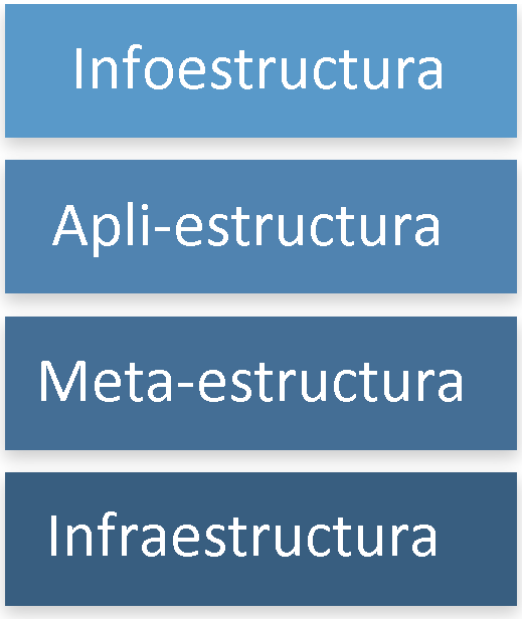
El siguiente diagrama de arquitectura simplificado se toma de una plataforma SaaS real, pero se generaliza para eliminar las referencias a los productos específicos en uso:



1.1.4 Modelo lógico

A un alto nivel, tanto la computación en la nube como la tradicional se adhieren a un modelo lógico que ayuda a identificar diferentes capas en función de la funcionalidad. Esto es útil para ilustrar las diferencias entre los diferentes modelos de computación:

- *Infraestructura*: Los componentes principales de un sistema informático: cómputo, red y almacenamiento. La base sobre la que se basa todo lo demás. Las partes móviles.
- *Meta-estructura*: Los protocolos y mecanismos que proporcionan la interfaz entre la capa de infraestructura y las otras capas. El pegamento que une las tecnologías y permite la administración y configuración.
- *Info-estructura*: Los datos y la información. Contenido en una base de datos, almacenamiento de archivos, etc.
- *Apli-estructura*: Las aplicaciones implementadas en la nube y los servicios de aplicaciones subyacentes utilizados para construirlos. Por ejemplo, las funciones de Plataforma como Servicio, como colas de mensajes, análisis de inteligencia artificial o servicios de notificación.



Diferentes enfoques de seguridad se asignan a las diferentes capas lógicas. Seguridad de aplicaciones para la infraestructura de aplicaciones, seguridad de los datos a la info-estructura y seguridad de la infraestructura para la infraestructura.

La diferencia clave entre la computación en la nube y la tradicional es la meta-estructura. La meta-estructura de la nube incluye los componentes del plano de administración, que están habilitados para la red y de forma remota. Otra diferencia clave es que, en la nube, se tiende a duplicar en cada capa. La infraestructura, por ejemplo, incluye tanto la infraestructura utilizada para crear la nube como la infraestructura virtual utilizada y administrada por el usuario de la nube. En una nube privada, la misma organización podría necesitar administrar ambas; en la nube pública, el proveedor gestiona la infraestructura física mientras el consumidor gestiona su parte de la infraestructura virtual.

Como veremos más adelante, esto tiene profundas implicaciones sobre quién es el responsable de, y el administrador de, la seguridad.

Estas capas tienden a asignarse a diferentes equipos, disciplinas y tecnologías que se encuentran comúnmente en las organizaciones de TI. Si bien las diferencias de gestión de seguridad más obvias e inmediatas se encuentran en la meta-estructura, la nube difiere ampliamente de la informática tradicional dentro de cada capa. La escala de las diferencias dependerá no solo de la plataforma en la nube, sino de cómo exactamente el usuario de la nube utiliza la plataforma.

Por ejemplo, una aplicación nativa de la nube que hace una gran utilización de los productos *PaaS* de un proveedor de servicios en la nube experimentará más diferencias en la aplicación que la migración de una aplicación existente, con cambios mínimos, a la Infraestructura como servicio.

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

1.2.1 Alcance y responsabilidades de la seguridad en la nube y el cumplimiento

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. Piénselo 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*. Piense en ello como una matriz de responsabilidad que depende del proveedor de 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 la nube es responsable de casi toda la seguridad, ya que el usuario de 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 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 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 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 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.

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 de nube dado. Es menos importante si un proveedor de 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 nube y el consumidor. ¿Qué hace el proveedor? ¿Qué necesita hacer el consumidor? ¿El proveedor de la nube permite al consumidor hacer lo que necesita? ¿Qué está garantizado en los contratos de contrato y 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:

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

Cloud Security Alliance proporciona dos herramientas para ayudar a cumplir estos requisitos:

- El Cuestionario de Iniciativa de Evaluaciones de Consenso (CAIQ). Una plantilla estándar para que los proveedores de la nube documenten sus controles de seguridad y cumplimiento.
- 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. El *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.

1.2.2 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 usar 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 en este documento.

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

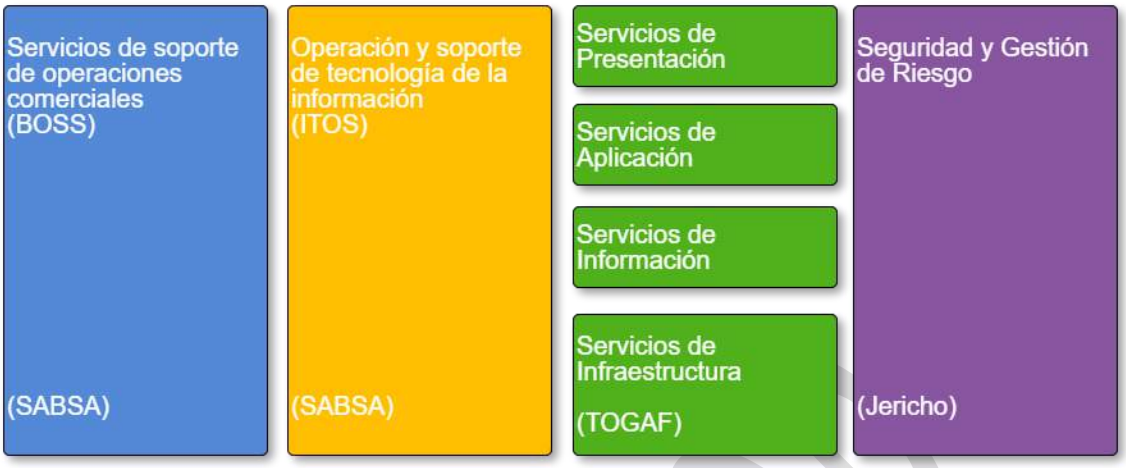
- *Las arquitecturas de referencia* son plantillas para implementar la seguridad en la nube, generalmente generalizadas (por ejemplo, una arquitectura de referencia de seguridad IaaS). Pueden ser muy abstractos, bordeando lo conceptual, o bastante detallados, bajando hasta controles y funciones específicos.

- *Los patrones de diseño* son soluciones reutilizables para problemas particulares. En seguridad, un ejemplo es la administración de registros *IaaS*. Al igual que con las arquitecturas de referencia, pueden ser más o menos abstractas o específicas, incluso bajando 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.

El CSA ha revisado y recomienda los siguientes modelos:

- La CSA arquitectura empresarial
- La 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 - Código de práctica para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.



A lo largo de esta Guía, también nos referimos a otros modelos específicos de dominio.

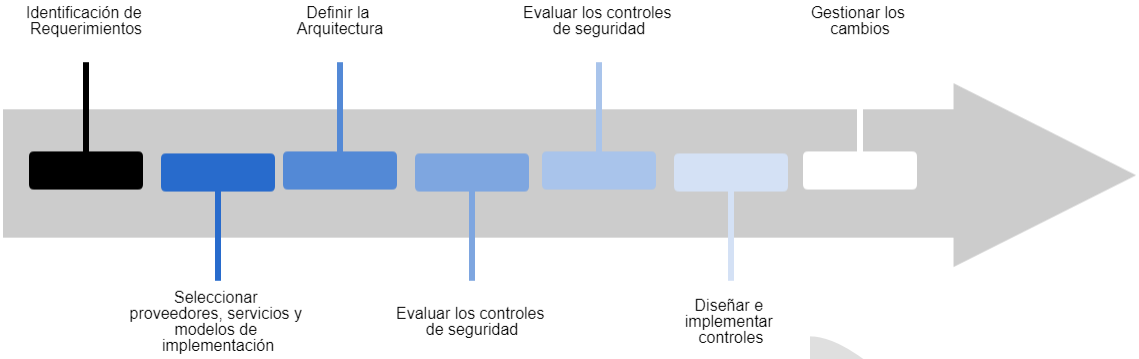
1.2.2.1 Un modelo simple de proceso de seguridad en la nube

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.
- Seleccione su proveedor de nube, servicio y modelos de implementación.
- Definir la arquitectura.
- Evaluar los controles de seguridad.
- Identificar las lagunas de control.
- Diseñar e implementar controles para llenar los vacíos.
- 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. 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 la nube antes de comenzar a traducir los requisitos de seguridad en controles.



1.3 Áreas de enfoque crítico

Los otros 13 dominios que componen el resto de la Guía CSA resaltan áreas de preocupación para la computación en la nube y están ajustados para abordar los "puntos problemáticos" de seguridad estratégicos y tácticos dentro de un entorno de nube, y pueden aplicarse a cualquier combinación de servicio en la nube y modelo de implementación.

Los dominios se dividen en dos grandes categorías: Gobierno y Operaciones. Los dominios de gobierno son amplios y abordan cuestiones estratégicas y de políticas dentro de un entorno de computación en la nube, mientras que los dominios operacionales se centran en preocupaciones de seguridad e implementación más tácticas dentro de la arquitectura.

1.3.1 Gobernando la nube

Dominio	Título	Descripción
2	Gobernanza y gestión de riesgos empresariales	La capacidad de una organización para gobernar y medir el riesgo empresarial introducido por la computación en la nube. Elementos como la precedencia legal para infracciones de acuerdos, capacidad de las organizaciones de usuarios para evaluar adecuadamente el riesgo de un proveedor de nube, responsabilidad de proteger datos confidenciales cuando tanto el usuario como el proveedor pueden tener la culpa, y cómo las fronteras internacionales pueden afectar estos problemas.
3	Asuntos legales: Contratos y descubrimiento electrónico	Posibles problemas legales al usar la computación en la nube. Las cuestiones que se abordan en esta sección incluyen los requisitos de protección para la información y los sistemas informáticos, las leyes de divulgación de violaciones de seguridad, los requisitos reglamentarios, los requisitos de privacidad, las leyes internacionales, etc.
4	Gestión de cumplimiento y auditoría	Mantener y probar el cumplimiento cuando se utiliza la computación en la nube. Aquí se tratan cuestiones relacionadas con la evaluación de cómo la computación en la nube afecta al cumplimiento de las políticas de seguridad interna, así como los diversos requisitos de cumplimiento (normativo, legislativo y de otro tipo). Este dominio incluye alguna dirección para probar el

		cumplimiento durante una auditoría.
5 	Gobierno de la información	Gobernando los datos que se colocan en la nube. Aquí se discuten los elementos que rodean la identificación y el control de los datos en la nube, así como los controles de compensación que se pueden usar para lidiar con la pérdida de control físico cuando se mueven datos a la nube. Se mencionan otros elementos, como quién es responsable de la confidencialidad de los datos, la integridad y la disponibilidad.

1.3.2 Operando la nube

Dominio	Título	Descripción
6 	Plano de Gestión y Continuidad del Negocio	Asegurar el plano de gestión y las interfaces administrativas utilizadas al acceder a la nube, incluidas las consolas web y las *API*. Garantizar la continuidad del negocio para implementaciones en la nube.
7 	Seguridad de Infraestructura	Seguridad del núcleo de la infraestructura de la nube, incluidas las redes, la seguridad de la carga de trabajo y las consideraciones de la nube híbrida. Este dominio también incluye fundamentos de seguridad para nubes privadas.
8 	Virtualización y contenedores	Seguridad para hipervisores, contenedores y redes definidas por software.
9 	Respuesta a incidentes, notificación y remediación	Detección, respuesta, notificación y reparación adecuada de incidentes. Esto intenta abordar los elementos que deberían estar en su lugar, tanto a nivel de proveedor como de usuario, para permitir el manejo adecuado de incidentes y análisis forense. Este dominio lo ayudará a comprender las complejidades que trae la nube a su programa actual de manejo de incidentes.
10 	Seguridad de aplicaciones	Asegurar el software de la aplicación que se ejecuta o se está desarrollando en la nube. Esto incluye elementos tales como si es apropiado migrar o diseñar una aplicación para que se ejecute en la nube y, de ser así, qué tipo de plataforma en la nube es la más adecuada (*SaaS*, *PaaS* o *IaaS*).
11 	Seguridad y cifrado de datos	Implementando la seguridad y el cifrado de datos, y garantizando la administración escalable de claves.
12 	Identidad, derecho y administración de acceso.	Administrar identidades y aprovechar los servicios de directorio para proporcionar control de acceso. La atención se centra en los problemas que se encuentran al extender la identidad de una organización a la nube. Esta sección proporciona información sobre cómo evaluar la preparación de una organización para llevar a cabo una Gestión de acceso, idoneidad e identidad (*IdEA*) basada en la nube.

13 	Seguridad como servicio	Proporcionar aseguramiento de seguridad facilitado por terceros, administración de incidentes, certificación de cumplimiento y supervisión de identidad y acceso.
14 	Tecnologías relacionadas	Tecnologías establecidas y emergentes con una estrecha relación con la computación en la nube., incluidas el *Big Data*, el Internet de las cosas y la informática móvil.

1.4 Recomendaciones

- Comprender las diferencias entre la computación en la nube y la infraestructura tradicional o la virtualización, y cómo la abstracción y la automatización afectan 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 la nube.
- Los proveedores de 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 también quién es responsable de cada uno.
- Usar un modelo de proceso de seguridad en la nube para seleccionar proveedores, arquitecturas de diseño, identificar brechas de control e implementar controles de seguridad y cumplimiento.

1.5 Créditos

- Arquitectura de referencia y modelo lógico basado en el trabajo de Christofer Hoff.

Dominio 2 Gobierno y Gestión del Riesgo Corporativo

2.0 Introducción

El gobierno o gobernanza y la gestión del riesgo son temas increíblemente amplios. Esta guía se focaliza en cómo cambian en la computación en la nube; esta guía no es ni debería ser considerada un manual o una exploración amplia de estos temas fuera de la nube.

Para profesionales de la seguridad, la Computación en la nube impacta en cuatro áreas del gobierno y la gestión del riesgo:

- El Gobierno incluye las políticas, los procesos y controles internos que incluyen cómo está funcionando una organización. Todo desde las estructuras y políticas hasta el liderazgo y otros mecanismos de gestión.

Para más Información sobre la gobernanza por favor ver

** ISO/IEC 38500:2015 - Information Technology - Governance of IT for the organization*

** ISACA - COBIT - A Business Framework for the Governance and Management of Enterprise IT*

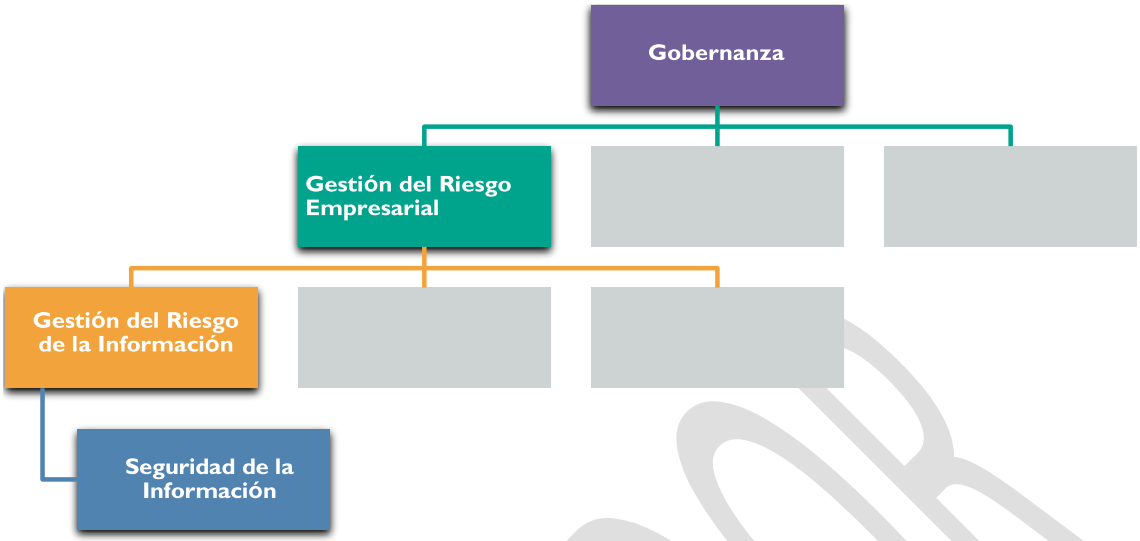
** ISO/IEC 27014:2013 - Information Technology - ISO/IEC 27014:2013 - Information Technology - Security techniques - Governance of information security*

- La *Gestión del riesgo empresarial* incluye gestionar el riesgo global para la organización, alineado con el gobierno de la organización y su tolerancia al riesgo. La gestión del riesgo empresarial incluye todas las áreas de riesgo, no únicamente las relacionadas con la tecnología.

- La *Gestión del riesgo de la información* cubre la gestión del riesgo de la información incluyendo la tecnología de la información. Las organizaciones encaran todo tipo de riesgos, desde los financieros a los físicos, y la información solamente es uno de los múltiples activos que una organización necesita gestionar.

- La *Seguridad de la información* es el conjunto de instrumentos y prácticas para la gestión del riesgo de la información. La seguridad de la información no es la razón de ser de la gestión de los riesgos de la información; políticas, contratos, seguros, y otros mecanismos que también tienen un rol (incluyendo la seguridad física para la información no digital).

  Sin embargo, el rol principal, si es que no es *el* rol, de la seguridad de la información es proveer de procesos y controles para proteger la información electrónica y los sistemas que se usan para acceder a ella. En una jerarquía simplificada, la seguridad de la información es una herramienta para la gestión del riesgo de la información, que es un instrumento para la gestión del riesgo empresarial, que es una herramienta de gobernanza. Las cuatro están estrechamente relacionadas, pero requieren un enfoque, procesos e herramientas individuales.



2.1: Jerarquía Simplificada del Riesgo y de la Gobernanza

Las cuestiones legales y el cumplimiento están cubiertas en los Dominios 3 y 4 respectivamente. La gestión del riesgo y la gobernanza de los datos están cubiertas en el Dominio 5. La seguridad de la información es esencialmente en el resto de esta guía.

2.1 Visión general

2.1.1 Gobierno

La computación en la nube afecta al gobierno, ya que introduce una tercera parte dentro del proceso (en el caso de una nube pública o nube privada hospedada) o posiblemente altera las estructuras internas de gobernanza en el caso de nube privada auto-hospedada. La primera cuestión a recordar en el gobierno de la Computación en la nube es que *una organización nunca puede externalizar la responsabilidad del gobierno*, incluso cuando se utilizan proveedores externos. Esto es siempre cierto, nube o no, pero es útil tenerlo presente cuando se navega por los conceptos de la Computación en la nube de modelos de responsabilidad compartida.

Los proveedores de servicio en la nube intentan aprovechar economías de escala para gestionar los costes y las capacidades. Esto significa crear servicios extremadamente estandarizados (incluyendo contratos y acuerdos de nivel de servicio) que son homogéneos para todos los clientes. Los modelos de gobierno necesariamente no pueden tratar de la misma forma a los proveedores de la nube que en la que tratan a los proveedores externos de servicio dedicados, los cuales típicamente personalizan sus ofertas, incluyendo los acuerdos legales, para cada cliente.

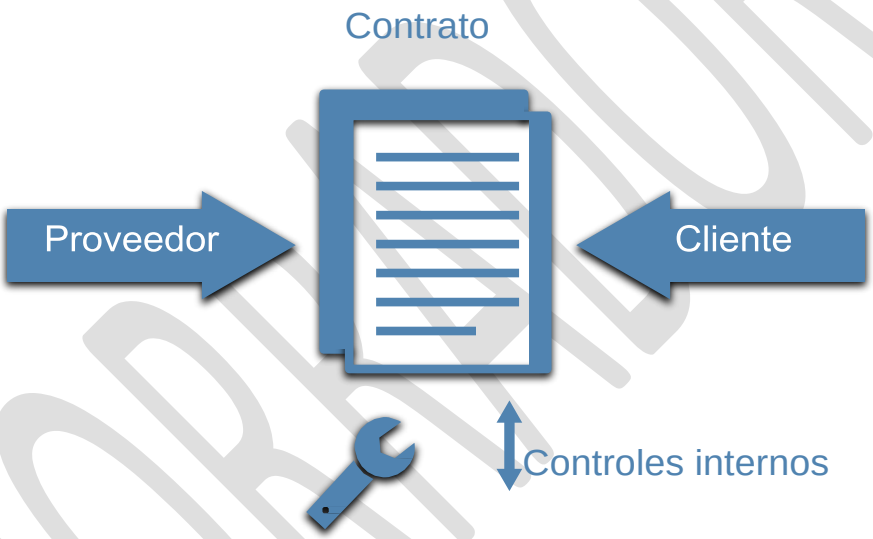
La computación en la nube cambia las *responsabilidades* y los mecanismos para la implementación y la gestión del gobierno. Las responsabilidades y mecanismos para la gobernanza se definen en el contrato, como en cualquier otra relación de negocio. Si el área afectada no está en el contrato, no hay mecanismos disponibles para hacer cumplir al proveedor, y es una brecha de gobernanza. Las brechas de gobernanza no necesariamente

excluyen utilizar el servicio del proveedor, pero requieren que el cliente ajuste sus propios procesos para cerrar las brechas o aceptar los riesgos asociados.

2.1.1.1 Herramientas para el gobierno de la nube

Como con cualquier otra área, hay herramientas de gestión específicas para la gobernanza. Esta relación se focaliza más en herramientas orientadas a proveedores externos, pero estas mismas herramientas pueden a menudo utilizarse internamente para despliegues privados:

- *Contratos*: la herramienta principal es el contrato entre el proveedor de la nube y el cliente de la nube (esto es aplicable para las nubes públicas y privadas). El contrato es su única garantía de cualquier nivel de servicio o compromiso – asumiendo que no hay un incumplimiento de contrato, que mete todo en un escenario legal. Los contratos son las principales herramientas para extender la gobernanza entre los socios de negocio y proveedores.



Los contratos definen las relaciones entre los proveedores y clientes y son la herramienta principal para que los clientes extiendan la gobernanza a sus proveedores.

- *Evaluaciones de proveedores (proveedor de la nube):* El cliente potencial de la nube realiza las evaluaciones utilizando la información disponible y los procesos y técnicas permitidas. Combinan investigaciones contractuales y manuales con análisis de terceros (las declaraciones legales a menudo utilizadas para comunicar los resultados de una evaluación o auditoría) e investigación técnica. Son muy similares a cualquier evaluación de proveedores y pueden incluir aspectos como viabilidad financiera, historia, características de las ofertas, declaraciones de terceros, retroalimentación entre colegas, y otras. Más adelante en este Dominio y en el Dominio 4 se desarrollan más detalladamente las evaluaciones.

- *Informe de cumplimiento legal:* los informes de cumplimiento legal incluyen toda la documentación sobre los proveedores internos y de las evaluaciones externas de cumplimiento legal. Los informes de auditoría de controles, que una organización puede realizar por sí misma, que un cliente puede realizar a un proveedor (aunque usualmente

no es una opción en la nube) o bien realizarlo por un tercero de confianza. Se prefieren auditorías y evaluaciones de terceros ya que proporcionan una validación independiente (asumiendo que se confía en el tercero).

Los informes de cumplimiento legal a menudo están disponibles para los interesados y los clientes de la nube, pero pueden estar solo disponibles bajo *NDA* o para clientes contratados. Esto es a menudo requerido por la firma que realizó la auditoría y no necesariamente estará completamente bajo el control del proveedor de la nube.

Las evaluaciones y auditorías deberían basarse en estándares (hay muchos). Es crítico entender el alcance, no solo el estándar utilizado. Estándares como *SSAE* 16 tienen un alcance definido, que incluye *qué* se evalúa (e.j. servicios del proveedor) así como *qué controles* son evaluados. Un proveedor puede 'pasar' una auditoría que no incluya ningún control de seguridad, con lo que resulta poco útil para los gestores de la seguridad y del riesgo. También se requiere considerar la confianza de las evaluaciones realizadas por un tercero que ha de ser equivalente en las actividades que se realicen en una evaluación propia. No todas las empresas de auditoría (o auditores) son iguales y su experiencia, historia, y cualificaciones deben incluirse en las decisiones de gobierno.

El registro de **Cloud Security Alliance *STAR*** es un programa de seguridad y de archivo de documentación para las evaluaciones del proveedor de la nube basadas en CSA *Cloud Control Matrix and Consensus Assessments Initiative Questionnaire*. Algunos proveedores también distribuyen documentación para certificaciones adicionales y evaluaciones (incluyendo autoevaluaciones).

2.1.2 Gestión del riesgo empresarial

La Gestión del Riesgo Empresarial es la gestión global del riesgo para una organización. Al igual que con el gobierno, el contrato define los roles y responsabilidades para la gestión del riesgo entre el proveedor de la nube y el cliente en la nube. Y, como con la gobernanza, nunca se puede externalizar en un proveedor externo la responsabilidad general ni la responsabilidad de la gestión de riesgos.

Para más información sobre la gestión del riesgo ver

* *ISO 31000:2009 - Risk management – Principles and guidelines*
* *ISO/IEC 31010:2009 - Risk management – Risk assessment techniques*
* [*NIST* Special Publication 800-37 Revision 1] (updated June 5, 2014) (http://nvlpubs.*nist*.gov/nistpubs/SpecialPublications/*NIST*.SP.800-37r1.pdf)

La gestión del riesgo en la nube está basada en el *modelo compartido de responsabilidades* (que a menudo se discute en referencia a la seguridad). El proveedor de la nube acepta cierta responsabilidad sobre algunos riesgos, pero el cliente en la nube es el responsable de todos los riesgos que no asume el proveedor. Esto es especialmente evidente cuando se evalúan las diferencias entre los modelos de servicio, el proveedor gestiona más riesgos en *SaaS* y el usuario en *IaaS*. Pero, de nuevo, el usuario de la nube es en última instancia el responsable de sus riesgos; solo se delega en el proveedor de la nube parte de la *gestión de riesgos*. Esto es

cierto incluso con una nube privada auto-hospedada; en esas situaciones, una unidad organizativa transmite la gestión de algunos de sus riesgos en el proveedor interno de la nube en lugar de en un tercero, y los *SLAs* internos y los procedimientos reemplazan a los contratos externos.

La Gestión del Riesgo Empresarial se basa en buenos contratos y documentación que permiten conocer dónde está la división de responsabilidades y los potenciales riesgos no tratados. Mientras que el gobierno se centra casi exclusivamente en los contratos, la gestión del riesgo puede profundizar en las capacidades tecnológicas y de procesos del proveedor, basada en su documentación. Por ejemplo, un contrato rara vez definirá cómo se implementará la seguridad de redes. La revisión de la documentación del proveedor proporcionará mucha más información que ayude a adoptar una decisión más efectiva sobre el riesgo.

La *tolerancia al riesgo* es la cantidad de riesgo en la organización que están dispuestos a aceptar la dirección y las partes interesadas. Ésta varía según el activo, no debe ser general para un proveedor particular; más bien, las evaluaciones deben alinearse con el valor y los requisitos de los activos involucrados. El hecho de que un proveedor de nube pública sea externo y que el usuario pueda estar preocupado por la infraestructura compartida para algunos activos no significa que no esté dentro del riesgo tolerado para todos los activos. En términos prácticos significa que se creará una matriz de servicios en la nube con todos los tipos de activos que se permiten en esos servicios. Mudarse a la nube no cambia la tolerancia al riesgo, simplemente cambia su gestión.

2.1.3 Los efectos del modelo de servicio y del modelo de despliegue

Al considerar las diversas opciones disponibles no sólo con los proveedores de servicios en la nube sino también en la forma en la que se proporcionan dichos servicios en la nube, se debe prestar atención a como los modelos de Servicio y Despliegue afectan a la capacidad de gestionar la gobernanza y el riesgo.

2.1.3.1 Modelos de servicio

Software
Como servicio
(*SaaS*)

En la mayoría de los casos, *SaaS* es el ejemplo más crítico de la necesidad de un contrato negociado. El contrato protegerá la capacidad de gobernanza o validar el riesgo en relación con los datos almacenados, procesados, transmitidos con y en la aplicación. Los proveedores de *SaaS* tienden a agruparse en uno de los extremos del espectro tamaño/capacidad y la probabilidad de contrato negociado es mucho mayor si el proveedor *SaaS* es pequeño. Desafortunadamente, algunos proveedores pequeños de SaaS no pueden operar con un nivel de sofisticación que alcance o exceda las capacidades de gobernanza y gestión del riesgo del cliente. Concretando, el nivel de visibilidad del funcionamiento real de la infraestructura que proporciona *SaaS* se limita a lo que se muestra en el interfaz desarrollado por el proveedor de la nube.

Plataforma Como servicio (*PaaS*)

Continuando con los modelos de servicio, el nivel de detalle que está disponible y (la consiguiente capacidad de auto-gestionar el gobierno y los problemas de riesgo) se incrementa. La probabilidad de un contrato totalmente negociado en este modelo es probablemente menor que en cualquiera de los otros modelos. Esto es porque el principal motor del *PaaS* es desarrollar una prestación sencilla con una alta eficiencia.

PaaS por lo general se suministra con una *API* enriquecida, y algunos proveedores han habilitado la recopilación de algunos de los datos necesarios para probar que los *SLAs* se están cumpliendo. Dicho esto, el cliente todavía se encuentra en la posición de tener que hacer un esfuerzo significativo para determinar si las estipulaciones contractuales proporcionan efectivamente el nivel de control o apoyo requerido para habilitar la gobernanza o la gestión de riesgos.

Infraestructura Como servicio (*IaaS*)

La Infraestructura como Servicio es el modelo en la nube que más se acerca a un centro de datos tradicional (o incluso la gestión tradicional de la externalización de un centro de datos), y la buena noticia es que la mayoría de las actividades existentes de gobernanza y gestión de riesgo que las organizaciones han construido y utilizado son directamente transferibles. Sin embargo, hay nuevas complejidades relacionadas con la orquestación subyacente y gestión por capas como las descritas en el Dominio 1 que permiten una infraestructura que a menudo se han pasado por alto.

En muchos sentidos, el gobierno y la gestión de riesgos de la orquestación y la gestión de capas es consistente con la infraestructura subyacente (redes, energía, HVAC, etc.) de un centro de datos tradicional. Están presentes los mismos problemas de gobernanza y gestión de riesgo, pero la exposición de esos sistemas es suficientemente diferente por lo que se requieren cambios en el proceso existente. Por ejemplo, controlar quién puede realizar los cambios de configuración en la red, quién cambia las cuentas en dispositivos individuales en el plano de gestión de la nube.

2.1.3.2 Modelos de despliegue

Pública

Los clientes de la nube tienen una capacidad reducida para gobernar las operaciones en una nube pública ya que el proveedor es responsable de la gestión y el gobierno de su infraestructura, empleados y todo lo demás. A menudo el cliente tiene una reducida capacidad para negociar los contratos, lo que afecta a la forma de extender su gobernanza en la nube. La escasa flexibilidad de los contratos es una propiedad natural del alquiler compartido. Los proveedores no necesariamente pueden ajustar los contratos y operaciones para cada cliente pues todo se ejecuta en un conjunto de recursos compartidos que utilizan el mismo conjunto de procesos. Adaptarse a los diferentes clientes incrementa el coste, ocasionando o introduciendo una compensación, y a menudo es la línea divisoria entre utilizar una nube pública o privada. La nube privada

hospedada permite una personalización completa, pero a un coste mayor debido a la pérdida de las economías de escala.

Esto no significa que no se deba intentar negociar el contrato, pero se ha de reconocer que no siempre es posible; en vez de esto, se necesitará elegir entre distintos proveedores (cuál puede ser menos seguro), o ajustar las necesidades y utilizar mecanismos alternativos de gobernanza o de mitigación.

Utilizando una analogía, pensar en un servicio de transporte. Cuando se utiliza un transportista/proveedor común no se puede definir su funcionamiento. Cuando se ponen documentos sensibles en un paquete y confías en ellos (transportista/proveedor) se aceptan sus obligaciones en el despliegue de la seguridad dentro de las expectativas de los Acuerdos de Nivel de Servicio.

Privada

La nube pública no es el único modelo que impacta en la gobernanza; incluso la nube privada puede tener un efecto. Si una organización permite que un tercero gestione su nube privada (que es muy común) esto afecta a la gobernanza igual que cuando se subcontrata a un proveedor. Se compartirán las responsabilidades junto con las obligaciones definidas en el contrato.

Aunque es probable que tenga más control sobre los términos contractuales, es importante asegurarse de que cubran los mecanismos de gobernanza necesarios. A diferencia de un proveedor público, que tiene varios incentivos para mantener su servicio bien documentado y en niveles de rendimiento estándar, funcionalidad y competitividad: una nube privada alojada puede ofrecer exactamente lo que está en el contrato, con todo lo demás a un costo adicional. Esto *debe* ser considerado y contabilizado en negociaciones, con cláusulas para garantizar que la plataforma misma permanezca actualizada y competitiva. Por ejemplo, al exigir al proveedor que actualice a la última versión de la plataforma de nube privada dentro de un cierto período de tiempo de lanzamiento y después de su firma.

Con una nube privada alojada de forma autónoma, la gobernanza se centrará en los acuerdos de nivel de servicio interno para el usuario de la nube (empresas u otras unidades organizativas) y modelos de transferencia de costes y facturación para proporcionar acceso a la nube.

Híbrida y colectiva

Cuando se contemplan **entornos de nube híbrida**, la estrategia de gobernanza debe considerar un conjunto mínimo de controles a los que se compromete el Proveedor del Servicio en la Nube en un contrato y los acuerdos internos de gobernanza de la organización

El usuario de la nube está conectando o bien dos entornos en la nube o un entorno en la nube y un centro de datos. En cualquier caso, la gobernanza general es la intersección de esos dos modelos. Por ejemplo, si se utiliza un enlace a una red dedicada para conectarse a la nube de un centro de datos se ha de dar cuenta de los problemas de gobierno que afectan a ambos escenarios.

En una **nube colectiva** se comparten plataformas con múltiples organizaciones, pero no son públicas, el gobierno se extiende a las relaciones con todos los miembros de la comunidad, no sólo entre el proveedor y el cliente. Es una mezcla de la forma de abordar la gobernanza en la nube pública y en la privada, mediante la que se aprovecharán economías de escala en relación con las herramientas generales de gobernanza y los contratos, no obstante, se puede llegar a un consenso entre los miembros de la comunidad, para realizar ajustes que permitan trabajar como si la nube fuese privada. Esto incluye las relaciones entre los miembros de la comunidad, relaciones financieras, así como en la forma de reaccionar cuando un miembro abandona la comunidad.

2.1.3.3 Intercambios en la gestión de riesgos en la nube

Existen ventajas y desventajas en la administración del riesgo empresarial para los despliegues en la nube. Estos factores son, como era de esperar, más pronunciados en la nube pública que en la nube privada hospedada:

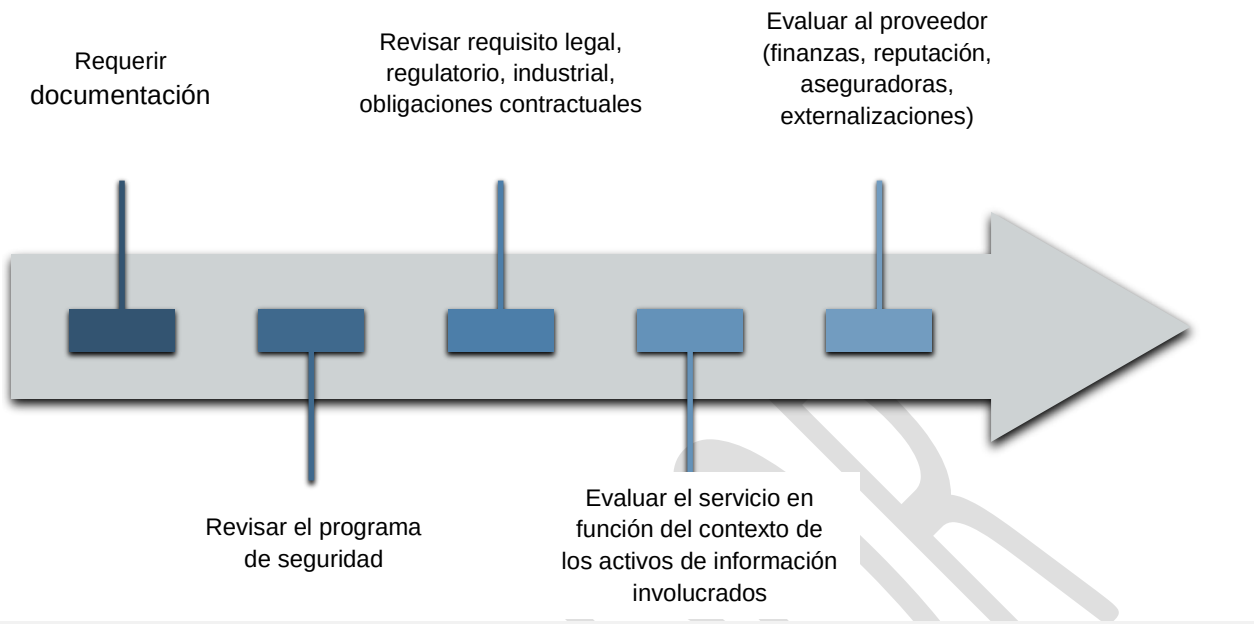
- Hay menos controles físicos sobre los activos, su gestión y procesos. No se puede controlar físicamente la infraestructura o los procesos internos del proveedor.
- Hay una mayor dependencia de los contratos, las auditorías y las evaluaciones, ya que se carece en el día a día de visibilidad o de la gestión.
- Esto introduce la necesidad de una gestión proactiva de las relaciones y de adherencia a los contratos, que se extiende más allá de la firma del contrato inicial y de las auditorías. Los proveedores de la nube evolucionan constantemente sus productos y servicios para seguir siendo competitivos, estas innovaciones continuas pueden exceder, estirar o no estar cubiertas por los acuerdos existentes y evaluaciones.
- Los clientes en la nube tienen una necesidad reducida (y una reducción de costes asociada) para gestionar los riesgos que acepta el proveedor de la nube bajo el modelo de responsabilidad compartida. No se externaliza la responsabilidad de gestionar el riesgo, pero sin duda se puede externalizar la gestión de algunos riesgos.

2.1.3.4 Herramientas para la gestión del riesgo en la nube

Los siguientes procesos ayudan a formar la base de la gestión del riesgo en los despliegues de computación en la nube. Uno de los principios básicos de la gestión de riesgos es que se puede *gestionar, transferir, aceptar o evitar* riesgos. Pero todo ha de comenzar con una evaluación adecuada.

La evaluación del proveedor sienta las bases para el programa de gestión de riesgos en la nube:

- Solicitar o adquirir documentación.
- Revisar los programas de seguridad y la documentación.
- Revisar cualquier requisito legal, regulatorio, contractual y jurisdiccional tanto para el proveedor como usted mismo. (Ver el Dominio 3: Legal para más información)
- Evaluar el servicio contratado en el contexto de sus activos de información.
- Evaluar por separado al proveedor en general, así como las finanzas/estabilidad, reputación y contratistas.



Proceso de Evaluación del Proveedor

Revisar periódicamente las auditorías y evaluaciones para asegurar que están actualizadas:

- No asumir que todos los servicios de un proveedor en particular cumplen con los mismos estándares de auditoría / evaluación. Pueden variar.
- Las evaluaciones periódicas deben programarse y *automatizarse* si es posible.

Después de revisar y comprender qué riesgos gestiona el proveedor de la nube, lo que queda es el riesgo residual. El riesgo residual a menudo se puede gestionar mediante la implementación de controles (e.j. encriptación). La disponibilidad e implementación específica de controles del riesgo varía mucho entre los proveedores en la nube, en particular según los servicios/características, los modelos de servicio y su despliegue. Si después de las evaluaciones y los controles que se hayan implementado todavía hay un riesgo residual las únicas opciones son transferirlo, aceptar el riesgo o evitarlo.

Transferir el riesgo, a menudo mediante un seguro, es un mecanismo imperfecto, especialmente para riesgos de la información. Algunas de las pérdidas financieras asociadas se pueden compensar con un elemento clave perdido, pero no ayudará con la pérdida de un evento secundario (como la pérdida de clientes) – especialmente una pérdida intangible o difícil de cuantificar, como el daño reputacional. Desde la perspectiva de las compañías de seguros, el ciber-seguro es también un campo incipiente sin la profundidad de las tablas actuariales utilizadas por otras formas de seguro, como los de fuego o inundación, e incluso la compensación financiera puede no ajustar el coste asociado con el evento primario perdido. Comprenda los límites.

2.2 Recomendaciones

- Identificar las responsabilidades compartidas de seguridad y gestión del riesgo basadas en la elección del despliegue de la nube y del modelo de servicio. Desarrollar un Marco de trabajo/Modelo de gobernanza de la nube en base a las mejores prácticas de la industria más relevantes, estándares globales, y regulaciones como *CSA CCM, COBIT 5, NIST RMF, ISO/IEC 27017, HIPAA, PCI DSS, EU GDPR*, etc.
- Comprender cómo afecta un contrato a su marco de trabajo/modelo de gobernanza.
    - Obtener y revisar los contratos (y cualquier documento referenciado) antes de llegar a un acuerdo.
    - No asumir que se puede negociar eficazmente un contrato con un proveedor en la nube, pero esto tampoco debería impedir el uso de ese proveedor.
    - Si un contrato no puede ser negociado eficazmente y percibe un riesgo inaceptable, considerar mecanismos alternativos para gestionar este riesgo (e.j. monitorización o encriptación).
- Desarrollar un proceso para las evaluaciones del proveedor en la nube.
    - Esto debería incluir:
        - Revisión del contrato.
        - Revisión del cumplimiento legal reportado por la propia organización.
        - Documentación y políticas.
        - Auditorías y evaluaciones disponibles.
        - Revisiones de servicio adaptándose a los requisitos del cliente.
        - Fuertes políticas de gestión del cambio para monitorizar por parte de la organización de los cambios en el uso de los servicios en la nube.
    - Si las reevaluaciones son posibles deben realizarse de forma programada o automatizarse.
- Los proveedores de servicios en la nube deberían ofrecer un acceso fácil a la documentación y a los informes que se necesiten por los potenciales clientes de cara a las evaluaciones.
    - Por ejemplo, el registro CSA STAR.
- Alinear los requisitos de riesgo con los activos específicos involucrados y la tolerancia al riesgo para esos activos.
- Crear una metodología específica de gestión de riesgos y de aceptación/mitigación de riesgos para evaluar los riesgos de cada solución.
- Usar controles para gestionar los riesgos residuales.
    - Si los riesgos residuales permanecen, elegir aceptar o evitar los riesgos.
- Utilizar herramientas para buscar proveedores autorizados según el tipo de activo (e.j. vinculado a la clasificación de datos), uso de la nube y la gestión.

Dominio 3 Cuestiones Legales, Contratos y Descubrimiento Electrónico

3.0 Introducción

Este dominio destaca algunos de las dificultades legales que surgen al mover datos a la nube; al contratar proveedores de servicios en la nube; y al manejar las solicitudes de descubrimiento electrónico surgidas en procesos judiciales. Nuestra visión general no puede abordar aquí todas las potenciales situaciones legales. Para solucionar sus los problemas concretos, debe contar con asesoramiento legal específico para la (s) jurisdicción (es) en las que tiene la intención de operar y / o en la que residen sus clientes. Además, tenga en cuenta que las leyes y regulaciones cambian con frecuencia y, por lo tanto, debe verificar la relevancia de la información contenida en este dominio antes de confiar por completo en ella. El dominio 3 se refiere principalmente a las implicaciones legales de la computación en la nube pública y las nubes privadas alojadas por terceros. Aunque este dominio incluye algunos aspectos del gobierno de datos y la auditoría o el cumplimiento legal, estos temas se tratan con más profundidad en los dominios 4 y 5.

Las áreas específicas cubiertas en este dominio incluyen lo siguiente:

- Asuntos legales
- Acuerdos de servicios en la nube (contratos)
- Acceso de terceros a documentos electrónicos almacenados en la nube

3.1 Visión general

3.1.1 Marcos legales que rigen la protección de datos y la privacidad

En todo el mundo, muchos países han adoptado marcos legales que establecen obligaciones legales tanto a organizaciones públicas como privadas sobre la protección de la privacidad de los datos personales, así como sobre la seguridad de la información y los sistemas informáticos. La mayoría de estas leyes se basan en parte en los principios de privacidad de la información desarrollados a fines de la década de 1960 y en la de 1970 y posteriormente aclarados y ampliados en el documento “Pautas de Protección de la Privacidad” de la Organización para la Cooperación y el Desarrollo Económico (OCDE).
Bajo estas leyes, el controlador de datos (típicamente la entidad que tiene la relación principal con una persona) tiene prohibido recopilar y procesar datos personales a menos que se cumplan ciertos criterios. Por ejemplo, si la persona ha dado su consentimiento para la recopilación de sus datos para los fines que se han propuesto (el “Sujeto de datos”, entonces el controlador puede recopilar los datos y procesarlos de acuerdo con el consentimiento otorgado. Estas leyes definen numerosas obligaciones legales, como por ejemplo de confidencialidad y de seguridad, para las entidades que acceden a datos personales. Cuando el controlador de datos encarga a un tercero que procese datos del controlador (los procesadores de datos), el controlador sigue siendo responsable ante las personas de la recopilación y el procesamiento de esos datos. Por ello, el controlador de datos debe garantizar que dichos terceros tomen las

medidas de seguridad técnicas y organizativas adecuadas para salvaguardar los datos personales que procesan.

Aunque existe este consenso general en la materia, diversos países del mundo han desarrollado en más detalle su legislación en materia de protección de datos, de forma que ocasionalmente pueden existir conflictos entre estas legislaciones nacionales. Como resultado, los proveedores de la nube y los usuarios de la nube que operan en múltiples regiones tienen dificultades para asegurar el cumplimiento legal con todos los diferentes requisitos locales de protección de datos. En muchos casos, puede ser necesario cumplir simultáneamente con las leyes de diferentes países, de acuerdo con lo siguiente:

- La ubicación del proveedor de la nube
- La ubicación del usuario de la nube
- La ubicación del sujeto de datos
- La ubicación de los servidores
- La jurisdicción legal del contrato entre las partes, que puede ser diferente de la ubicación de cualquiera de las partes involucradas
- Cualquier tratado, acuerdo u otro marco legal existente que sea de aplicación en esas diversas ubicaciones.

Los requisitos legales aplicables variarán tremendamente en función de las distintas jurisdicciones y entidades legales y marcos involucrados.

3.1.1.1 Enfoques comunes

Muchos países han adoptado leyes nacionales u ómnibus (que se aplican a todas las categorías de datos personales) o leyes sectoriales (que se aplican a categorías específicas de datos) que tienen por objeto proteger la privacidad de las personas.

3.1.1.2 Medidas de seguridad requeridas

Estas leyes a menudo contienen disposiciones que requieren la adopción de medidas de seguridad, reconociendo que garantizar la seguridad de los datos personales es esencial para garantizar la protección de la privacidad de las personas. Al mismo tiempo, también se puede esperar que las compañías adopten medidas técnicas, físicas y administrativas razonables para proteger una amplia gama de datos, incluyendo datos personales, datos financieros, secretos comerciales y otros datos sensibles de la empresa contra su pérdida, uso indebido o alteración.

3.1.1.3 Restricciones a las transferencias de datos transfronterizas

Muchos países prohíben o restringen la transferencia de información fuera de sus fronteras. En la mayoría de los casos, la transferencia está permitida solo si el país al que se transfieren los datos ofrece un "nivel adecuado de protección" (según se define en la legislación nacional del país de origen) de la información personal y los derechos de privacidad de las personas cuyos datos se transfieren. El objetivo de este requisito es garantizar que se mantenga el nivel de protección de las personas cuyos datos se transfieren a través de las fronteras al mismo nivel que lo estaban con políticas vigentes antes de la transferencia de datos.
Alternativamente, es posible que el importador y exportador de datos deba firmar un contrato que garantice el mantenimiento de los derechos de privacidad de las personas. Según los países implicados en la transferencia, los requisitos para garantizar esta protección adecuada pueden ser complejos y rigurosos. En algunos casos, puede ser necesario obtener el permiso previo de las Autoridades de Protección de Datos nacionales antes de realizar la transferencia internacional de datos.
Además, algunos países están comenzando a exigir que ciertos datos se almacenen dentro de su territorio. Este es el caso, por ejemplo, de las nuevas leyes de localización de datos de Rusia y China, que requieren que ciertos datos personales de las personas que residen en sus países tengan que estar almacenados dentro de las fronteras del país.

3.1.1.4 Ejemplos regionales

A continuación, hay ejemplos de leyes de privacidad y seguridad de la información y marcos legales vigentes en numerosas partes del mundo.

Australia
En Australia, son dos leyes las que mayormente brindan protección a los consumidores de servicios en la nube: la Ley de Privacidad de1988 (*Privacy Act*) y la Ley de Consumo de Australia de 2010 (*Australian Consumer Law* o ACL). La Ley de Privacidad incluye los 13 Principios de Privacidad (APP) australianos, que se aplican a todas las organizaciones privadas

y sin fines de lucro con una facturación anual mayor a 3 millones de dólares australianos, todos los proveedores privados de servicios de salud y algunas pequeñas empresas.
En febrero de 2017, Australia modificó su Ley de Privacidad de 1988 para exigir que las empresas notifiquen las brechas de seguridad que se produzcan a los residentes australianos afectados y al Comisionado de Información de Australia. Se debe notificar una brecha de seguridad si (a) hay un acceso no autorizado o divulgación de información personal que podría resultar en un daño grave; o (b) se pierde información personal en circunstancias en las que es probable que se produzca un acceso o divulgación no autorizados, y si ocurriera tal acceso o divulgación, es probable que cause daños graves a cualquiera de las personas cuya información ha podido ser accedida o divulgada.
ACL protege a los consumidores contra contratos falsos o engañosos y la mala conducta de los proveedores, como las no notificaciones de brechas. La Ley de Privacidad puede ser aplicada por los clientes australianos, incluso si el proveedor de servicios en la nube tiene su sede en otro lugar, e incluso si el contrato de servicios de nube establece otra jurisdicción.

China

En los últimos años, China ha acelerado el ritmo de adopción de marcos legales relativos a la privacidad y a la seguridad de la información de las personas y de las compañías. Su Ley de Seguridad Cibernética (*Cyber Security Law*) de 2017 regula las operaciones tanto de los operadores de redes como de los operadores de infraestructuras críticas. En mayo de 2017, el gobierno chino publicó su propuesta de Medidas sobre la Seguridad de las Transferencias Transfronterizas de Información Personal e Información Importante (*Measures on the Security of Cross-Border Transfers of Personal Information and Important Data*), que se están evaluando para su posible implementación.
La Ley de Seguridad Cibernética de 2017 exige que los operadores de red cumplan con una serie de requisitos de seguridad, incluido el diseño y la adopción de medidas de seguridad de la información; la formulación de planes de respuesta ante emergencias de seguridad cibernética; y prestar la asistencia y apoyo que sean requerido por los investigadores, cuando sea necesario, para proteger la seguridad nacional y para la investigación de delitos. La ley exige que los proveedores de productos y servicios informen a sus usuarios sobre los defectos y vulnerabilidades conocidos y que denuncien dichos defectos y vulnerabilidades a las autoridades pertinentes.
La Ley de Seguridad Cibernética de 2017 también impone varias obligaciones de seguridad a los operadores de infraestructuras críticas, en aspectos de organización interna, formación de personas, copias de seguridad; respuesta ante emergencias, inspecciones de seguridad y evaluaciones anuales de los riesgos de ciberseguridad; e informar a las autoridades pertinentes. Además, la ley incluye un requisito sobre la localización de datos, que requiere que la información personal y otros datos importantes se almacenen en los territorios de la República Popular de China.
Durante el segundo trimestre de 2017, China emitió un Borrador de Regulaciones sobre Transferencias de Datos Transfronterizas para complementar la Ley de Seguridad Cibernética. Este borrador es más ambicioso que la actual Ley de Seguridad Cibernética, ampliando su alcance, imponiendo nuevos requisitos de revisión de seguridad a las empresas que estén valorando envío de datos al exterior. Expandirían los requisitos de localización de datos e

incrementarían las categorías de información que deben almacenarse solo en territorio chino. En particular, incluirían en esta categoría la información personal y los datos importantes recopilados por cualquier operador de red. El panorama de ciberseguridad y privacidad, tal como se define en la Ley de Seguridad Cibernética, está en evolución y aún no se ha estabilizado.

Japón

En Japón, la Ley de Protección de la Información Personal (*Act on the Protection of Personal Information*, *APPI*) exige que el sector privado proteja la información y los datos personales de forma segura. Existen varias otras leyes nacionales, como la Ley de Protección de la Información Personal en poder de los Órganos Administrativos (*Law on the Protection of Personal Information Held by Administrative Organs*) u otras leyes relativas a sectores específicos, como la industria de la salud. Existen también leyes específicas para profesionales, como la Ley de Médicos Profesionales (*Medical Practitioners' Act*); la Ley de Enfermeras y parteras de la sanidad pública (*Act on Public Health Nurses, Midwives and Nurses*); y la Ley de Farmacéuticos (*Pharmacist Act*), que exigen que estos profesionales de la salud registrados mantengan la confidencialidad de la información del paciente.

La ley *APPI* está admitiendo enmiendas desde septiembre de 2017, limitando la capacidad de transferir datos personales a terceros al requerir el consentimiento previo del sujeto de datos cuyos datos se transfieren. Este consentimiento no es necesario si el país de destino tiene un marco establecido para la protección de la información personal que cumpla con el estándar especificado por la Comisión de Protección de Información Personal.

Rusia

Las leyes rusas de protección de datos contienen restricciones importantes sobre el procesamiento de datos, incluido la necesidad de consentimiento del sujeto de datos para la mayoría de las formas de procesamiento. Sin embargo, el aspecto más importante del marco legal ruso sobre el manejo de la información personal es su ley de localización de datos. Desde septiembre de 2015, las empresas deben almacenar en Rusia los datos personales de los ciudadanos rusos. Roskomnadzor, el regulador ruso de Protección de Datos, ya comenzó a aplicar la ley y bloqueó el acceso a una red social que no tenía presencia física en Rusia, pero que ofrecía una versión en idioma ruso de su servicio.

La Unión Europea (UE) adoptó el Reglamento General de Protección de Datos (*General Data Protection Regulation* o *GDPR*) en 2016, que es vinculante para todos los Estados miembros

de la UE, así como para los miembros del Espacio Económico Europeo (EEE). *GDPR* entra en vigor el 25 de mayo de 2018. La entrada en vigor de *GDPR* en esa fecha deroga la Directiva 95/46/EC sobre Protección de Datos Personales, que ha sido la base legal de las disposiciones de las leyes nacionales de protección de datos de todos los estados miembros de la UE y del EEE.

El otro documento importante que rige los aspectos de la protección de los datos personales en la UE/EEE es la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas. Esta directiva se está eliminando progresivamente y se ha publicado un primer borrador de un Reglamento de Privacidad Electrónica (*E-Privacy Regulation*), que la reemplazaría y que podría entrar en vigor a partir del 25 de mayo de 2018, pero es probable que haya demoras.

Desde el punto de vista de la seguridad, la Directiva de Seguridad de la Información de Red (Directiva NIS, *Network Information Security Directive*) está allanando el camino a requisitos de seguridad más estrictos. Adoptada en 2016, la Directiva *NIS* requiere que los estados miembros de la UE/EEE implementen nuevas leyes de seguridad de la información para la protección de infraestructura crítica y servicios esenciales para mayo de 2018. Los proveedores de servicios en la nube y algunos usuarios de la nube probablemente se verán afectados por las leyes nacionales que implementarán la Directiva NIS.

Regulación general de protección de datos (*GDPR*)

GDPR es directamente vinculante para cualquier corporación que procese los datos de ciudadanos de la UE, y estará bajo la jurisdicción a la autoridad de supervisión de datos o los tribunales del estado miembro que tengan la relación más estrecha con las personas o entidades que manejan esos datos personales.

Aplicabilidad: GDPR se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento en la UE/EEE de un controlador o procesador, independientemente de si el procesamiento se lleva a cabo en la UE/EEE o no. También se aplica al tratamiento de datos personales de personas que se encuentran en la UE/EEE por un controlador o un procesador no establecido en la UE/EEE si el procesamiento se produce en (a) la oferta de bienes o servicios, independientemente de si son de pago o no; o (b) el seguimiento del comportamiento de un interesado, cuando el comportamiento se produce dentro de la UE/EEE.

Legalidad: El procesamiento de datos personales está permitido solo si (a) el interesado ha dado libremente una evidencia específica, informada e inequívoca de su consentimiento para el procesamiento de sus datos personales, o (b) el procesamiento está autorizado por una disposición legal.

Obligaciones de responsabilidad: GDPR ha creado numerosas obligaciones para las empresas. Por ejemplo, *GDPR* requiere que las compañías mantengan registros de sus actividades de procesamiento de datos. El procesamiento de ciertas categorías de datos requiere realizar una "Evaluación de Impacto de Privacidad" (*PIA*, *Privacy Impact Assessment*) previa. Se espera que las compañías desarrollen y operen sus productos y servicios de acuerdo con los principios de Privacidad por Diseño y Privacidad por Defecto.

Derechos de sujetos de datos: Los sujetos de datos tienen derecho a la información sobre el procesamiento de sus datos: el derecho a oponerse a ciertos usos de sus datos personales; los derechos de rectificación y borrado de datos; ser compensado por los daños sufridos como

resultado del procesamiento de datos ilegal; el derecho al olvido; y el derecho a la portabilidad de datos. La existencia de estos derechos afecta significativamente las relaciones del servicio en la nube.

Restricciones transfronterizas de transferencia de datos: Está prohibida la transferencia de datos personales fuera de la UE/EEE a países que no ofrecen un nivel similar de protección de datos personales y derechos de privacidad. Para demostrar que ofrecerá tal "nivel de protección adecuado" requerido, una empresa puede usar uno de varios métodos, como aplicar cláusulas contractuales estándar (SCC, *Standard Contractual Clauses*), adherirse al acuerdo EU-USA *Privacy Shield*, obtener la certificación de sus reglas corporativas (*BCRs, Binding Corporate Rules*), o cumplir con algún Código sectorial de Conducta aprobado (*Code of Conduct*) u otro mecanismo de certificación aprobado. En casos raros, la transferencia puede realizarse con el consentimiento explícito e informado del sujeto de datos o si se aplican otras excepciones.

Brechas de seguridad: GDPR requiere que las empresas informen que han sufrido una brecha de la seguridad. Los requisitos de presentación de informes están basados en el riesgo y existen diferentes requisitos para informar el incumplimiento a la Autoridad de Supervisión y a sujetos de datos afectados por la brecha. Las infracciones deben ser reportadas dentro de las 72 horas posteriores a que la compañía conozca la ocurrencia del incidente.

Diferencias entre los Estados Miembros: Hay numerosos casos en que cada estado miembro puede adoptar sus propias reglas. Por ejemplo, Alemania requiere que se designe un Delegado de Protección de Datos (DPO, *Data Protection Officer*) si la compañía tiene más de nueve empleados.

Sanciones: El incumplimiento de *GDPR* exponen a una compañía a sanciones significativas. Estas sanciones pueden alcanzar hasta el cuatro por ciento de su facturación o ingreso bruto global, o hasta 20 millones de euros.

Directiva de Seguridad de la Información de Red (Directiva *NIS*)

La Directiva *NIS* entró en vigor en agosto de 2016, requiriendo que cada estado miembro de la UE/EEE complete la trasposición de la Directiva en su legislación nacional en mayo de 2018. La Directiva NIS establece un marco para tener confianza a cierto nivel de que las redes y sistemas de información resistirán acciones que comprometen bien la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados; bien los servicios que son ofrecidos o accesibles a través de esas redes y sistemas de información.

La Directiva *NIS* requiere que las leyes nacionales de los estados miembros impongan requisitos de seguridad de la red y de la información a los operadores de servicios esenciales, es decir, entidades que proporcionan un servicio esencial para el mantenimiento de actividades sociales y/o económicas críticas; y cuando un incidente en la red y los sistemas de información de ese servicio tendría efectos perturbadores significativos en la provisión de ese servicio. Los requisitos que deben ser incluidos en las leyes nacionales incluyen los siguientes:

- Tomar medidas técnicas y organizativas para gestionar los riesgos que suponen para la seguridad de las redes y los sistemas de información utilizados en sus operaciones.
- Tomar las medidas apropiadas para prevenir y minimizar el impacto de incidentes que afecten la seguridad de las redes y los sistemas de información utilizados para la

provisión de tales servicios esenciales, para facilitar la continuación en la prestación de dichos servicios.
- Notificar, sin demora indebida, a las autoridades u organismos competentes los incidentes que tengan un impacto significativo en la continuidad de los servicios esenciales que prestan.
- Proporcionar la información necesaria para evaluar la seguridad de sus redes y sistemas de información.
- Proporcionar evidencia de la implementación efectiva de las políticas de seguridad como, por ejemplo, los resultados de una auditoría de seguridad.

La Directiva *NIS* también exige que las leyes nacionales de los estados miembros impongan requisitos de seguridad de la red y de la información a los proveedores de servicios digitales, como los *marketplaces* (por ejemplo, plataformas de comercio electrónico), servicios de computación en la nube; y motores de búsqueda web. Los proveedores de servicios digitales establecidos fuera de la UE que prestan servicios dentro de la UE entran dentro del alcance de la Directiva *NIS*.
Las legislaciones nacionales de los estados miembros también deberán exigir a los proveedores de servicios digitales que identifiquen y tomen medidas técnicas y organizativas apropiadas y proporcionadas para gestionar los riesgos que suponen para la seguridad de las redes y los sistemas de información que utilizan, como la gestión de incidentes, la gestión de continuidad del negocio, supervisión, auditoría y pruebas, y cumplimiento con estándares internacionales.
Las legislaciones nacionales de los Estados miembros tendrán que exigir a los proveedores de servicios digitales que tomen medidas para prevenir y minimizar el impacto de los incidentes. Deberán notificar a las autoridades u organismos competentes, sin demora indebida, cualquier incidente que tenga un impacto sustancial en la prestación de un servicio, incluida información suficiente para permitir que la autoridad o el organismo competente determine la importancia de cualquier impacto transfronterizo. Si un operador de servicios esenciales se apoya en un proveedor de servicios digitales externo para un servicio que es esencial, el operador deberá notificar cualquier impacto significativo en la continuidad de los servicios esenciales debido a un incidente que afecte al proveedor de servicios digitales.

América Central y del Sur
Los países de América Central y del Sur también están adoptando leyes de protección de datos a un ritmo rápido. Cada una de estas leyes incluye un requisito de seguridad e impone al

controlador de datos la carga de garantizar la protección y seguridad de los datos personales dondequiera que se encuentren y especialmente cuando se transfieren a un tercero.
Por ejemplo, Argentina, Chile, Colombia, México, Perú y Uruguay aprobaron leyes de protección de datos inspiradas principalmente en la directiva europea 95/46/EC, y pueden incluir referencias al Marco de Privacidad de APEC. La ley federal de protección de datos de México incluye disposiciones sobre comunicación de brechas de seguridad.

América del Norte: Estados Unidos
Debido a su enfoque sectorial, Estados Unidos tiene cientos de reglamentaciones federales, estatales y locales, que tratan desde los detalles de un plan de seguridad de la información hasta las reglas para comunicar brechas de seguridad. Por ello, las organizaciones que hacen negocios en los Estados Unidos o recopilan o procesan información personal o de otro tipo de personas o empresas ubicadas en los Estados Unidos, están sujetas a menudo a diversas leyes de seguridad de la información o privacidad en los diversos ámbitos federal, estatal o local. La variedad y complejidad de estas reglas pueden ser desalentadoras tanto para los proveedores o usuarios de servicios en la nube como para los proveedores de servicios y subcontratistas que participan en la provisión de estos servicios.

Leyes federales de EE. UU.
Numerosas leyes federales y sus regulaciones relacionadas, como la Ley Gramm-Leach-Bliley (*GLBA*), la Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996 (*HIPAA*, *Health Insurance Portability and Accountability Act*) y la Ley de Protección de la Privacidad en Línea para Menores de 1998 (*COPPA*, *Children's Online Privacy Protection Act*), contienen disposiciones relativas a la privacidad y la seguridad de la información personal. Las disposiciones relacionadas con la seguridad obligan a las empresas a adoptar medidas de seguridad razonables al procesar datos personales.
La mayoría de estas leyes requieren que las compañías tomen medidas de seguridad cuando contraten subcontratistas y proveedores de servicios, en tanto que las organizaciones se hacen responsables de los actos de sus subcontratistas. Por ejemplo, los requisitos de seguridad y privacidad de *GLBA* e *HIPAA* exigen que las organizaciones sujetas a ellas obliguen mediante contrato escrito a sus subcontratistas a usar medidas de seguridad razonables y cumplir con las disposiciones de privacidad de datos.

Leyes estatales de los Estados Unidos
Además de las leyes y regulaciones federales, la mayoría de los estados de EE. UU. tienen leyes relacionadas con la privacidad y / o la seguridad de los datos. Estas leyes se aplican a cualquier entidad que recopile o procese información personal (como se define de forma restrictiva en la legislación aplicable) de las personas que residen en ese estado, independientemente de dónde se almacenan los datos en los Estados Unidos.
Algunas leyes estatales son elaboradas. Ver, por ejemplo, los extensos requisitos bajo "Estándares para la Protección de la Información Personal de los Residentes de la Mancomunidad" ("*Standards for the Protection of Personal Information of Residents of the Commonwealth*") de Massachusetts o 201 *CMR* 17.00. Otras leyes estatales son más generalistas (ver la ley del estado de Washington *RCW* 19.255.020(2)(b) que asigna sanciones

sobre la base del cumplimiento) y un pequeño número de leyes estatales hacen referencia a otras normas específicas (como la seguridad de datos de la industria de tarjetas de pago Estándar, *PCI-DSS* o "*Payment Card Industry Data Security Standard*" mencionado anteriormente). La mayoría de las leyes estatales que abordan los problemas de seguridad de la información requieren que la compañía tenga un contrato escrito con el proveedor del servicio con medidas de seguridad razonables. Numerosas leyes estatales también exigen que las empresas brinden la protección adecuada de la privacidad y la seguridad de los datos personales, y requieren que sus proveedores de servicios hagan lo mismo.

Leyes de reporte de brechas de seguridad

Numerosas leyes o normas federales de seguridad, como las que rigen para los proveedores de servicios de salud y la mayoría de las leyes estatales, exigen que las entidades que hayan tenido brechas de seguridad que hayan podido comprometer categorías específicas de datos, como información de salud del paciente (*PHI*, *Patient Health Information*) notifiquen con prontitud la existencia de esta brecha de Seguridad a las personas afectadas, y en muchos casos, a agencias estatales o federales.

El correcto conocimiento y la comprensión de estas leyes son fundamentales tanto para los clientes y proveedores de servicios en la nube, ya que las brechas de seguridad a menudo derivan en sobrecostes significativos. Por ejemplo, los costes legales derivados de posibles demandas colectivas. Algunas de las últimas brechas de seguridad han afectado a cientos de millones de personas, y los costos legales y daños derivados de las brechas que las empresas afectadas han debido afrontar también han sido importantes.

Agencias federales y estatales

Además de las leyes y regulaciones específicas, los proveedores y usuarios de la nube deben conocer la "ley común de privacidad y seguridad", el apodo dado al conjunto de instrucciones y consentimientos que publicados por las agencias gubernamentales federales y estatales tras completar sus investigaciones sobre incidentes y eventos de seguridad.

Durante casi 20 años, agencias del gobierno de Estados Unidos como la Comisión Federal de Comercio (FTC) y los Fiscales Generales Estatales han utilizado los poderes que les otorgan las leyes federales o estatales de lucha contra las "prácticas desleales y engañosas" para llevar a cabo investigaciones en empresas cuyas prácticas de privacidad o seguridad eran inconsistentes con sus declaraciones públicas, lo que calificaba sus prácticas como injustas o engañosas. Los numerosos decretos de consentimiento emitidos sea por la FTC de acuerdo con la Sección 5 de la Ley de la FTC: Actos o prácticas desleales o engañosos, sea por los Fiscales Generales Estatales en casos similares según las respectivas leyes de prácticas desleales y engañosas de sus estados—como resultados de las investigaciones de seguridad realizadas por estas entidades, ofrecen orientaciones de interés importante sobre los puntos de vista y objetivos que mantienen las agencias federales o estatales con respecto a la recopilación, el uso y la protección de la información personal.

3.1.2 Contratación y selección de proveedores

Incluso para actividades no sujetas a regulación, los clientes de la nube pueden tener la obligación contractual de proteger la información personal de sus propios clientes, contactos o empleados para asegurar que los datos no se utilicen con fines distintos a los previstos ni se divulguen o compartan con terceras. Esta obligación puede derivarse, por ejemplo, de los Términos y Condiciones o de la Declaración de Privacidad propias de la empresa, o de los contratos que la empresa ha suscrito con terceros. Por ejemplo, un procesador de datos puede estar obligado por las condiciones de su Acuerdo de Servicios a procesar datos personales, pero solo para ciertos fines. Alternativamente, la empresa puede tener suscrito contratos (como acuerdos de servicio) con sus clientes, en los que ha asumido compromisos específicos para proteger datos (personales o de la compañía), limitar su uso, garantizar su seguridad, usar encriptación, etc. La organización debe ser capaz de garantizar que, si aloja datos bajo su control en la nube, tendrá la capacidad continua de cumplir con las promesas y los compromisos asumidos en sus avisos de privacidad u otros contratos. Los datos en la nube deben usarse solo para los fines para los que se recopilaron.

Si los avisos de privacidad permiten a los sujetos de datos individuales tener acceso a sus datos personales, modificarlos o eliminarlos, el proveedor de servicios en la nube también debe permitir que estos derechos de acceso, modificación y eliminación se puedan ejercer tan eficazmente como en una relación sin nube.

Cuando los datos o las operaciones se transfieren a la nube, la responsabilidad de proteger y asegurar esos datos generalmente sigue siendo del controlador de esos datos, incluso si en algunas circunstancias esta responsabilidad pudiera estar compartida con otras entidades. Incluso si se apoya en un tercero para alojar o procesar sus datos, el controlador de datos sigue siendo responsable de cualquier pérdida, daño o mal uso de los mismos. Por lo tanto, es prudente y puede ser requerido por ley o regulación que el controlador de datos y el proveedor de la nube suscriban un acuerdo formal escrito que defina claramente las funciones, las expectativas de las partes y la asignación de las numerosas responsabilidades asociadas a estos datos. Tal acuerdo también debe identificar claramente los usos permitidos y prohibidos de los datos, y las medidas que se tomarán si los datos fuesen robados o comprometidos.

Las leyes, regulaciones, estándares y las mejores prácticas relacionadas discutidas anteriormente también requieren que los controladores de datos se aseguren de que estas obligaciones se cumplan mediante las diligencias debidas (*due diligence*: antes de la ejecución del contrato) o auditorías de seguridad (durante la ejecución del contrato).

3.1.2.1 Diligencia debida (en inglés *Due Diligence*) interna

Las empresas son controladores de los datos que se les han confiado. Como se vio anteriormente, numerosas leyes, regulaciones y contratos prohíben, restringen y limitan la revelación y transferencia de datos a un tercero. Por ejemplo, la información de salud protegida bajo *HIPAA* no se puede transferir a un tercero o "socio comercial" sin imponer obligaciones específicas al receptor. Además, si los datos se originan en un país extranjero, es probable que haya obstáculos significativos para una transferencia internacional con destino en países que se considera que no brinda "protección adecuada" a los derechos de privacidad y datos personales.

Antes de suscribir la prestación de servicio de computación en la nube, tanto el proveedor del servicio en la nube como su cliente deben evaluar sus propias prácticas, necesidades y

restricciones para identificar las barreras legales existentes y los requisitos legales que han de satisfacerse. Por ejemplo, el cliente de la nube debe determinar si su modelo de negocio permite el uso de servicios de computación en la nube y en qué condiciones. La naturaleza de su negocio podría ser tal que la ley le impida ceder el control de sus propios datos corporativos. Un proveedor en la nube puede considerar prudente realizar una evaluación previa del coste de prestar servicio a ciertos mercados que podrían estar sujetos a requisitos legales con los que el vendedor no está familiarizado.

Un cliente de la nube debe investigar si ha está sujeto a acuerdos de confidencialidad o de uso de datos que podrían restringir la transferencia de datos a terceros, incluso si estos terceros son proveedores de servicios. Si la compañía, o posible cliente de la nube, ha firmado acuerdos de confidencialidad para proteger la información personal o secretos comerciales, probablemente dichos acuerdos prohíban la subcontratación de un proveedor sin permiso previo del propietario de los datos. Un acuerdo de uso de datos suscrito por la empresa puede requerir el consentimiento explícito del cliente para poder subcontratar el procesamiento de los datos del cliente. Esa restricción sería aplicable en la mayoría de los casos a las transferencias de datos a un proveedor de servicios en la nube. En estas circunstancias, mover datos a una nube sin el permiso previo del cliente (propietario de los datos) provocaría un incumplimiento en el acuerdo de uso de datos con ese cliente.

En otros casos, los datos pueden ser tan delicados o confidenciales que no deberían simplemente transferirse a un servicio en la nube, o transferirse adoptando precauciones importantes. Este podría ser el caso, por ejemplo, de los archivos que se refieren a proyectos de gran importancia, como los planes de I+D, o los planes para una próxima salida a bolsa, fusión o adquisición.

3.1.2.2 Monitoreo, prueba y actualización

El entorno de la nube no es estático. Evoluciona y las partes involucradas deben adaptarse a esta evolución. Se recomienda el monitoreo, prueba y evaluación periódica de los servicios en la nube para asegurarse de que las medidas de privacidad y seguridad requeridas siguen aplicándose correctamente. Sin pruebas periódicas de servicios en la nube, la eficacia del control puede verse comprometida sin que sea detectado.

Además, el panorama legal, normativo y técnico en el que opera cualquier empresa cambia rápidamente. Las nuevas amenazas de seguridad, las nuevas leyes y los nuevos requisitos de cumplimiento deben abordarse con prontitud. Tanto los clientes como los proveedores de la nube deben mantenerse al tanto de los requisitos legales, normativos, contractuales u otros y asegurarse de que sus operaciones sigan cumpliendo con las leyes y regulaciones aplicables, y que las medidas de seguridad continúen evolucionando a medida que surjan nuevas tecnologías.

3.1.2.3 Diligencia debida externa

Antes de suscribir cualquier contrato, una parte fundamental de la diligencia debida debe incluir la solicitud y revisión de todos los aspectos relevantes de las operaciones de la otra parte. En este caso, los del proveedor o vendedor de nube propuesto. Un cliente de servicios en la nube necesita asegurarse de que comprende la aplicación o servicio concreto que está

contemplando adquirir. El alcance de la diligencia debida y el tiempo invertido dependerán de las circunstancias. El proceso puede completar se un día, una semana o un mes dependiendo de las necesidades específicas del cliente, la naturaleza de los datos a procesar, la sensibilidad e intensidad del procesamiento y otros factores que harían que una operación particular sea rutinaria o altamente sensible.

Por lo tanto, dependiendo de la naturaleza del proyecto propuesto, la diligencia debida puede implicar la evaluación de la naturaleza y la integridad de los servicios prestados, la reputación de la calidad o la estabilidad del servicio, la disponibilidad de niveles de mantenimiento por el proveedor, la capacidad de respuesta de servicio al cliente, la velocidad de la red y la ubicación de los centros de datos. Entrevistar a otros clientes puede proporcionar información valiosa. También puede ayudar en la toma de decisión la revisión de existencia de demandas, pleitos y reclamaciones hechos al proveedor de servicios en la nube y buscar información disponible de fuentes abierta para evaluar su reputación.

En la mayoría de los casos, el cliente de la nube querrá evaluar al menos el nivel de servicio aplicable, los acuerdos legales y de términos de servicio, las políticas de privacidad, la política de comunicaciones de seguridad; y las evidencias facilitadas para demostrar el cumplimiento de los requisitos legales aplicables (por ejemplo, requisitos sobre los registros generados) para garantizar que las condiciones de servicio establecidos por el proveedor de la nube son adecuadas para el cliente. Dependiendo de la profundidad e intensidad esperada de la diligencia debida, los temas a investigar pueden incluir lo siguiente:

- ¿El servicio será fiable y fácil de usar?
- ¿Cómo se usarán los servidores para procesar los datos?
- ¿Cómo operará y se proporcionará el servicio?
- ¿Se almacenarán mis datos con los datos de otros clientes?
- ¿Cómo se protegerán los datos contra intrusiones o desastres?
- ¿Cómo evolucionará el precio a lo largo del tiempo?
- ¿El proveedor de la nube satisfará mis necesidades de capacidad de cálculo y de control de acceso de la empresa?
- ¿El vendedor de la nube seguirá funcionando durante los próximos años? ¿Cuál es su perfil financiero?
- ¿Qué niveles de servicio se ofrecerán?
- ¿Qué medidas de seguridad se usan?
- ¿Qué sucederá en caso de una brecha de seguridad?

La revisión de todos los términos y condiciones del acuerdo de servicios en la nube (incluidos todos los anexos, adjuntos y apéndices) es una buena diligencia debida para cualquier proyecto nuevo. Es especialmente crítico para los servicios en la nube, ya que algunos términos y condiciones del proveedor no podrán ser negociados por el cliente. En esos casos, el cliente deberá tomar una decisión informada sobre si el servicio se suscribe o no.

3.1.2.4 Negociaciones de contratos

Los contratos en la nube pretenden describir con precisión la interpretación de sus términos por todas las partes. Las partes pueden desear implantar contractualmente numerosas

precauciones y medidas para reducir su exposición a riesgos legales, comerciales y de reputación derivados del uso de servicios en la nube.
El contacto propuesto siempre debe revisarse cuidadosamente, incluso cuando se expresa que sus condiciones no son negociables. Por una parte, es posible que en realidad sí pudieran negociar algunos cambios. Por otra parte, aun cuando efectivamente no fuese objeto de negociación, cada comprador de servicios en la nube debe comprender las consecuencias e implicaciones derivadas del compromiso que está asumiendo. Un contrato no negociable probablemente carezca de algunas protecciones habitualmente necesarias para un cliente típico. En este caso, el cliente debe sopesar los riesgos de renunciar a estas protecciones contra los posibles beneficios.

3.1.2.5 Confianza en auditorías y declaraciones de terceros

Las auditorías y el cumplimiento se tratan con más detalle en el Dominio 4, pero hay dos consideraciones que pueden afectar los requisitos contractuales y legales. En la computación en la nube, las auditorías y certificaciones de terceros se utilizan con frecuencia para asegurar que la infraestructura del proveedor de la nube cumple con los marcos de referencia auditados o certificados, lo que permite que el cliente asegure a su vez el cumplimiento legal de los servicios que desarrolla a partir de los servicios en la nube. Es fundamental que un proveedor publique y que el cliente evalúe el alcance de la evaluación de terceros y qué funciones y servicios se incluyen en la misma.
Por ejemplo, la última versión del servicio de almacenamiento de un proveedor de servicios en la nube puede no ser compatible con *HIPAA* (y por lo tanto el proveedor puede no estar en condiciones de firmar un acuerdo de servicios de almacenamiento para un cliente que requiera cumplimiento con *HIPAA*), aunque muchas de sus otras ofertas de servicios sí pudieran ser utilizados de manera compatible con *HIPAA*.

3.1.3 Descubrimiento electrónico

Las reglas de los EE. UU. sobre "descubrimiento" --el proceso mediante el cual la parte contraria en un proceso legal obtiene documentos privados para su uso en el proceso-- cubre una amplia variedad de posibles documentos. En particular, el descubrimiento no tiene por qué limitarse a documentos que desde el principio se sabe que serán admisibles como prueba en el tribunal; Más bien, el descubrimiento se aplicará a todos los documentos razonablemente identificados como posibles evidencias admisibles (evidencias que son simultáneamente relevante y probatoria por una parte). Ver la Regla 26, Reglas Federales de Procedimiento Civil (*FRCP*).
En los últimos años, muchos litigantes han eliminado, perdido o modificado evidencias, lo que resultó perjudicial para la defensa de su caso. En estos casos, las Reglas Federales de Procedimiento Civil permiten, entre otras sanciones, indemnizar económicamente a la parte no responsable de la destrucción; en algunos casos, un jurado puede ser advertido sobre la existencia de una "inferencia adversa" (es decir, se informaría al jurado de que asuma que la evidencia no disponible contenía la información menos favorable a la posición de la parte que la destruyó). Ver la Regla 37, *FRCP*. Como resultado de la jurisprudencia en la materia, *FRCP* se

modificó para aclarar las obligaciones de las partes, especialmente en el caso de la información almacenada electrónicamente (*ESI*, *Electronically Stored Information*).
Dado que la nube se convertirá en el repositorio de la mayoría de *ESI* necesaria en un litigio o una investigación, los proveedores de servicios en la nube y sus clientes deben planificar cuidadosamente cómo podrán identificar todos los documentos que pertenecen a un caso, con el fin de poder cumplir con los estrictos los requisitos impuestos por *FRCP* 26 con respecto a *ESI*, y los equivalentes a estas leyes en cada estado. A este respecto, el cliente y el proveedor del servicio en la nube deben tener en cuenta los siguientes problemas cuando un cliente está sujeto a una solicitud de descubrimiento y el proveedor de nube dispone de datos potencialmente relevantes.

3.1.3.1 Posesión, custodia y control

En la mayoría de las jurisdicciones de los Estados Unidos, la obligación de una parte de aportar la información relevante se limita a los documentos y datos que se encuentran en su posesión, custodia o control. Que esta información relevante esté almacenada en un tercero, como un proveedor de la nube, generalmente no obvia la obligación de aportar esta información. Sin embargo, no todos los datos alojados en un proveedor de la nube pueden estar bajo el control dl cliente (por ejemplo, los sistemas para uso en recuperación de desastres o ciertos metadatos creados y mantenidos por el proveedor de la nube para operar sus propios servicios). La definición al inicio del contrato de los datos que sí están y que no están disponibles para el cliente puede interesar tanto al cliente como al proveedor. Las obligaciones del proveedor de servicios en la nube como procesador de datos con respecto a la producción de información en respuesta a un proceso legal son cuestiones que cada jurisdicción debe resolver.

3.1.3.2 Aplicaciones y entornos relevantes de la nube

En ocasiones, una aplicación o entorno de nube concreta podría ser relevante para resolver un litigio. En estas circunstancias, esa aplicación o entorno probablemente no estarán bajo el control del cliente y requieren que se envíe una citación, requerimiento judicial u otro documento dirigido directamente al proveedor.

3.1.3.3 Herramientas de búsqueda y descubrimiento electrónico

En un entorno de nube, un cliente puede no ser capaz de aplicar o usar las herramientas de descubrimiento electrónico que utiliza en su propio entorno. Además, un cliente puede no tener las herramientas o los derechos administrativos suficientes para buscar o acceder a todos los datos alojados en la nube. Por ejemplo, mientras un cliente puede acceder buscar simultáneamente en varias cuentas de correo electrónico ubicadas en su servicio local, es posible que no tenga esta capacidad con las cuentas de correo electrónico alojadas en la nube. Por ello, los clientes deben tener en cuenta los posibles gastos y periodos de obtención de información adicionales derivados de su acceso limitado. Este problema puede resolverse por adelantado si el cliente identifica esta necesidad y pueda negociar o complementar el acuerdo de servicio en la nube cuando se suscribe por primera vez. De lo contrario, el cliente de la nube puede no tener más opción que abordar cada caso individualmente y, por lo tanto, podría tener que pagar por servicios adicionales del proveedor de la nube.

3.1.3.4 Conservación y retención

Según el servicio en la nube y su modelo de implementación que utiliza un cliente, la conservación de la información en la nube puede ser no tener cambios frente a las infraestructuras de TI clásicas, o puede ser mucho más complejo.
En los Estados Unidos, las partes generalmente están obligadas a tomar medidas razonables para prevenir la destrucción o modificación de datos en su posesión, custodia o control que sabe, o debería razonablemente saber, que son relevantes para una causa judicial pendiente o previsible o para una investigación oficial (Esto a menudo se denomina "retención por litigio" o "*litigation hold*" en la destrucción de documentos). Estas cuestiones se abordan de manera amplia por la Norma Federal de Procedimiento Civil 37, aunque existen infinidad de decisiones jurisdiccionales que se aplican a posibles partes en litigio. En la Unión Europea, la preservación de la información se rige por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006. Japón, Corea del Sur y Singapur tienen iniciativas similares de protección de la información. En América del Sur, Brasil y Argentina cuentan con el Proyecto de ley Azeredo y la Ley de retención de datos de Argentina de 2004, Ley No. 25.873, respectivamente.

3.1.3.5 Leyes de retención de datos y obligaciones de mantenimiento de registros

Además de las obligaciones de preservación de datos derivadas de las leyes de los EE. UU. con respecto al descubrimiento electrónico, las empresas deben ser conscientes de que la existencia de leyes de retención de datos que requieren que las entidades sujetas a las mismas retengan datos durante períodos de tiempo establecidos.
Costos y almacenamiento: La conservación de datos puede requerir que se retengan grandes volúmenes de datos durante períodos prolongados. Los clientes deben considerar estas preguntas y determinar los riesgos asumibles en el campo antes de moverse a la nube:

- ¿Cuáles son las implicaciones de la retención de datos, de acuerdo con el acuerdo de nivel de servicio (SLA) suscrito?
- ¿Qué sucede si los periodos de tiempo de conservación requeridos legalmente exceden el tiempo de conservación previsto en los términos del SLA?
- Si el cliente conserva los datos en la nube o en sus instalaciones, ¿Quién paga el almacenamiento extendido? ¿A qué costo?
- ¿Tiene el cliente la capacidad de almacenamiento de estos datos, de acuerdo con el SLA suscrito?
- ¿Puede el cliente descargar efectivamente los datos de manera forense para que puedan conservarse en soportes no inmediatamente accesibles?

Alcance de la conservación: Una parte en un litigio tiene derecho únicamente a los datos alojados en la nube que contienen, o se calcula razonablemente que conducen a, información relevante y probatoria para el problema legal en cuestión, pero no tiene derecho a absolutamente todos los datos en la nube o en la aplicación (el límite exacto de este acceso probablemente se resuelva en el marco de cada causa particular). Sin embargo, si el cliente no tiene la capacidad de conservar solo la información o los datos relevantes con suficiente granularidad, es posible que se requiera conservar la información en exceso para garantizar

una conservación razonable, dependiendo de la investigación. Luego, se examina el total de la información para determinar qué debe y qué no debe entregarse como parte del proceso de descubrimiento electrónico. Este proceso, denominado revisión de documentos o revisión de privilegios, puede ser realizado por el equipo jurídico del cliente o, en algunos casos, con la ayuda de software específico especializado. La forma en que se catalogan las cada vez más voluminosas de cantidades de información que se generan en un proceso de descubrimiento electrónico es actualmente objeto de I+D tanto legal como técnica.

Almacenamiento dinámico y compartido: La carga de trabajo y recursos adicionales para preservar los datos en la nube puede ser relativamente modesta si el cliente tiene espacio para mantenerla en su lugar, si los datos son relativamente estáticos y si las personas con acceso son limitadas y tienen la formación necesaria sobre cómo conservar los datos. Sin embargo, en un entorno de nube que sistemáticamente modifica o purga los datos en su plataforma, o en el que los datos se comparten con personas que desconocen la necesidad de conservación de datos, la necesaria conservación será más difícil. Después de que un cliente determina qué información es relevante y necesita ser conservada, el cliente puede necesitar efectuar actividades específicas con el proveedor para determinar la manera razonable de conservar dicha información.

3.1.3.6 Recopilación de información

Debido a la posible falta de control administrativo que un cliente tiene sobre sus datos en la nube, la recolección de datos desde ese entorno puede ser más difícil, más lenta y más costosa que su equivalente desde servicios en red local. En particular, un cliente puede no tener el mismo nivel de visibilidad de sus datos en la nube, y puede tener dificultades para comparar los datos recopilados con los datos existentes en la nube para determinar que la exportación fue razonablemente completa y precisa.

Acceso y ancho de banda: En la mayoría de los casos, el volumen de acceso de un cliente a sus datos en la nube está determinado como parte de su *SLA*. Esto puede limitar su capacidad de recopilar grandes volúmenes de datos de forma rápida y con calidad forense (es decir, conservando todos los metadatos razonablemente relevantes). Clientes y proveedores de servicios en la nube deberían considerar este problema desde el comienzo de su relación y establecer un protocolo (y el costo asociado del mismo) para el acceso extraordinario en el marco de procesos legales. En ausencia de estos acuerdos, los clientes deben asumir los tiempos y costos adicionales implicados por la recopilación de datos desde la nube cuando así se lo solicitan las otras partes y los tribunales en el marco de procesos legales. Tenga en cuenta que *FRCP* 26 (b) (2) (B) excusa a un litigante que puede demostrar que la información solicitada no es razonablemente accesible.

Sin embargo, un tribunal puede ordenar la realización incondicional de actividades de descubrimiento electrónico de dichas fuentes si la parte solicitante puede mostrar por qué esta información es necesaria y no puede obtenerse de otra manera.

Como elemento adicional a valorar, el derecho de acceso de un cliente puede proporcionarle acceso al total de datos, pero quizás no proporciona el grado de funcionalidad que más adecuado para una situación dada. Por ejemplo, un cliente puede tener acceso al histórico de tres años de datos transaccionales comerciales, pero solo puede descargar los datos en bloques de máximo dos semanas debido a restricciones de funcionalidad. Además, un cliente

puede un acceso o visión limitada de los metadatos. Un cliente prudente debe aprender qué es posible con las herramientas disponibles antes de que sea necesario usarlas como parte de un proceso judicial.

Forense: La obtención de imágenes bit a bit de una fuente de datos en la nube es generalmente difícil o imposible. Por razones de seguridad obvias, los proveedores son reacios a permitir el acceso físico a su hardware, particularmente en un entorno multiusuario donde un cliente puede obtener de esta forma acceso a los datos de otros clientes. Incluso en una nube privada, los análisis forenses pueden ser extremadamente difíciles, y es posible que los clientes tengan que notificar estas limitaciones al abogado de la otra parte o a los tribunales. (Nuevamente, *FRCP* 26 (b) (2) (B) puede proporcionar alivio de tales cargas excesivas). Afortunadamente, este tipo de análisis forense rara vez se justifica en la computación en la nube, porque el entorno a menudo consiste en una jerarquía de datos estructurados o virtualización que no proporciona información relevante adicional significativa en un análisis bit por bit.

Integridad razonable: Un cliente que deba atender una solicitud de descubrimiento electrónico debe tomar medidas razonables para validar que la recopilación de datos realizada desde de su proveedor de nube es completa y precisa, especialmente cuando los procedimientos ordinarios para atender la solicitud no están disponibles o no son suficientes y se han utilizado medidas específicas en el marco del proceso legal para obtener la información. Este proceso de recopilación de datos de la nube es independiente y distinto del proceso de verificación de que los datos almacenados en la nube sean precisos, autenticados o admisibles.

Límites a la accesibilidad: Debido a las diferencias en la forma en que se almacenan los datos y los derechos y privilegios de acceso disponibles para el propietario de los datos, hay casos en los que un cliente no puede acceder a todos sus datos almacenados en una nube. El cliente y el proveedor de la nube pueden tener que analizar la solicitud de información y las estructuras de datos que serán manejadas para atenderla por relevancia, materialidad, proporcionalidad o accesibilidad cuando responden a una solicitud de descubrimiento.

3.1.3.7 Acceso directo

En entornos no de nube, el acceso directo de una parte solicitante al entorno de TI de la parte demandada no suele ser atendido (Ocurre de vez en cuando. De hecho, algunos tribunales son partidarios de realizar incautaciones sin previo aviso de equipos de TI con el fin de preservar la evidencia en casos civiles, incluidas las disputas laborales). En un entorno de la nube, esta opción es incluso menos probable, o directamente imposible ya que su análisis forense puede ser después y a su vez también imposible. Es posible que algunos proveedores de nube no puedan proporcionar tal acceso directo, ya que el hardware y las instalaciones a su vez no estén en su poder, y fuera de su custodia o control, y la parte solicitante debería negociar directamente con el proveedor para dicho acceso.

3.1.3.8 Información proporcionada en formatos no estándar

Los proveedores de servicios en la nube a menudo almacenan datos en sistemas altamente propietarios y aplicaciones que los clientes no controlan. En general, se espera que ESI se

produzca en formatos estándar (como PDF para documentos electrónicos), a menos que la información perdida por la conversión a este formato (como los metadatos) sea relevante para la disputa. Los datos en el formato exacto en que los maneja la nube pueden ser inútiles para la parte solicitante. En estas circunstancias, puede ser mejor para todos los involucrados -la parte solicitante, el cliente y el proveedor- exportar la información relevante dentro del propio entorno de nube utilizando protocolos estándar, prestando la debida atención a la conservación de la información relevante.

3.1.3.9 Autenticación

En este contexto, la autenticación debe entenderse como la autenticación forense de datos para su admisión como evidencia. (Esto no debe confundirse con la autenticación del usuario, que es un componente de la gestión de la identidad). Almacenar datos en la nube no afecta la capacidad de garantizar la autenticidad de los datos de cara a su admisión como evidencia. La pregunta clave es si el documento es lo que pretende ser. Por ejemplo, un correo electrónico no es más o menos auténtico porque se almacenó en un sistema local de una empresa o porque se almacenó en la nube; la pregunta es si se almacenó con integridad, de modo que los tribunales puedan confiar en que no se ha modificado desde que se creó. En ausencia de otra evidencia, como manipulación o piratería, los documentos no deben considerarse más o menos admisibles o confiables simplemente porque fueron creados o almacenados en la nube.

3.1.3.10 Cooperación entre proveedor y cliente en *e-discovery*

El mejor interés de los proveedores y clientes se obtiene al considerar las complicaciones causadas por un descubrimiento electrónico al comienzo de su relación, y al incluirlo como parte de su *SLA*. Los proveedores pueden considerar diseñar su oferta de servicios en la nube para incluir servicios de descubrimiento electrónico para atraer clientes ("*Discovery by Design*" o “Descubrimiento por Diseño”). En cualquier caso, los clientes y proveedores deberían valorar disponer de acuerdo de cooperación razonable en la materia, para la asistencia cruzada en este tipo de solicitudes de descubrimiento electrónico dirigido a cualquiera de los dos.

3.1.3.11 Respuesta a una citación o mandato de búsqueda

En caso de que un proveedor de servicios en la nube reciba de un tercero una solicitud para proporcionar información, puede llegarle como una citación, una orden o una orden judicial en la que se exige el acceso a los datos del cliente. El cliente puede querer tener la capacidad de recurrir contra la solicitud de acceso a fin de proteger la confidencialidad de sus datos. Con este fin, el acuerdo de servicio en la nube debe exigir que el proveedor de servicios en la nube notifique al cliente que se recibió una citación y le da tiempo a la compañía para presentar recurso en contra.

El proveedor de servicios en la nube podría tener la tentación de responder a la solicitud abriendo sus instalaciones y proporcionando al solicitante todo aquello que sea requerido. Antes de hacerlo, el proveedor de servicios en la nube debe garantizar, en consulta con sus asesores legales, que la solicitud es legal y sólida. El proveedor de servicios en la nube debe analizar cuidadosamente la solicitud antes de divulgar la información bajo su custodia, y

considerar si puede cumplir con sus obligaciones para con sus clientes si entrega esta información. En algunos casos, un proveedor puede estar en mejores condiciones para atender las necesidades de sus clientes presentando recursos contra demandas de información demasiado amplias o problemáticas.

3.1.3.12 Más información

Para obtener más información sobre el descubrimiento y la información almacenada electrónicamente, hay una gran variedad de fuentes. Una que puede ser de interés es la Conferencia de Sedona, un instituto de investigación y educación sin fines de lucro que durante varios años ha hecho recomendaciones influyentes sobre el manejo de ESI, que a su vez han influido en a esta área emergente de la ley. Tenga en cuenta, sin embargo, que sus recomendaciones no tienen son parte de la jurisprudencia.

3.2 Recomendaciones

- Los clientes de la nube deben comprender los marcos legales y regulatorios relevantes, así como los requisitos y restricciones contractuales que se aplican al manejo de los datos o datos (ya sean propios o bajo su custodia), y como dirige sus operaciones, antes de mover sistemas y datos a la nube.
- Los proveedores de servicios en la nube deben divulgar de forma clara y visible sus políticas, requisitos y capacidades, incluidos todos los términos y condiciones que se aplican a los servicios que prestan.
- Los clientes de la nube deben realizar una evaluación exhaustiva de un proveedor de servicios en la nube propuesto antes de firmar cualquier contrato, y deben actualizar periódicamente esta evaluación y controlar el alcance, la naturaleza y la coherencia de los servicios que compran.
- Los proveedores de la nube deben publicar sus políticas, requisitos y capacidades para cumplir con las obligaciones legales de los clientes, tales como el descubrimiento electrónico.
- Los clientes de la nube deben comprender las implicaciones legales del uso de cada proveedor concreto de la nube y adaptarlos a sus requisitos legales.
- Los clientes de la nube deben comprender las implicaciones legales de dónde opera físicamente el proveedor de la nube y dónde almacena la información.
- El cliente de la nube debe decidir cómo elige dónde se alojarán sus datos, si la opción está disponible, para cumplir con sus propios requisitos jurisdiccionales.
- Los clientes y proveedores de la nube deben tener una comprensión clara de los requisitos legales y técnicos para cumplir con cualquier solicitud de descubrimiento electrónico.
- Los clientes de la nube deben entender que aceptar sin lectura previa o sin prestar atención los diversos acuerdos legales que se ofrecen mediante menús o ventanas emergentes para su aceptación durante el proceso para contratar servicios en la nube,

no invalida la posibilidad de que un proveedor requiera al proveedor para realizar una diligencia debida.

Dominio 4 Cumplimiento y Gestión de Auditoría

4.0 Introducción

Las organizaciones se enfrentan a nuevos desafíos a medida que migran de los CPD tradicionales a la nube. Entregar, medir y comunicar el cumplimiento legal de una multitud de regulaciones en múltiples jurisdicciones se encuentran entre los más grandes desafíos. Tanto los clientes como los proveedores deben entender y apreciar las diferencias jurisdiccionales y sus implicaciones en los estándares, procesos y prácticas existentes de cumplimiento legal y auditoría. La naturaleza distribuida y virtualizada de la computación en la nube requiere un ajuste significativo de los enfoques basados en instancias definidas y físicas de información y procesos.

Además de proveedores y clientes, los reguladores y los auditores también se están ajustando al nuevo mundo de computación en la nube. Pocas normas existentes se escribieron para tener en cuenta los entornos virtualizados o los despliegues en la nube. Un usuario de la nube puede ser desafiado a mostrar a los auditores que la organización está cumpliendo las leyes y regulaciones. Comprender la interacción de la computación en la nube y el entorno regulatorio es un componente clave de cualquier estrategia en la nube. Los clientes, auditores y proveedores de la nube deben considerar y comprender lo siguiente:

- Implicaciones regulatorias para usar un servicio o proveedor en la nube en particular, prestando especial atención a cualquier problema transfronterizo o multi-jurisdiccional cuando corresponda.
- Asignación de responsabilidades de cumplimiento legal entre el proveedor y el cliente, incluyendo proveedores indirectos (es decir, el proveedor de la nube de tu proveedor de la nube). Esto incluye el concepto de herencia de cumplimiento legal donde un proveedor puede tener partes de su servicio certificadas en cuanto a cumplimiento lo que las saca del alcance de auditoría del cliente, pero el cliente sigue siendo responsable para el cumplimiento legal de todo lo que construyen sobre el proveedor.
- Capacidades del proveedor para demostrar el cumplimiento legal, incluido la generación de documentos, la producción de evidencias y cumplimiento legal del proceso, de manera oportuna.

Algunos temas adicionales específicos de la nube a los se debe prestar especial atención incluyen:

- El papel de las auditorías y certificaciones del proveedor y cómo afectan el alcance de auditoría (o evaluación) del cliente.
- Comprender qué características y servicios de un proveedor de nube están dentro del alcance de que auditorías y evaluaciones.
- Gestionar el cumplimiento legal y las auditorías a lo largo del tiempo.
- Trabajar con reguladores y auditores que pueden carecer de experiencia con la tecnología de computación en la nube.

- Trabajar con proveedores que pueden carecer de experiencia en auditoría y cumplimiento legal normativo.

4.1 Visión general

Lograr y mantener el cumplimiento legal de un montón de normas y estándares modernos es una actividad central para la mayoría de los equipos de seguridad de la información y una herramienta fundamental de gobernanza y gestión de riesgos. Tanto es así que las herramientas y los equipos en este ámbito tienen su propio acrónimo: GRC, para gobernanza, riesgo y cumplimiento legal. Aunque está estrechamente relacionado con las auditorías, que son un mecanismo clave para respaldar, asegurar y demostrar el cumplimiento legal, hay más para cumplir que las auditorías y más en auditar que usar estas para asegurar cumplimiento legal regulatorio. Para nuestros propósitos:

- El cumplimiento legal valida la conciencia y la adherencia a las obligaciones corporativas (por ejemplo, responsabilidad social, ética, leyes aplicables, regulaciones, contratos, estrategias y políticas). El proceso de cumplimiento legal evalúa el estado de esa conciencia y adhesión, evaluando adicionalmente los riesgos y los costos potenciales del incumplimiento legal frente a los costos para lograr el cumplimiento legal, y por lo tanto prioriza, financia e inicia cualquier acción correctiva que se considere necesaria.
- Las auditorías son una herramienta clave para probar (o refutar) el cumplimiento legal. También utilizamos auditorías y evaluaciones para respaldar las decisiones de riesgo de incumplimiento legal.

Esta sección trata sobre estos dominios interrelacionados de forma individual para centrarse mejor en las implicaciones que la computación en la nube tiene en cada uno.

4.1.1 Cumplimiento

La tecnología de la información en la nube (o en cualquier lugar en realidad) está cada vez más sujeta a un montón de políticas y regulaciones de gobiernos, grupos industriales, relaciones comerciales y otras partes interesadas. La gestión del cumplimiento legal es una herramienta de gobernanza; es la forma en que una organización evalúa, remedia y demuestra que cumple con estas obligaciones internas y externas.

Las regulaciones, en particular, típicamente tienen fuertes implicaciones para la tecnología de la información y su gobernanza, especialmente en términos de monitoreo, gestión, protección y divulgación. Muchas regulaciones y obligaciones requieren un cierto nivel de seguridad, por lo que la seguridad de la información está tan profundamente acoplada con el cumplimiento legal. Los controles de seguridad son, por lo tanto, una herramienta importante para asegurar el cumplimiento legal, y la evaluación y prueba de estos controles es una actividad central para los profesionales de la seguridad. Esto incluye evaluaciones incluso cuando son realizadas por auditores internos o externos dedicados.

4.1.1.1 Cómo la nube cambia el cumplimiento

Al igual que con la seguridad, el cumplimiento legal en la nube es un modelo de responsabilidad compartida. Tanto el proveedor de la nube como el cliente tienen responsabilidades, pero el cliente *siempre es el responsable final de su propio cumplimiento legal*. Estas responsabilidades se definen a través de contratos, auditorías / evaluaciones y detalles de los requisitos de cumplimiento legal.

Los clientes de la nube, particularmente en la nube pública, deben confiar más en las certificaciones de terceros del proveedor para comprender su alineamiento y las ausencias de cumplimiento legal. Dado que los proveedores de la nube pública dependen de las economías de escala para administrar los costos, a menudo no permitirán que los clientes realicen sus propias auditorías. En cambio, de forma similar a las auditorías financieras de las empresas públicas, se relacionan con una empresa externa para realizar auditorías y emitir certificaciones. Por lo tanto, el cliente en la nube no suele definir el alcance o realizar la auditoría por sí mismo. En su lugar, deberán confiar en estos informes y certificaciones para determinar si el servicio cumple con sus obligaciones de cumplimiento legal.

Muchos proveedores de servicios en la nube están certificados para diversas regulaciones y requisitos de la industria, como *PCI DSS, SOC1, SOC2, HIPAA*, mejores prácticas / marcos de referencia como CSA *CCM*, y regulaciones globales / regionales como la *GDPR* de la EU. A veces se les denomina auditorías de paso. Una auditoría de paso es una forma de *herencia de cumplimiento legal*. En este modelo, todas o algunas de las infraestructuras y servicios del proveedor de la nube se someten a una auditoría según un estándar de cumplimiento legal. El proveedor se responsabiliza por los costos y el mantenimiento de estas certificaciones. Las auditorías de proveedores, incluidas las auditorías de paso, deben entenderse dentro de sus limitaciones:

- Certifican que el *proveedor* cumple con los requisitos.
- Sigue siendo responsabilidad del cliente *crear aplicaciones y servicios que cumplan la legislación y regulación aplicable en la nube*.
- Esto significa que la infraestructura / los servicios del proveedor no están dentro del alcance de la auditoría / evaluación de un cliente. Pero todo lo que el cliente construye está dentro del alcance.
- El cliente sigue siendo el responsable final de mantener el cumplimiento legal de lo que construye y administra. Por ejemplo, si un proveedor *IaaS* tiene certificación *PCI DSS*, el cliente puede construir su propio servicio acorde con *PCI* en esa plataforma y la infraestructura y las operaciones del proveedor deberían estar fuera del alcance de evaluación del cliente. Sin embargo, el cliente puede fácilmente ir en contra de *PCI* y fallar en su evaluación si no diseña su propia aplicación ejecutándose en la nube correctamente.

Con la herencia de cumplimiento legal, la infraestructura del proveedor de la nube está fuera del alcance de la auditoría de cumplimiento legal de un cliente, pero todo lo que el cliente configura y desarrolla sobre los servicios certificados sigue dentro del alcance.

Los problemas de cumplimiento legal en la nube no se limitan a auditorías de paso; la naturaleza de la nube también crea diferenciadores adicionales.

Muchos proveedores de servicios en la nube ofrecen CPDs distribuidos globalmente que se ejecutan desde una consola / plataforma de administración central. Todavía es responsabilidad del cliente administrar y comprender dónde implementar datos y servicios, y aun así mantener su cumplimiento legal en jurisdicciones nacionales e internacionales.

Las organizaciones tienen la misma responsabilidad en informática tradicional, pero la nube reduce drásticamente la fricción de estas implementaciones potencialmente internacionales, por ejemplo, un desarrollador puede implementar datos regulados en un país no conforme sin tener que solicitar un CPD internacional y firmar múltiples niveles de contratos, si los controles apropiados no se habilitan para evitar esto.

No todas las características y servicios dentro de un proveedor de nube dado cumplen necesariamente y están certificados / auditados con respecto a todas las regulaciones y estándares. Es obligatorio que el proveedor de la nube comunique las certificaciones y atestados claramente, y para que los clientes entiendan los alcances y las limitaciones.

4.1.2 Gestión de auditoría

Un gobierno corporativo adecuado incluye naturalmente auditoria y seguridad. Las auditorías deben llevarse a cabo de manera independiente y deben diseñarse sólidamente para reflejar las mejores prácticas, los recursos apropiados, protocolos y estándares probados. Antes de ahondar en las implicaciones de la nube, debemos definir el alcance de la gestión de auditoría relacionada con la seguridad de la información.

Las auditorías y evaluaciones son mecanismos para documentar el cumplimiento legal de los requisitos internos o externos (o identificar deficiencias). Los informes deben incluir una determinación de cumplimiento legal, así como una lista de problemas identificados, riesgos y recomendaciones de remediación. Las auditorías y las evaluaciones no se limitan a la seguridad de la información, pero las relacionadas con la seguridad de la información generalmente se centran en evaluar la efectividad de la gestión y los controles de seguridad. La

mayoría de las organizaciones están sujetas a una combinación de auditorías y evaluaciones internas y externas para garantizar el cumplimiento legal de los requisitos internos y externos.

Todas las auditorías tienen un alcance variable y una declaración de aplicabilidad, que define qué se evalúa (por ejemplo, todos los sistemas con datos financieros) y a qué controles (por ejemplo, un estándar de la industria, alcance personalizado o ambos). Un testimonio es una declaración legal de un tercero, que puede usarse como su declaración de hallazgos de auditoría. Los testimonios son una herramienta clave al evaluar y trabajar con los proveedores de la nube, ya que el cliente de la nube no siempre puede realizar sus propias evaluaciones.

La gestión de auditoría incluye la gestión de todas las actividades relacionadas con las auditorías y evaluaciones, como la determinación de los requisitos, el alcance, la programación y las responsabilidades.

4.1.2.1 Cómo la nube cambia la gestión de la auditoría

Algunos clientes de la nube pueden estar acostumbrados a auditar a proveedores externos, pero la naturaleza de la computación en la nube y los contratos con los proveedores de la nube a menudo impiden cosas como las auditorías locales. Los clientes deben comprender que los proveedores pueden (y a menudo deberían) considerar las auditorías locales como un riesgo de seguridad al proporcionar servicios multi-cliente. Las múltiples auditorías locales de un gran número de clientes presentan desafíos logísticos y de seguridad claros, especialmente cuando el proveedor confía en los activos compartidos para crear grupos de recursos.

Los clientes que trabajen con estos proveedores deberán confiar más en las certificaciones de terceros en lugar de las auditorías que realizan ellos mismos. Dependiendo del estándar de auditoría, los resultados reales solo pueden ser entregados bajo un acuerdo de confidencialidad (ADC), lo que significa que los clientes deberán suscribir un acuerdo legal básico antes de obtener el acceso a los certificados para evaluaciones de riesgos u otros fines evaluativos. Esto a menudo se debe a requisitos legales o contractuales con la firma de auditoría, no debido a un intento de ofuscación por parte del proveedor de la nube.

Los proveedores de servicios en la nube deben comprender que los clientes aún necesitan la garantía de que el proveedor cumple con sus obligaciones contractuales y regulatorias, y deben proporcionar certificaciones de terceros rigurosas para demostrar que cumplen con sus obligaciones, especialmente cuando el proveedor no permite evaluaciones directas del cliente. Estos deben basarse en los estándares de la industria, con ámbitos claramente definidos y la lista de controles

> *La recopilación y el mantenimiento de artefactos de cumplimiento legal cambiarán cuando se utilice un proveedor de la nube.*

específicos evaluados. La publicación de certificaciones y atestados (en la medida permitida legalmente) ayudará mucho a los clientes de la nube a evaluar a los proveedores. El Registro STAR de Cloud Security Alliance ofrece un repositorio central para que los proveedores difundan públicamente estos documentos.

Algunos estándares, como *SSAE* 16, comprueban que los controles documentados funcionan como fueron diseñados / requeridos. El estándar no define necesariamente el alcance de los controles, por lo que ambos son necesarios para realizar una evaluación completa. Además, los testimonios y certificaciones no se aplican necesariamente a todos los servicios ofrecidos por un proveedor de la nube. Los proveedores deben tener claro qué servicios y características están cubiertos, y es responsabilidad del cliente prestar atención y comprender las implicaciones sobre el uso que hacen del proveedor.

Ciertos tipos de auditorías y evaluaciones técnicas de los clientes (como una evaluación de vulnerabilidad) pueden estar limitados en los términos de servicio del proveedor y pueden requerir permiso. Esto es a menudo para ayudar al proveedor a distinguir entre una evaluación legítima y un ataque.

Es importante recordar que los testimonios y las certificaciones son actividades puntuales. Un testimonio es una declaración de una evaluación "durante un período de tiempo" y puede no ser válida en cualquier punto futuro. Los proveedores deben mantener actualizado cualquier resultado publicado o se arriesgan a exponer a sus clientes a riesgos de incumplimiento legal. Dependiendo de los contratos, esto podría incluso llevar a exposiciones legales al proveedor. Los clientes también son responsables de garantizar que confían en los resultados actuales y realizar un seguimiento cuando los estados de sus proveedores cambian con el tiempo.

Los instrumentos son los registros, la documentación y otros materiales necesarios para las auditorías y el cumplimiento legal; son la evidencia para apoyar las actividades de cumplimiento legal. Tanto los proveedores como los clientes tienen la responsabilidad de producir y administrar sus respectivos instrumentos.

Los clientes son en última instancia responsables de que los instrumentos respalden sus propias auditorías y, por lo tanto, necesiten saber qué ofrece el proveedor y crear sus propios instrumentos para cubrir cualquier brecha. Por ejemplo, al crear un registro más sólido en una aplicación, ya que los registros del servidor en PaaS pueden no estar disponibles.

4.2 Recomendaciones

- El cumplimiento legal, la auditoría y la seguridad deben ser continuos. No deberían verse como simples actividades puntuales, y muchos estándares y regulaciones se están moviendo más hacia este modelo. Esto es especialmente cierto en la computación en la nube, donde tanto el proveedor como el cliente tienden a estar en un flujo más constante y rara vez están en un estado estático.
- Los proveedores de la nube deberían:
    - Comunicar claramente sus resultados de auditoría, certificaciones y testimonios prestando especial atención a:
        - El alcance de las evaluaciones.
        - Qué características / servicios específicos están cubiertos en qué ubicaciones y jurisdicciones.

        - Cómo los clientes pueden implementar aplicaciones y servicios que cumplan el marco legal y regulatorio en la nube.
        - Cualquier responsabilidad y limitaciones adicionales del cliente.
    - Los proveedores de la nube deben mantener sus certificaciones / testimonios a lo largo del tiempo y comunicar de manera proactiva cualquier cambio en el estado.
    - Los proveedores de la nube deberían involucrarse en iniciativas continuas de cumplimiento legal para evitar la creación de zonas no cubiertas y, por lo tanto, riesgos para sus clientes.
    - Proporcionar a los clientes evidencia e instrumentos comúnmente requeridos de cumplimiento legal, como registros de actividad administrativa que el cliente no puede recolectar por sí mismo.

- Los clientes de la nube deberían:
    - Comprender sus obligaciones de cumplimiento legal total antes de implementar, migrar o desarrollar en la nube.
    - Evaluar los testimonios y certificaciones de terceros de un proveedor y alinearlas con las necesidades de cumplimiento legal.
    - Comprender el alcance de las evaluaciones y certificaciones, incluidos los controles y las características / servicios cubiertos.
    - Intentar seleccionar auditores con experiencia en computación en la nube, especialmente si las auditorías y certificaciones de paso se usarán para administrar el alcance de la auditoría del cliente.
    - Asegurar que comprende los testimonios de cumplimiento legal que ofrece el proveedor y recopilar y administrar eficazmente dichos testimonios.
        - Crear y recolectar sus propios testimonios cuando los testimonios del proveedor no son suficientes.
    - Mantener un registro de los proveedores de la nube utilizados, los requisitos de cumplimiento legal relevantes y el estado actual. La Matriz de controles en la nube de Cloud Security Alliance puede respaldar esta actividad.

Dominio 5 Gobierno de la Información

5.0 Introducción

El objetivo fundamental de la seguridad de la información es la protección de los datos que son utilizados por nuestros sistemas y aplicaciones. A medida que las compañías evolucionan hacia tecnologías de computación en la nube, los métodos tradicionales de protección se ven desafiados por las nuevas arquitecturas basadas en la nube. La elasticidad, entorno multi-propietario, las nuevas arquitecturas físicas y lógicas y los modelos abstractos de controles requieren nuevas estrategias de seguridad de los datos. En muchas implementaciones en la nube, los usuarios llegan a transferir datos a entornos externos, o incluso públicos, para usos, contextos y herramientas que hubieran sido inimaginables hace sólo unos pocos años.

La gestión de la información en la era de la computación en la nube es un gran desafío que afecta a todas las organizaciones y requiere, no sólo nuevas medidas técnicas de protección, sino también de nuevos enfoques de gobierno. Aunque la computación en la nube afecta a todas las áreas del gobierno de la información, impacta particularmente en el cumplimiento legal, la privacidad y el diseño de políticas corporativas, debido a la creciente complejidad de trabajar con terceras partes y gestionar los límites jurisdiccionales.

Definición de gobierno de la información / gobierno del dato:

Garantizar que los datos y la información se usan de acuerdo con las políticas, estándares y estrategias corporativas, incluyendo sus objetivos regulatorios, contractuales y de negocio.

Los datos están siempre sujetos a una gran variedad de requisitos: algunos impuestos por agentes externos, como reguladores, clientes o socios. Y también hay requisitos internos basados en nuestra tolerancia al riesgo o simplemente en razones operativas. El gobierno de la información trata tanto los controles como las estructuras corporativas utilizados para garantizar que gestionamos la información de acuerdo con nuestros objetivos y requisitos.

Los requisitos de gobierno de la información y de los datos se ven afectados por varias características derivadas del hecho de usar la nube para su almacenamiento:

- *Multi-propiedad:* presenta implicaciones delicadas en materia de seguridad. Cuando se guarda información en nubes públicas, esta se almacena en infraestructuras compartidas con otros *propietarios* (“*tenants*”) sobre los que no se puede establecer confianza por completo. Incluso en un entorno de nube privada, los datos se almacenan y gestionan en infraestructuras compartidas entre múltiples unidades de negocio, que probablemente tengan diferentes necesidades de gobierno.

- *Responsabilidad compartida de seguridad:* cuanto más se comparten los entornos, más se comparte la responsabilidad en materia seguridad. Cada vez es más común que la información pertenezca y sea gestionada por diferentes equipos, incluso de diferentes

organizaciones. Por lo tanto, es importante saber reconocer la diferencia entre el Responsable de los datos y el Encargado del tratamiento de los datos.

- *Propietario (responsable de datos,* como su nombre indica, es el dueño de la información. No siempre la identidad del Propietario está perfectamente clara. Si un cliente nos facilita algún dato, podría ocurrir tanto que nos convirtamos en propietarios de esos datos, como que el cliente conserve la propiedad, en función de los requisitos legales o contractuales aplicables, o de las políticas del cliente. Si almacenas la información en un proveedor de nube pública deberías seguir siendo el propietario de la misma, aunque esto podría variar en función de los contratos con el proveedor.

- *Custodio (encargado de tratamiento),* se refiere a quién es el encargado de gestionar los datos. Si un cliente te facilita sus datos personales y no tienes el derecho para ser el titular, eres simplemente el custodio. Esto significa que sólo puedes utilizarlos de las maneras para la que se hayan autorizado. Si utilizas un proveedor de nube pública este será, del mismo modo, custodio de la información, aunque puede que también sigas ejerciendo ciertas responsabilidades dependiendo de qué controles implementes o gestiones directamente. La utilización de un proveedor no elimina tu propia responsabilidad. Básicamente el propietario define las reglas (en algunas ocasiones de manera indirecta en cumplimiento de requisitos legales) y el custodio implementa las reglas. Las líneas y roles entre el propietario y el custodio se ven impactados por la infraestructura de la nube, especialmente en el caso de nube pública.

El almacenamiento de datos de clientes en la nube introduce una tercera parte en el modelo de gobierno, el proveedor de nube.

- *Límites jurisdiccionales y soberanía de datos:* debido a que la nube, por definición, permite el acceso ubicuo, aumentan las posibilidades de almacenar información en más ubicaciones (jurisdicciones) reduciendo las dificultades para la migración de datos. Algunos proveedores puede que no sean demasiado transparentes con la ubicación de los datos, mientras en otras situaciones se necesiten controles adicionales para restringir la información a determinadas ubicaciones.

- *Cumplimiento, regulación y políticas de privacidad:* Estos aspectos pudieran verse impactados por el uso de la computación en la nube debido a la combinación de proveedores y jurisdicciones. Por ejemplo, el contrato con un cliente pudiera no permitir compartir o usar información en un proveedor en la nube o pudiera exigir la aplicación de ciertos requisitos de seguridad (como por ejemplo cifrado).

- *Destrucción y eliminación de datos:* esto se relaciona con las características técnicas de la plataforma en la nube. ¿Es posible garantizar la destrucción y eliminación de datos de acuerdo con las políticas aplicables?

Una migración a la nube se puede aprovechar para revisar las arquitecturas de información. Hoy en día, muchas de las arquitecturas de información son inconexas debido a que se diseñaron hace décadas y han hecho frente a continuos cambios tecnológicos. La migración a la nube ofrece una muy buena oportunidad para revisar cómo gestionamos la información e identificar oportunidades de mejora mejorar. No se trata de migrar los problemas actuales a la nube, sino de aprovechar el momento para rediseñar lo necesario.

5.1 Visión general

Las tareas de “Gobierno de los Datos” o “Gobierno de la Información” se ocupan de garantizar que los datos y la información se usan de acuerdo con las políticas, estándares y estrategias corporativas, satisfaciendo sus requisitos y objetivos regulatorios, contractuales y de negocio. Los datos y la información no son exactamente lo mismo, aunque se suele utilizar indistintamente. La información se origina en los datos con valor. Para nuestro propósito utilizaremos ambos términos por igual.

5.1.1 Dominios de gobierno de información en la nube

No se van a cubrir todos los dominios del gobierno de la información, sino que nos vamos a centrar aquellos que se ven impactados por un tratamiento en la nube: La computación en la nube impacta en casi todos los dominios de gobierno de la información

- *Clasificación de información.* Se relaciona generalmente con áreas de cumplimiento y afecta a la ubicación de la información y a los requisitos de los tratamientos de información. No todo el mundo necesariamente implementa un sistema de clasificación de información, pero si lo aplica, es necesario adaptarlo para la nube.
- *Políticas de gestión de información.* Está relacionado con la clasificación de información y deben ser ajustadas para los escenarios de servicio en la nube. Deberían cubrir las capas de infraestructura, plataforma y aplicación (*SPI*, en inglés), debido a que, por ejemplo, enviar información a un proveedor SaaS es muy diferente a construir tu propia aplicación *IaaS*. Se necesita establecer qué está permitido llevar a la nube y dónde. ¿Qué productos y servicios? ¿Con qué requerimientos de seguridad?
- *Ubicación y políticas jurisdiccionales.* Tienen una clara implicación en la nube. Cualquier alojamiento externo debe cumplir con los requerimientos de ubicación y jurisdiccionales. Es entendible que las políticas internas puedan adaptarse a la nube, pero los requisitos legales son rígidos (ver el domino sobre aspectos legales para más información). Es necesario entender que los tratados y leyes pueden crear conflictos. Cuando se manejan datos sometidos a regulación es necesario trabajar conjuntamente con el departamento legal para asegurar el cumplimiento de la mejor manera posible.

- *Autorizaciones.* La computación en la nube requiere cambios mínimos en las autorizaciones. Para entender mejor cómo impacta, visite los contenidos de esta guía sobre ciclo de vida de seguridad de la información.
- *Propiedad.* La organización es siempre responsable de los datos y de la información lo cual también aplica a cuando nos movemos a la nube.
- *Custodia.* El proveedor de nube puede convertirse en custodio de la información. La información alojada en el proveedor de nube, aunque cuando haya sido cifrada adecuadamente, está todavía bajo custodia de la organización.
- *Privacidad.* La privacidad es un conjunto de requerimientos regulatorios, obligaciones contractuales y compromisos con los clientes. Es necesario entender la totalidad de los requisitos y asegurar que se alinean las políticas de gestión de la información y de seguridad.
- *Controles contractuales.* Se trata de la herramienta legal disponible para extender los requerimientos de gobierno a terceras partes, como los proveedores de la nube.
- *Controles de seguridad.* Son la herramienta para implementar el gobierno de datos, y cambian significativamente en la computación en la nube. Visite el Dominio 11 “Seguridad de Datos y Cifrado” de esta guía para más información.

5.1.2 El ciclo de vida de la seguridad de datos

Aunque la Gestión del Ciclo de Vida de la Información es un campo bastante maduro, no se adapta de manera perfecta a las necesidades de los profesionales de seguridad. El Ciclo de Vida de la Seguridad de Datos es diferente de la gestión del ciclo de vida de la información y pone de manifiesto las diferentes necesidades desde una perspectiva de seguridad. A continuación, se muestra un resumen de este ciclo de vida, que está disponible en versión completa en https://securosis.com/blog/data-security-lifecycle-2.0. Se trata simplemente de una herramienta para ayudar a comprender los límites de la seguridad y de los controles sobre la información y no pretende ser una herramienta exhaustiva para todo tipo de datos. Es más bien un modelo de trabajo para ayudar a evaluar, a alto nivel, la seguridad de la información, buscando áreas de mejora.

El ciclo de vida incluye seis fases desde la creación hasta la destrucción. Aunque se muestra como una progresión lineal, la información, una vez creada, puede moverse entre las distintas fases sin restricciones, y puede que no pase por todas las etapas (por ejemplo, no todos los datos finalmente se eliminan).

Crear. La creación es la generación de cualquier contenido digital nuevo o la alteración, actualización y/o modificación de contenido existente.

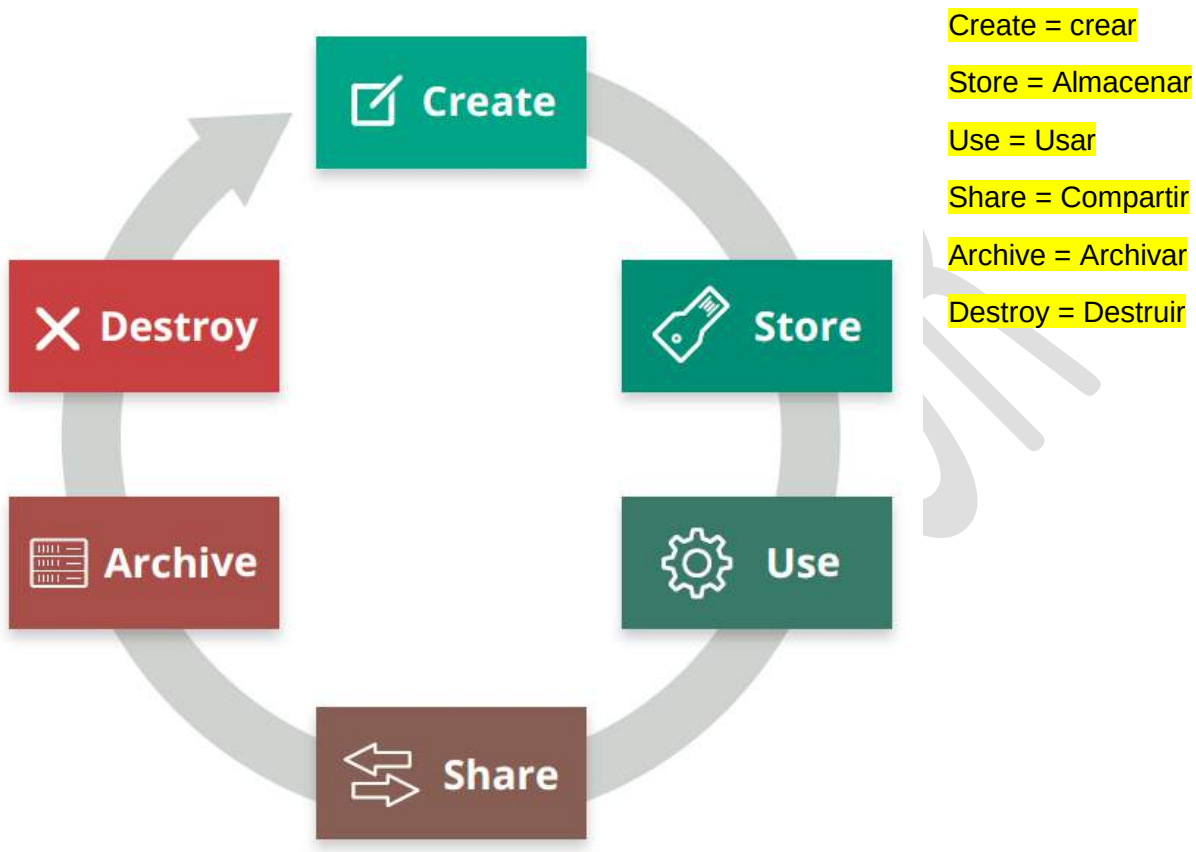
Almacenar. Es el acto de depositar datos digitales en algún tipo de repositorio de almacenamiento. Normalmente ocurre simultáneamente con la creación de datos.

Uso. La información se ve, se procesa o se utiliza de algún otro modo (sin incluir la modificación).

Compartir. La información se hace accesible para otras entidades tales como usuarios, clientes y socios.

Archivo. La información deja de ser usada de manera activa y entra en un repositorio de almacenamiento a largo plazo o archivo.

Eliminación. La información o datos se eliminan permanentemente utilizando medios lógicos o físicos (p.e. *cryptoshredding*).

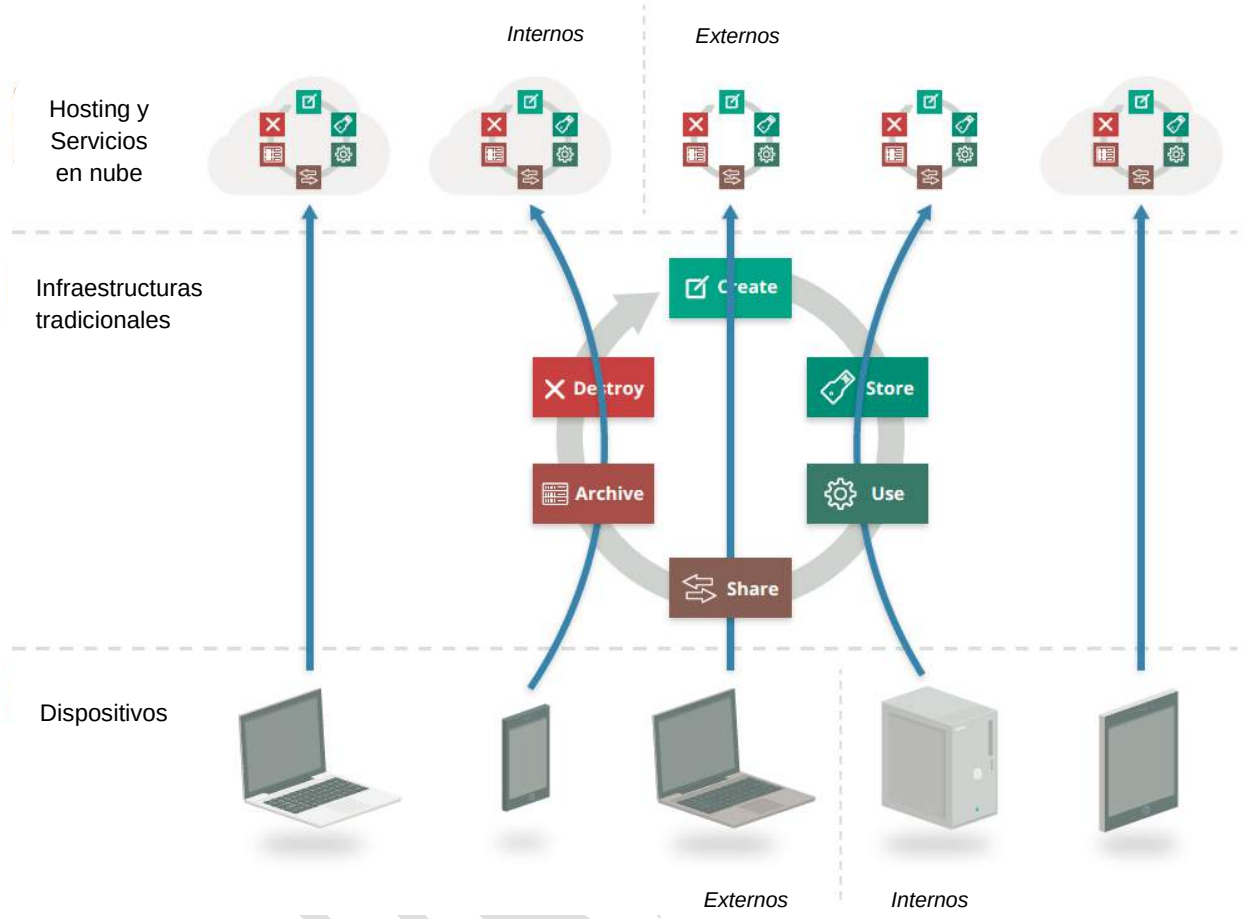


El ciclo de vida de la seguridad de los datos

5.1.2.1 Ubicaciones y derechos de acceso

El ciclo de vida representa las fases por las que atraviesa la información, pero no aborda ni su ubicación ni cómo se accede a la misma.

Ubicaciones: Puede visualizarse pensando en el ciclo de vida no cómo una única operación linear, sino más bien como una serie de ciclos de vida más pequeños ejecutándose en diferentes entornos. En casi cualquier fase la información puede entrar, salir o moverse entre estos entornos.



El acceso y almacenamiento de datos puede seguir múltiples modelos, cada uno con su propio ciclo de vida

Debido a todas las posibles cuestiones regulatorias, contractuales o jurisdiccionales, es extremadamente importante entender tanto la ubicación lógica, como la ubicación física de los datos.

Derechos de acceso: Cuando los usuarios conocen dónde están los datos y cómo se mueven, necesitan saber quién accede y cómo. Hay dos aspectos a tener en cuenta:

- ¿Quién accede a la información?
- ¿Cómo acceden (dispositivo y canal)?

Hoy en día se utilizan una gran variedad de dispositivos para acceder a la información. Cada dispositivo tiene características de seguridad diferentes y pueden utilizar distintas aplicaciones o clientes.

5.1.2.1 Funciones, actores y controles

El próximo paso consiste en identificar qué funciones se puede hacer con los datos, dado un determinado actor (persona o sistema) en una determinada ubicación.

Funciones: Es posible realizar tres posibles tipos de acciones con un dato:

- *Lectura:* ver o leer el dato. Se consideran también en esta acción la creación, copiado, transferencia, diseminación, y otros intercambios de información.
- *Procesado:* realizar una transacción sobre el dato; actualizarlo; utilizarlo en una transacción de negocio, etc.
- *Almacenamiento: conservar el dato (en un archivo, base de datos, etc.).*

La siguiente tabla muestra qué funciones mapean con qué fases del ciclo de vida:

	Crear	Almacenar	Usar	Compartir	Archivar	Eliminar
Leer	X	X	X	X	X	X
Procesar	X		X			
Almacenar		X			X	

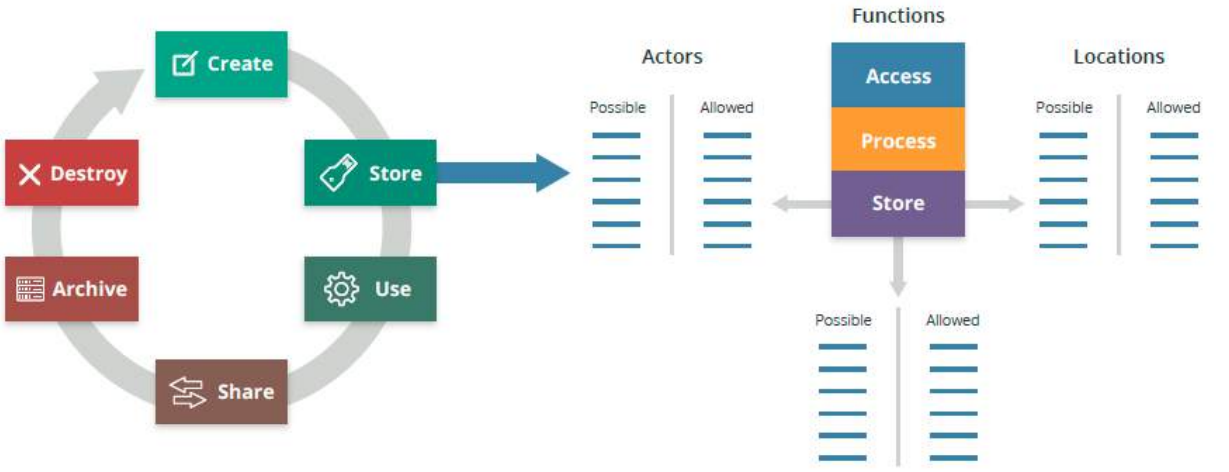
Tabla 1. Fases del ciclo de vida de la Información

Un actor (persona, aplicación, sistemas o proceso, pero no un dispositivo de acceso) debe realizar cada función desde una ubicación.

Controles: Un control restringe la ejecución a las acciones permitidas desde la lista total de posibles acciones. La siguiente tabla muestra una forma de listar las posibilidades, para que el usuario pueda mapearla con controles.

Función		Actor		Ubicación	
Disponible	Permitida	Disponible	Permitida	Disponible	Permitida

Mapeo ciclo de vida con funciones y controles



Mapeo ciclo de vida con funciones y controles

5.2 Recomendaciones

- Establecer los requerimientos de gobierno de información antes de planificar una transición a la nube. Esto incluye requerimientos regulatorios y legales, obligaciones contractuales y políticas corporativas. Puede que sea necesario actualizar las políticas y estándares corporativos para permitir el tratamiento de datos a terceras partes.
- Asegurar que las políticas y prácticas de gobierno de información se amplían para cubrir los servicios prestados desde la nube. Esto puede hacerse mediante controles contractuales y de seguridad.
- Utilizar el ciclo de vida de seguridad de la información, cuando sea necesario, para ayudar a modelar los controles y el tratamiento de datos.
- En lugar de simplemente trasladar a la nube las arquitecturas de información actuales, generalmente ya inconexas, aprovechar la migración a la nube para replantear y reestructurar la arquitectura. No arrastres anteriores malos hábitos.

Dominio 6 Plano de Gestión y Continuidad del Negocio

6.0 Introducción

El Plano de Gestión (*Management Plane*) es la diferencia individual más significativa entre las arquitecturas tradicionales y la computación en la nube. Esta no es toda la meta-estructura (definida en el Dominio 1) sino que es la interfaz para conectarse con la meta-estructura y configurar la mayor parte de los servicios en la nube.

Siempre existirá un Plano de Gestión, integrado por las herramientas y las interfaces que utilizamos para administrar nuestra infraestructura, plataformas y aplicaciones, pero la nube permite abstraer y centralizar la administración de los recursos. En lugar de controlar la configuración de los centros de datos con servidores y cables, ahora se controla mediante *APIs* y consolas web.

Por lo tanto, obtener acceso al Plano de Gestión es como obtener acceso sin restricciones a su Centro de Datos, salvo que se apliquen los controles de seguridad adecuados para limitar quién puede acceder al Plano de Gestión y qué pueden hacer dentro de él.

Para pensarlo en términos de seguridad, el Plano de Gestión consolida muchas cosas que anteriormente manejamos a través de sistemas y herramientas independientes, para después hacerlas accesibles desde Internet con un único conjunto de credenciales de autenticación.

Esta no es una pérdida neta por seguridad, porque también hay ganancias, pero se trata de un modelo claramente distinto que impacta en cómo debemos evaluar y administrar la seguridad.

La centralización también trae beneficios de seguridad. No hay recursos ocultos, siempre conocerás dónde están todos los activos bajo tu responsabilidad en todo momento y cómo están configurados. Esta es una nueva capacidad que se origina tanto en el acceso ubicuo a la información como en la medición de los servicios, características propias de la computación en la nube. El controlador de la nube siempre necesita saber qué recursos están en condiciones de ser usados (*pooling)*, cuáles no y a quién se le han asignado.

Esto no significa que todos los activos que se muevan a la nube se administren de la misma manera. El controlador de la nube no puede analizar los servidores en ejecución o abrir archivos bloqueados, ni comprender las implicaciones de los datos e información concretos de los usuarios de la nube.

Al final, esta es una extensión del Modelo de Responsabilidad Compartida discutido en el Dominio 1 y a lo largo de esta Guía. El Plano de Gestión es responsable de administrar los activos y recursos disponibles en la nube, mientras que el usuario de la nube es responsable

de cómo él mismo configura sus servicios en la nube, y de otros activos que despliega sobre la misma.

- El proveedor de la nube es responsable de garantizar que el Plano de Gestión sea seguro y las funciones de seguridad necesarias estén disponibles para el consumidor de la nube, como, por ejemplo, la capacidad de asignar derechos con granularidad suficiente para controlar lo que alguien puede hacer incluso si tienen acceso al Plano de Gestión.

- El consumidor de la nube es responsable de configurar correctamente sus usos permitidos en el Plano de Gestión, así como de asegurar y gestionar sus credenciales.

6.0.1 Continuidad del negocio y recuperación ante desastres en la nube

La Continuidad de Negocio y Recuperación ante Desastres (*BC/DR*) es tan importante en la computación en la nube como lo es para cualquier otra tecnología. Además de las diferencias resultantes de la posible participación de un proveedor externo (habitual en *BC/DR*), hay consideraciones adicionales debido a las diferencias inherentes al uso de recursos compartidos.

Los tres aspectos principales de *BC/DR* en la nube son:

- Garantizar la continuidad y la recuperación en el mismo proveedor de nube que ya presta el servicio. Estas son las herramientas y técnicas para diseñar mejor su implementación en la nube para mantener el servicio en funcionamiento si pierde el despliegue realizado o ante problemas puntuales del proveedor de nube.

- Preparación y administración de interrupciones del proveedor de nube. Esto se extiende desde los problemas más localizados que pueden ser resueltos con un buen diseño o soluciones temporales, hasta las interrupciones más amplias que eliminan el servicio del proveedor total o parcialmente, pero siempre excediendo las medidas de recuperación ante desastres existentes.

- Valorar las opciones de portabilidad de servicios entre proveedores de nube. Esta decisión podría deberse tanto por desear características de servicio diferentes, como por la pérdida completa del servicio del proveedor en caso de, por ejemplo, salida del mercado o disputas legales.

6.0.1.1 Diseño de servicios resiliente a fallos

Si bien las plataformas en la nube pueden ser increíblemente resilientes, la resiliencia de activos de nube concretos e individuales suele ser menor frente a sus equivalentes en infraestructuras tradicionales. Esto se debe a la fragilidad inherentemente mayor de los recursos virtualizados que se ejecutan en entornos altamente complejos.

Esto se refiere especialmente cierto a recursos de computación, redes y almacenamiento, ya que permiten un acceso casi directo al recurso físico, mientras que los proveedores de la nube aplican controles de resiliencia adicionales para sus plataformas y aplicaciones sobre el *IaaS* en que se apoyan.
Sin embargo, esto significa que los proveedores de la nube tienden a ofrecer opciones para mejorar la resiliencia, a menudo más allá de lo asequible (a igualdad de costes) en la infraestructura tradicional. Por ejemplo, al habilitar múltiples "zonas" donde puede implementar máquinas virtuales dentro de un grupo auto-escalable, que abarque centros de datos físicamente distintos, mejorando la disponibilidad total del servicio. O puede configurarse un servicio con reparto de carga entre las zonas, de modo que, si una zona entera se pierde, el servicio permanece activo. Esto es bastante difícil de implementar en un centro de datos tradicional, donde normalmente no es rentable construir múltiples zonas físicas aisladas sobre las que implementar aplicaciones con balanceo de carga entre zonas y reconfiguración automática.

Pero esta resiliencia adicional solo está disponible si el servicio se diseña para aprovecharla. La implementación del servicio en una sola zona, o incluso en una sola máquina virtual en una sola zona, es menos resiliente que la implementación en un solo servidor físico en buen estado.

Esta es la razón por la cual una estrategia de migración masiva a la nube moviendo servicios y máquinas virtuales sin cambios arquitectónicos (en inglés, "*lift and shift*") puede reducir la resiliencia. Las aplicaciones existentes rara vez fueron diseñadas e implementadas para aprovechar estas capacidades de resiliencia, así la virtualización y la migración directa sin cambios pueden aumentar las probabilidades de fallos individuales.

La facilidad de integrar estas capacidades es mayor cuando se trabaja a nivel *IaaS* y mucho menor trabajando a nivel SaaS, al igual que ocurre en la implantación de la seguridad en la nube. A nivel *SaaS*, el servicio está condicionado a la capacidad del proveedor de la nube de mantener todo el servicio. Con *IaaS* se puede diseñar el servicio para responder ante fallos, poniendo más responsabilidad en sus manos. *PaaS*, como de costumbre, está en el medio: algunos *PaaS* pueden tener opciones de resiliencia configurables, mientras que otras plataformas están completamente bajo el control único del proveedor.

En general, es clave asentar un enfoque basado en el riesgo:

- No todos los activos necesitan la misma continuidad.
- No se complique planificando las interrupciones del proveedor porque perciba que está perdiendo el control de la aplicación: compruebe los datos históricos de desempeño.
- Esfuércese por realizar diseños de servicios que puedan responder a *RTOs* y *RPOs* equivalentes a los de la infraestructura tradicional.

6.1. Visión general

6.1.1 Seguridad del plano de gestión

El Plano de Gestión se refiere a las interfaces para administrar sus activos en la nube. Si implementa máquinas virtuales en una red virtual, el Plano de Gestión es la herramienta para crear esas máquinas y configurar esa red. En servicios *SaaS*, el Plano de Gestión suele ser la pestaña "administrador" de la interfaz de usuario y donde se configuran cosas como usuarios del servicio, configuraciones del servicio para la organización, etc.
El Plano de Gestión controla y configura la meta-estructura (definida en el Dominio 1), y también es parte de la propia meta-estructura. Recordemos que la computación en la nube toma activos físicos (como redes y procesadores) y los utiliza para crear grupos de recursos. La Meta-estructura es el elemento central que permite crear y aprovisionar los recursos en los grupos y retirar dichos recursos de los grupos en los que estaban asignados. El Plano de Gestión incluye las interfaces para construir y administrar la nube propiamente dicha, así como las interfaces para que los usuarios de nube administren los recursos que tienen asignados.

El plano de gestión es una herramienta clave para habilitar y aplicar la asignación separada de recursos y el aislamiento de los mismos en un entorno multi-propietario. Limitar quién puede hacer qué con las *APIs* de los servicios de nuevo es otro medio importante para segregar clientes de la nube, y a diferentes usuarios de un mismo cliente.

6.1.1.1 Accediendo al plano de gestión

El Plano de Gestión está accesible mediante *APIs* e interfaces web. Las *APIs* permiten automatizar la gestión de los servicios en la nube. Son el pegamento que mantiene unidos los componentes de la nube y permite su orquestación. Además, y dado que no todos los usuarios desean automatizar tanto la administración de su nube, las consolas web proporcionan interfaces visuales para los administradores. En muchos casos, las consolas web simplemente usan las mismas *API* a las que puede acceder directamente.
Los proveedores y las plataformas en la nube a menudo también ofrecen librerías para el de desarrollo de software (*SDK*) e interfaces de línea de comando (*CLI*) para facilitar la integración con sus *API*.

- Las consolas web son administradas por el proveedor de nube. Pueden ser específicos de cada cliente de servicio de nube (por lo general, usan la redirección de *DNS* vinculada a la identidad federada). Por ejemplo, cuando un usuario particular se conecta a su aplicación para compartir archivos en la nube y tras iniciar la sesión, el proveedor le redirige a la "versión" de la aplicación específicamente configurada por el cliente al que pertenece el usuario. Esta versión tendrá su propio nombre de dominio asociado, que le permite integrarse más fácilmente con identidad federada (por ejemplo, en lugar de que todos sus usuarios inicien sesión en "application.com", inician sesión en "your-organization.application.com").

Como se mencionó, la mayoría de las consolas web ofrecen al cliente de nube una interfaz de acceso que se apoya en las mismas *API* a las que puede acceder directamente. Aunque, dependiendo de la plataforma o del proceso de desarrollo del proveedor, a veces puede encontrar discrepancias por la que una característica concreta está disponible antes en la *API* o en la interfaz web.

Las *API* suelen ser *REST* para servicios en la nube, ya que *REST* es fácil de implementar para servicios desplegados en Internet. Las *API REST* se han convertido en el estándar para los servicios basados en web, ya que se ejecutan a través de HTTP/S y, por lo tanto, funcionan bien en entornos heterogéneos.

Las *APIs REST* pueden usar varios mecanismos de autenticación, ya que no existe un estándar único para la autenticación en *REST*. La firma de solicitudes HTTP y OAuth son los más comunes; ambos utilizan técnicas criptográficas para validar los intentos de autenticación recibidos por la *API.*

Es habitual encontrar servicios que se autentican mediante contraseñas, una opción menos segura y que expone las credenciales a mayores riesgos. Es más frecuente en plataformas web antiguas o mal diseñadas que construyeron su interfaz web primero y solo agregaron acceso vía *API* más adelante. En estos servicios se deben usar cuentas específicas para el acceso vía *API*, a fin de reducir las oportunidades de exposición de credenciales.

6.1.1.2 Asegurar el plano de gestión

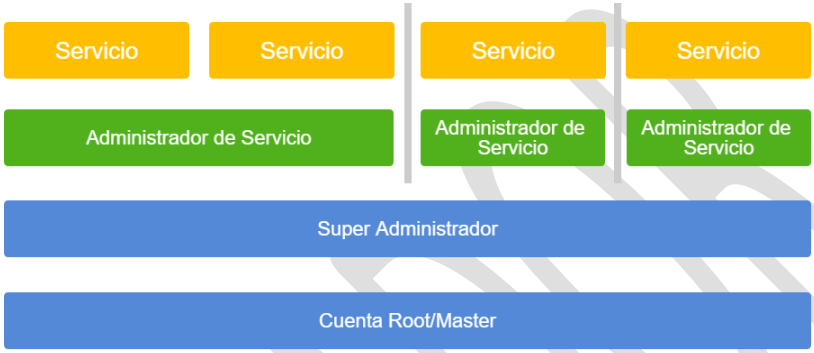
La Gestión de Identidades y Accesos (en inglés, *IAM*, "*Identity and Access Management*") combina identificación, autenticación y autorizaciones de usuarios (incluida la administración de acceso). Así es como se determina quién puede hacer qué dentro de su plataforma o proveedor de nube.

Las opciones, configuraciones e incluso los conceptos específicos varían mucho entre los distintos proveedores y plataformas de nube. Cada uno tiene su propia implementación y es posible que ni siquiera use las mismas definiciones para conceptos básicos como "grupos" y "roles".

Independientemente de plataformas o proveedores, siempre hay un propietario de cuenta con privilegios de super-administrador para administrar toda la configuración. Esta cuenta debe ser gestionada por la empresa (nunca por una única persona), tener un acceso muy contralado, y ser usada en muy pocas ocasiones.

De forma independiente a las cuentas personales de administradores, generalmente es posible crear cuentas de súper administrador para uso de administradores individual. Use estos privilegios con moderación; y aplíquelo también a escasos administradores ya que el compromiso o abuso de una de estas cuentas podría permitir a alguien cambiar o acceder a todos y cada uno de los servicios y datos.

Su plataforma o proveedor puede admitir cuentas de administrador con privilegios limitados a partes del servicio. A veces llamamos a estos "administradores del servicio" o "administradores del día a día". Estas cuentas no necesariamente exponen toda la implementación en caso de acceso irregular o si son comprometidas, y, por lo tanto, son mejores para las actividades más cotidianas. También ayudan a separar sesiones individuales, por lo que no es excepcional permitir que un único administrador humano acceda a múltiples cuentas de administrador de servicio (o roles) para que puedan iniciar sesión con solo los privilegios que necesitan para esa acción en particular en lugar de tener que exponer una gama mucho más amplia de derechos.



Ejemplos de cuentas de usuario de Plano de Gestión de nube en la línea de base, incluidos super-administradores y administradores de servicios.

Tanto los proveedores como los usuarios deben aplicar consistentemente el criterio de mínimo privilegio en la creación y asignación de cuentas para los usuarios, las aplicaciones y para el acceso al Plano de Gestión.

Todas las cuentas de usuario con privilegios deben usar autenticación de múltiple factor (*MFA*, en inglés *Multiple-Factor Authentication*). Si es posible, *todas* las cuentas de usuario del servicio en la nube (incluso cuentas de usuario individuales) deben usar *MFA*. Es uno de los controles de seguridad más efectivos para defenderse contra una amplia gama de ataques. Esto también es cierto independientemente del modelo de servicio: *MFA* es tan importante para *SaaS* como lo es para *IaaS*.
(Consulte el Dominio 12 de Gestión de Identidades para obtener más información sobre *IAM* y el papel de la federación y la autenticación fuerte, gran parte de la cual se aplica al Plano de Gestión de la nube).

6.1.1.3 Seguridad del plano de gestión al construir/proporcionar un servicio en la nube

Las responsabilidades son mayores para el responsable de construir y mantener el Plano de Gestión propiamente dicho, como por ejemplo en una implementación de nube privada. El usuario de servicios en la nube solo configura las partes del Plano de Gestión que el proveedor le expone, pero cuando usted es el proveedor de la nube, obviamente usted es responsable de todo.

Profundizar en los detalles de implementación está más allá del alcance de esta Guía, pero a un alto nivel hay cinco facetas principales para construir y administrar un Plano de Gestión seguro:

- *Seguridad perimetral:* Protección contra ataques contra los propios componentes del Plano de Gestión, como la web y las interfaces *API*. Incluye tanto controles básicos del tráfico en red como controles especializados y de protección de ataques a nivel de aplicación.
- *Autenticación de cliente:* Proporcionar mecanismos seguros para que los clientes se autentiquen en el Plano de Gestión. Esto debería usar estándares existentes (como la firma de solicitudes OAuth o HTTP) que sean criptográficamente válidos y estén bien documentados. La autenticación del cliente debe ser compatible con *MFA*, bien como opción, bien como requisito.
- *Autenticación interna y aprobación de credenciales:* Los mecanismos que utilizan los propios administradores del proveedor para conectarse con las zonas del Plano de Gestión no disponibles para el cliente. También incluye distinguir entre peticiones a las *APIs* con un usuario del cliente y un usuario administrador del proveedor. Cualquier acción de gestión del propio Plan de Gestión debería requerir *MFA*.
- *Autorización y derechos:* debe distinguir los permisos disponibles para los clientes y los permisos disponibles para los administradores del proveedor. La granularidad en estos derechos facilita a los clientes gestionar de forma segura sus propios usuarios y administradores. En el proveedor, la granularidad reduce los impactos de un posible compromiso o uso fraudulento de las cuentas de los administradores.
- *Registro, monitorización y alertas:* La generación consistente de registros de las acciones de los administradores y su monitorización es esencial para una seguridad y cumplimiento efectivos. Esto aplica tanto a lo que el cliente hace en sus cuentas, como a lo que hacen los empleados del proveedor en su administración diaria del servicio. La alerta de eventos inusuales es un control de seguridad importante para garantizar que la monitorización permite tomar acciones inmediatamente, y no simplemente algo que se observa una vez las acciones ya han ocurrido. Idealmente, los clientes de nube deberían poder acceder a los registros de su propia actividad en la plataforma de nube a través de *API* u otro mecanismo para integrarse con sus propios sistemas de registro de seguridad.

6.1.2 Continuidad del negocio y recuperación de desastres

Al igual que la seguridad y el cumplimiento, la Continuidad del Negocio y la Recuperación ante Desastres (*BC/DR*) es una responsabilidad compartida. Hay aspectos que el proveedor de la nube tiene que gestionar, pero el cliente de la nube es el responsable en última instancia de cómo se usan y administran los servicios en nube. Esto es especialmente cierto cuando se planifica cómo afrontar interrupciones totales o parciales del servicio del proveedor de nube.

Asimismo, e igual que ocurre en el caso de la seguridad, los clientes de nube tienen más control y responsabilidad en *IaaS* y menos en *SaaS*, con PaaS en el medio.

La *BC/DR* debe tener un enfoque basado en el riesgo. Muchas opciones de *BC* pueden tener un costo prohibitivo en la nube, pero también pueden no ser necesarias. Esto también ocurre en los centros de datos tradicionales, pero es habitual que los clientes de servicios en nube estén tentados a incrementar este control más de lo razonable para compensar la pérdida de control físico de los recursos derivada de la migración a la nube. Por ejemplo, las probabilidades de que un importante proveedor de *IaaS* cierre su negocio o cambie su modelo de negocio completo son bajas, mientras que en proveedores *SaaS* más pequeños o con una base empresarial menos robusta.

- Pídale al proveedor de nube sus estadísticas de interrupciones de servicio a lo largo del tiempo, ya que esto puede ayudar a informar sus decisiones de riesgo.

- Recuerde que estas capacidades varían entre los proveedores y deben incluirse en el proceso de selección del proveedor.

6.1.2.1 Continuidad del negocio dentro del proveedor de la nube

Cuando despliega activos en la nube, no puede asumir que la nube siempre estará allí, o que siempre prestará servicios de la manera que se espera. Las interrupciones y los problemas son tan comunes como con cualquier otra tecnología, aunque la nube puede ser, en general, más resiliente cuando el proveedor aporta mecanismos para soportar el diseño e implantación de servicios resilientes.

Este es un punto clave que requiere dedicarle un poco más de tiempo: como ya mencionamos, la naturaleza misma de la virtualización de recursos en grupos de uso compartido genera típicamente activos individuales (por ejemplo, una máquina virtual) menos resilientes. Por otro lado, la abstracción de recursos y la administración de todos los recursos a través del software abren la flexibilidad para habilitar más fácilmente características de resiliencia como el almacenamiento duradero y el equilibrio de carga entre distintas ubicaciones geográficas.

Aquí hay una gran variedad de opciones, y no todos los proveedores o plataformas son iguales, pero no se debe asumir que "la nube" como término general es más o menos resiliente que una infraestructura tradicional. A veces es mejor, a veces es peor, y conocer la diferencia se reduce a su evaluación de riesgos y a cómo usa el servicio en la nube.

Esta es la razón por la que generalmente es mejor volver a diseñar las implementaciones cuando las migra a la nube. Cambian tanto las propias necesidades de resiliencia, como las condiciones objetivas para alcanzarla. Se evitarán también así los fallos derivados de una relocalización directa al nuevo entorno de nube y se podrán aprovechar las ventajas específicas de las nuevas plataformas y servicios.

El objetivo es comprender y aprovechar las necesidades de *BC/DR* de la plataforma para que, una vez se tome la decisión de migrar a la nube, poder optimizar las nuevas capacidades de *BC/DR* disponibles en la nube antes de agregar capacidades adicionales a través de herramientas de terceros.

BC/DR debe tener en cuenta los diversos planos del servicio en la nube:

- *Meta-estructura:* Como las configuraciones de nube están controladas por software, debe disponerse de copia de seguridad de las mismas en un formato restaurable. Quizás no sea siempre posible, y es bastante raro en *SaaS*, pero existen herramientas para implementar esto en muchas plataformas *IaaS* (incluidos productos de terceros) que sea apoyan en esquemas de Infraestructura Definida por Software (*SDI*, *Software-Defined Infrastructure* en inglés).
  SDI: Permite crear plantillas de infraestructura para configurar todos o algunos aspectos de un despliegue en la nube. Estas plantillas se aplican directamente en la nube, o a través del uso de las *APIs* para orquestar la configuración. Este proceso debería incluir también los controles definidos (como *IAM* y registros), además del despliegue de la arquitectura, diseño de red o configuraciones de servicio.

- *Infraestructura:* Como se mencionó, cualquier proveedor de nube ofrecerá mecanismos para soportar mayor disponibilidad de servicio que la que se puede lograr de manera comparable en un centro de datos tradicional por el mismo coste. Pero estos mecanismos son efectivos en la arquitectura de servicio adecuada. La pura relocalización de servicios sin ajustes en la arquitectura, o rediseño de los mismos, a menudo resultarán en una disponibilidad menor.
  Asegúrese de comprender el modelo de costos de estas funciones, especialmente para implementarlas en las ubicaciones / regiones físicas del proveedor, donde el costo puede ser elevado. Algunos activos y datos se deben convertir para que funcionen en ubicaciones / regiones de la nube, por ejemplo, imágenes de máquinas personalizadas utilizadas para iniciar servidores. Estos activos deben estar incluidos en los planes.

- *Infostructura:* La sincronización de datos es a menudo uno de los problemas más difíciles de administrar en todas las ubicaciones, incluso si los costos reales de almacenamiento son manejables. Esto se debe al tamaño de los conjuntos de datos (frente al tamaño de los datos de configuración del servicio) y a la necesidad de mantener los datos sincronizados en todas las ubicaciones y servicios, algo que a menudo es difícil incluso en una única ubicación / sistema de almacenamiento.

- *Applistructure:* Este término incluye todo lo anterior, y también los activos de aplicaciones como código fuente, colas de mensajes, etc. Cuando un cliente construye sus propias aplicaciones en la nube, generalmente las desarrolla sobre servicios *IaaS* y / o *PaaS* proporcionados por el proveedor de nube, por lo que la resiliencia y la recuperación están inherentemente relacionadas con estos niveles de servicio. Pero la *Applistructure* incluye la gama completa de todo en una aplicación.

  Comprenda las limitaciones e implicaciones de *PaaS*, y planifique la interrupción de un componente de *PaaS*. Los proveedores de nube suelen proporcionar una gama de funciones disponibles para su integración por el cliente en aplicaciones: desde sistemas de autenticación hasta colas de mensajes y notificaciones. No es extraño que las

aplicaciones más modernas incluso integren este tipo de servicios por defecto y desde múltiples proveedores diferentes de la nube, creando una aplicación web más compleja.

Es razonable que desee discutir la disponibilidad de un componente o servicio con sus proveedores de nube. Por ejemplo, el servicio de base de datos de su proveedor *PaaS* puede tener distinto rendimiento y disponibilidad que un *IaaS* o una máquina virtual.

Cuando el cambio automático en el punto de prestación del servicio en la nube en tiempo real no es posible, diseñe su aplicación para una interrupción de servicio ordenada. Hay muchas técnicas de automatización para apoyar esto. Por ejemplo, si su servicio de cola se cae, eso debería disparar detener el "*front-end*" para que los mensajes no se pierdan.

En todo caso, siempre existe la opción de interrumpir el servicio por un tiempo. No siempre es imprescindible tener una disponibilidad sin interrupciones, pero si no puede aceptar una interrupción, asegúrese al menos de una caída ordenada del servicio, incluyendo en el servicio páginas de notificación de caída. Esto puede ser posible usando un servicio estático de emergencia al que se redirige el servicio vía *DNS*.

La metodología "*Chaos Engineering*" se usa a menudo para ayudar a desarrollar implementaciones de nube resilientes. Debido a que toda la nube está basada en *APIs*, *Chaos Engineering* usa herramientas para degradar selectivamente porciones de la nube para probar continuamente la continuidad del negocio.
Esto a menudo se realiza en producción, no solo en el entorno de prueba, y obliga a los ingenieros a asumir el error en lugar de verlo como un posible evento. Al diseñar sistemas para fallos, puede absorber mejor los fallos de componentes individuales.

6.1.2.2 Continuidad del negocio por la pérdida del proveedor de la nube

Siempre es posible una caída completa de un proveedor de nube, o al menos una parte importante de su infraestructura (como una geografía específica). La planificación de cómo afrontar la interrupción completa del proveedor de nube es difícil, debido a la tendencia natural de optimizar los servicios, adaptándolos a las mejoras de servicio del proveedor y la dificultad de alternativas esta situación. A veces puede migrar a una parte diferente de su servicio, pero en otros casos una migración interna simplemente no es viable, o se está absolutamente atado al proveedor.

Dependiendo del historial de incidentes de un proveedor en la nube, y sus capacidades de disponibilidad interna, puede ser adecuado la aceptación de este riesgo.

Asumir el corte de servicio puede ser otra opción, pero depende de los objetivos de tiempo de recuperación (*RTO*). En todo caso, debería disponerse de un servicio estático de información sobre la caída del servicio a través de una redirección *DNS*. El corte ordenado de servicio debería también incluir recibir y responder los accesos vía *API*, si el servicio ofrece *APIs*.

Tenga cuidado al seleccionar un proveedor o servicio secundario, si dicho servicio *SaaS* o *PaaS* también puede ubicarse o depender del mismo proveedor *IaaS* que el proveedor o servicio primario. No sirve de nada utilizar un proveedor secundario que falle a la vez que el proveedor principal cuando falle su proveedor de infraestructura, en el que ambos de apoyan.
Mover datos entre proveedores puede ser difícil, pero puede ser más fácil que mover la meta-estructura, los controles de seguridad, el registro, etc., que además pueden ser incompatibles entre plataformas.

Los servicios *SaaS* son a menudo la mayor preocupación de interrupción del servicio, puesto que dependen totalmente del proveedor. La extracción y el archivo programado de datos pueden ser su única opción de *BC* distinta de aceptar un corte de servicio. Extraer y archivar los datos en otro servicio en la nube, especialmente IaaS / *PaaS*, puede ser una mejor opción que hacerlo en instalaciones propias. Nuevamente, adopte un enfoque basado en el riesgo que incluya el historial específico de su proveedor.

Incluso si conserva sus datos, planifique disponer de una aplicación alternativa en la que sepa que puede recuperar sus datos. Si no puede usar los datos recuperados, no tiene una estrategia de recuperación viable.

Pruebe, pruebe y pruebe. Esto a menudo será más fácil que hacerlo en un centro de datos tradicional porque no está limitado por los recursos físicos disponibles, y puede añadir recursos adicionales que solo paga durante el periodo de la prueba.

6.1.2.3 Continuidad del negocio para la nube privada y los proveedores

Esto depende completamente del proveedor, y *BC/DR* debe incluir también todo lo relacionado con las instalaciones físicas. Los *RTO* y *RPO* serán estrictos, ya que, si la nube se cae, todos los servicios quedan interrumpidos.

Si está prestando servicios a otros, tenga en cuenta al construir sus planes de *BC* todos los requisitos contractuales, incluida la ubicación física de los datos. Por ejemplo, mover los datos durante la activación de la *BC* a una geografía diferente en una jurisdicción legal diferente puede violar contratos o leyes locales.

6.2 Recomendaciones

- Seguridad del Plano de Gestión (meta-estructura)
    - Asegúrese de que haya una sólida seguridad perimetral para conexiones con las *APIs* y las consolas web.
    - Use autenticación fuerte y *MFA*.
    - Mantenga un control estricto de las credenciales de las cuentas de super-usuario y las personas con acceso a las mismas y considere la doble autoridad para acceder a ellas.

        - Establecer cuentas múltiples con su proveedor ayudará a establecer permisos de granularidad suficiente en las distintas cuentas y a limitar el impacto de posibles incidentes (con *IaaS* y *PaaS*).
    - Use super-administradores y cuentas de administrador diarias separadas en lugar cuenta de super-administrador para todas las tareas.
    - Implemente sistemáticamente cuentas con mínimos privilegios para el acceso a la meta-estructura.
        - Esta es la razón por la que existen cuentas de acceso separadas de las de proveedor para desarrollo y para pruebas en la nube.
    - Utiliza *MFA* siempre que esté disponible.

- Continuidad del negocio
    - Diseñe una arquitectura de servicio que tenga en cuenta posibles fallos.
    - Adopte siempre un enfoque basado en el riesgo. Esto supone que, en el peor escenario, puede ser aceptable un corte de servicio o indisponibilidad parcial.
    - Incluya la alta disponibilidad de su proveedor de nube en el diseño de su servicio. En *IaaS* y *PaaS* esto a menudo es más fácil y más rentable que el equivalente en la infraestructura tradicional.
        - Aproveche las funciones específicas del proveedor.
        - Comprenda el historial de incidentes, las capacidades y las limitaciones del proveedor.
        - Debe considerarse siempre la opción de prestar el servicio desde dos ubicaciones, pero valorando el coste asociado a los requisitos de disponibilidad.
            - También asegúrese de que activos tales como imágenes o identificadores de activos se transforman para trabajar en las diferentes ubicaciones.
        - La continuidad del negocio de la meta-estructura es tan importante como la de los activos.
    - Prepárese para una caída ordenada en caso de una interrupción del servicio del proveedor de la nube.
        - Esto puede incluir planes de interoperabilidad y portabilidad del servicio a otros proveedores de nube o al mismo proveedor en una región de servicio diferente.
    - Para aplicaciones de muy altas necesidades de disponibilidad, pruebe primero con *BC* con el mismo proveedor en dos ubicaciones antes de intentar *BC* con otro proveedor.
    - Los proveedores de nube, incluida los de nube privada, deben proporcionar los niveles más altos de disponibilidad y mecanismos para que sus clientes puedan gestionar la disponibilidad de sus propios servicios.

Dominio 7 Seguridad de la Infraestructura

7.0 Introducción

La seguridad de la infraestructura es clave para operar de forma segura en la nube. La "infraestructura" es la unión de servidores y redes sobre la que se construye la nube. Para el propósito de esta Guía, se comienza con la seguridad de la computación y las redes, que incluye a su vez la carga de trabajo (*workload*) y las nubes híbridas. Aunque la seguridad en el almacenamiento es también una parte integral de la infraestructura, este aspecto se trata en profundidad en el Dominio 11: Seguridad de los datos y Cifrado. Este dominio cubre también las bases de la computación privada en la nube. No se tratan en esta Guía los aspectos de la seguridad tradicional de CPD, ya cubiertos por las guías y estándares existentes.

La seguridad de la infraestructura abarca las capas más inferiores de la seguridad, desde las instalaciones físicas hasta la configuración e implementación de los componentes de la infraestructura por parte del cliente. Estos son los componentes fundamentales sobre los que se construye la nube, incluyendo la seguridad de computación (carga de trabajo), redes y almacenamiento.

Para los propósitos de la Guía CSA nos enfocaremos en los aspectos específicos, relacionados con la nube, de la seguridad de la infraestructura. Existen en la actualidad corpus de conocimiento bien establecidos, así como estándares de la industria para la seguridad de CPD que los proveedores de servicios en la nube y los despliegues de nubes privadas pueden usar como referencia. Esta Guía debería considerarse como una capa adicional añadida sobre los extensos materiales disponibles ya existentes. De forma específica, este Dominio trata dos aspectos: consideraciones específicas de la nube para infraestructura subyacente y seguridad para redes y cargas de trabajo virtuales.

7.1 Visión general

En la computación en la nube se puede diferenciar dos capas con relación a la infraestructura:

- Los recursos básicos empleados para crear una nube. Se trata de los recursos lógicos (procesadores, memoria, etc.) redes y almacenamiento en bruto empleados para crear los grupos de recursos de la nube. Se incluyen, por ejemplo, la seguridad del software y hardware de red empleados para crear el grupo de recursos de red.
- La infraestructura abstracta o virtual gestionada por un usuario de la nube. Se trata de los activos de computación, red o almacenamiento reservados de los grupos de

recursos. Por ejemplo, la seguridad de una red virtual, tal y como es definida y gestionada por el usuario de la nube.

La información y consejos de este dominio se centran principalmente en la segunda capa, la seguridad de la infraestructura para el usuario de la nube. La seguridad de la infraestructura, más crítica para los proveedores de servicios en la nube (incluyendo aquellos que gestionan nubes privadas), está bien alineada con los estándares de seguridad para CPD ya existentes.

7.2 Virtualización de redes en la nube

En todas las categorías de nubes se hace uso de algún tipo de red virtual para abstraer la red física y crear de esta forma un grupo de recursos de red. Habitualmente el usuario de la nube aprovisiona los recursos de red deseados de este grupo, que puede configurarse dentro de los límites de la técnica de virtualización empleada. Por ejemplo, algunas plataformas en la nube solo permiten la asignación de direcciones IP dentro de subredes particulares, mientras que otras permiten al usuario de la nube la capacidad de aprovisionar redes virtuales de clase B enteras, así como definir por completo la arquitectura de la subred.

En el caso de un proveedor de servicios en la nube (incluyendo la gestión de nubes privadas), la segregación física de las redes que componen la nube es importante por motivos tanto de seguridad como operativos. Se observan habitualmente tres tipos de redes que se aíslan en distinto hardware para no tener ningún solape ni de tráfico ni funcional:

Gestión	• Del plano de gestión a los nodos
Almacenamiento	• De los nodos de almacenamiento (volúmenes) a los nodos de cómputo (instancias)
Servicio	• De Internet a los nodos de cómputo • Conexión entre instancias

Redes comunes subyacentes a IaaS

- La red de gestión para tareas de gestión y el tráfico de las *API*.
- La red de almacenamiento que conecta el almacenamiento virtual con las máquinas virtuales.
- La red de servicio que comunica las máquinas virtuales a Internet. Es la base del grupo de recursos de red para los usuarios de la nube.

Esta no es la única forma de construir una arquitectura de red privada en la nube, pero constituye un punto de partida común, especialmente para nubes privadas que no cuentan con el escalado masivo de los proveedores de nube pública públicos, pero aun así necesitan lograr un equilibrio entre rendimiento y seguridad.

En la actualidad existen dos grandes categorías de virtualización de redes para la computación en la nube:

- Redes de área local virtuales (*VLAN*): Las *VLAN* aprovechan las tecnologías de red ya existentes en gran parte del hardware de red actual. Las *VLAN* son ampliamente utilizadas en redes corporativas, incluso sin computación en la nube. Se emplean para segregar distintas unidades de negocio o funciones (como una red de invitados) dentro de redes de un solo propietario (CPD corporativos). Las *VLAN* no están diseñadas para la virtualización o seguridad a nivel de nube, no debiendo ser consideradas, por sí mismas, un control efectivo de seguridad para el aislamiento entre redes. Tampoco se consideran un sustituto a la segregación física de redes.

- Redes Definidas por Software (*SDN*, *Software Defined Networking*): Una capa de abstracción más completa, sobre el hardware de red, las *SDN* desacoplan el plano de control, de la red del de datos (se puede leer más sobre las bases de las *SDN* en su entrada en Wikipedia[1]). Esto permite abstraer las redes de las limitaciones tradicionales de una *LAN* (red de área local).

Existen múltiples implementaciones, tanto basadas en estándares como propietarias. Dependiendo de la implementación, las *SDN* pueden ofrecer una mayor flexibilidad y aislamiento. Por ejemplo, múltiples rangos de IP con solapamiento de direcciones, pero segregados para varias redes virtuales dentro de la misma red física. Si se implementan debidamente, a diferencia de las *VLANs* estándar, las *SDN* ofrecen un aislamiento de seguridad efectivo. Las *SDN* suelen ofrecer a su vez la posibilidad de definir arbitrariamente rangos de IP vía software, permitiendo a los clientes extender mejor sus redes existentes en la nube. Si el cliente necesita el rango 10.0.0.0/16 *CIDR* (*Classless Inter-Domain Routing*), una *SDN* es capaz de soportarlo independientemente del direccionamiento de red subyacente. Puede incluso soportar múltiples clientes usando los mismos bloques de direcciones IP internas.

A simple vista, una *SDN* puede parecer como una red normal a ojos del usuario de la nube, pero al tratarse de una abstracción más completa, funcionará internamente de forma completamente diferente. Las tecnologías subyacentes y la gestión de la *SDN* serán bastante más complejas, no pareciéndose en nada a lo que el usuario de la nube emplea. Por ejemplo, una *SDN* puede utilizar encapsulado de paquetes para que las máquinas virtuales y otros activos "estándar" no necesiten cambios en su pila de protocolos de red. La pila de virtualización recoge los paquetes de los sistemas operativos (SO) estándar conectándolos a través de un interfaz de red virtual, y los encapsula para moverlos dentro de la red real. La

[1] https://es.wikipedia.org/wiki/Redes_definidas_por_software

máquina virtual no necesita tener ningún conocimiento de la *SDN* más allá de un interfaz de red virtual compatible, que es facilitado por el hipervisor.

7.3 Cómo cambia la seguridad con las redes en la nube

La falta de una gestión directa de la red física subyacente afecta a las prácticas habituales de operación y gestión de red, tanto para el usuario como para el proveedor de la nube. Los patrones de seguridad de red más ampliamente utilizados dependen del control de las rutas de comunicación y de la interposición de dispositivos de seguridad. Esto no es factible para los clientes de la nube dado que solo operan a un nivel virtual.

Los sistemas de detección de intrusiones tradicionales (*IDS*), que reciben una copia de las comunicaciones entre equipos y las inspeccionan, no son compatibles en entornos en la nube: las herramientas de seguridad de los clientes deben depender de dispositivos virtuales interpuestos o de agentes de software instalados en las instancias. Esta situación crea cuellos de botella o aumenta el consumo del procesador, por lo que se debe asegurar que este nivel de monitorización es necesario antes de su implementación. Algunos proveedores de servicios en la nube pueden ofrecer algún tipo de monitorización de red integrada (y suelen existir más opciones en plataformas de nube privada), pero generalmente no suelen llegar al mismo nivel que la captura directa del tráfico en una red física.

7.3.1 Retos de los dispositivos virtuales

Puesto que el entorno de nube no es posible implantar dispositivos físicos interpuestos (excepto por los proveedores de la nube), deberán reemplazarse por dispositivos virtuales si todavía fueran imprescindibles y si la red en la nube soporta el enrutamiento necesario. Esto genera las mismas preocupaciones que la inserción de dispositivos virtuales para la monitorización de red:

- Los dispositivos virtuales se pueden convertir en cuellos de botella, ya que deben interceptar todo el tráfico sin poder dejar paso en caso de fallo.
- Los dispositivos virtuales pueden suponer un consumo significativo de recursos y suponer un aumento de costes para alcanzar los requisitos de rendimiento de red deseados.
- En caso de utilizarse dispositivos virtuales, deben soportar el auto-escalado a fin de igualar la elasticidad de los recursos que protegen. Dependiendo del producto, esto puede causar problemas si el fabricante no soporta un licenciamiento elástico compatible con el auto-escalado.
- Los dispositivos virtuales deben ser conscientes de su operación en la nube, así como de la capacidad de las instancias de moverse entre diferentes zonas geográficas o de disponibilidad. La velocidad del cambio en las redes en la nube es más alta que la de

las redes físicas, y las herramientas deben ser diseñadas teniendo en cuenta esta diferencia tan relevante.

- Los componentes de las aplicaciones en la nube tienden a estar distribuidos a fin de mejorar la resiliencia y, debido al auto-escalado, los servidores virtuales pueden tener tiempos de vida más cortos y ser más prolíficos. Esto afecta al diseño de las políticas de seguridad:
    - Las herramientas de seguridad deben ser capaces de gestionar altas tasas de cambio (por ej. servidores con tiempos de vida inferiores a una hora).
    - Las direcciones IP pueden cambiar con mucha más rapidez que en una red tradicional, algo que las herramientas de seguridad deben tener en cuenta. Idealmente los activos en la red deberían identificarse por un ID único, no por una dirección IP o un nombre de red.
    - Es menos frecuente que los activos tengan direcciones IP estáticas. Distintos activos pueden compartir la misma dirección IP por un corto periodo de tiempo. Los ciclos de vida tanto de la gestión de alertas como la respuesta ante incidentes deben ser modificados para garantizar que las alertas son operativas dentro de entornos tan dinámicos. Los activos existentes dentro de una única capa de aplicación pueden estar a menudo localizados en múltiples subredes por motivos de resiliencia, complicando aún más las políticas de seguridad basadas en direcciones IP. Debido al auto-escalado, los activos pueden ser efímeros, existiendo unas horas o incluso minutos. En el lado positivo, las arquitecturas en la nube suelen utilizar menos servicios por servidor, algo que mejora la capacidad de definir reglas de cortafuegos restrictivas. En lugar de una pila de servicios en una sola máquina virtual – como se hace en los servidores físicos, donde es necesario maximizar la inversión en el hardware – es práctica común ejecutar un conjunto más reducido de servicios, o incluso un único servicio, en una máquina virtual.

7.3.2 Beneficios de seguridad de las *SDN*

En el lado positivo, las redes definidas por software permiten establecer nuevos tipos de controles de seguridad, constituyendo en general una mejora de la seguridad de red:

- El aislamiento es más sencillo. Se pueden construir tantas redes aisladas como sea necesario sin restricciones debidas al hardware físico. Por ejemplo, si se ejecutan múltiples redes con los mismos rangos de direcciones CIDR, no hay forma lógica de que puedan comunicarse directamente debido a conflictos de direccionamiento. Esta es una forma excelente de segregar aplicaciones y servicios para diferentes contextos de seguridad. La micro-segmentación se comentará en mayor detalle más adelante.

- Los cortafuegos *SDN* (por ejemplo, los grupos de seguridad) pueden aplicarse a activos basándose en criterios más flexibles que los cortafuegos basados en hardware, ya que

éstos no están limitados a topologías físicas (esto aplica a muchos tipos de cortafuegos de software, pero no así en cortafuegos hardware). Los cortafuegos *SDN* establecen, generalmente, conjuntos de políticas que definen reglas de entrada y salida que pueden aplicarse a activos únicos o a grupos de activos, independientemente de su localización en la red (dentro de una red virtual dada). Por ejemplo, es posible crear un conjunto de reglas de cortafuegos que se apliquen a cualquier activo con una etiqueta específica. Es necesario tener en cuenta que cada plataforma emplea una terminología distinta y utiliza diferentes tecnologías para soportar esta capacidad, por lo que estos aspectos se tratan a nivel conceptual.

- Junto con la capa de orquestación de la plataforma en la nube, permiten combinaciones y políticas muy dinámicas y granulares, con menos sobrecostes de gestión que los cortafuegos hardware tradicional o aproximaciones basadas en servidor. Por ejemplo, si las máquinas virtuales en un grupo de auto-escalado se despliegan automáticamente en múltiples subredes con balanceo de carga entre ellas, es posible crear un conjunto de reglas de cortafuegos que se aplique a estas instancias independientemente de su subred o dirección IP. Es una característica clave para el establecimiento de redes seguras en la nube, que utiliza arquitecturas muy diferentes a la computación tradicional.
- Generalmente se comienza denegando por defecto todas las conexiones, siendo necesario empezar a abrirlas, al contrario que en la mayoría de las redes físicas.
    - Pensemos en la granularidad de un cortafuegos de servidor unido a las ventajas en la gestión de un dispositivo de red. Los cortafuegos de servidor tienen dos problemas: son difíciles de manejar a gran escala, y si el sistema en el que residen se ve comprometido son fácil de alterar o deshabilitar. Adicionalmente, el coste de enrutar todo el tráfico interno (incluso dentro de pares desde la misma subred) a través de un cortafuegos de red es prohibitivo. Los cortafuegos basados en software, como los grupos de seguridad, se gestionan desde fuera de un sistema, pero, aun así, se aplican a cada sistema sin costes adicionales de hardware ni necesidades complejas de aprovisionamiento. De esta manera se pueden realizar tareas, como aislar cada máquina virtual de una misma subred virtual, de manera sencilla.
    - Como se mencionado previamente, las reglas de cortafuegos pueden basarse en otros criterios, como por ejemplo etiquetas. Es necesario tener en cuenta que, aunque el potencial existe, las capacidades reales dependen de cada plataforma. Solo porque una red en nube esté basada en *SDN* no implica que sea segura.
    - Por defecto se eliminan muchos ataques de seguridad (dependiendo de la plataforma), como el ARP *spoofing* y otros *exploits* a bajo nivel, más allá de simplemente eliminar el *sniffing*. Esto se debe a la naturaleza inherente del *SDN* y la aplicación de más reglas basadas en software y análisis de los paquetes en tránsito.
    - Es posible el cifrado de paquetes a medida que se encapsulan.

- Como en el caso de los grupos de seguridad, otros diseños de enrutado y red pueden ser dinámicos y vinculados a la capa de orquestación de la nube, como puentes entre redes virtuales o conexiones a servicios internos *PaaS*.
- Existe el potencial de añadir nuevas funciones de seguridad de forma nativa.

7.3.3 Micro-segmentación y el Perímetro Definido por Software (*SDP*)

La micro-segmentación (en ocasiones denominada hiper-segregación) aprovecha las topologías de redes virtuales para ejecutar más redes, más pequeñas y más aisladas, sin incurrir costes adicionales de hardware que, históricamente, hacían que estos modelos fueran prohibitivos. Dado que todas las redes están definidas mediante software, sin muchos de los típicos problemas de direccionamiento, es más factible ejecutar estos entornos múltiples definidos por software.

Un ejemplo práctico y habitual basado en esta capacidad, es el de ejecutar muchas, o incluso todas, las aplicaciones en su propia red virtual y solo conectar esas redes cuando sea necesario. Esta medida reduce drásticamente el área de impacto si un atacante compromete un sistema individual, ya que no puede aprovechar la posición ganada para expandirse por todo el CPD.

Aunque no hay un incremento en los costes de inversión, ya que la micro-segmentación se basa en configuraciones de software, es posible tener un incremento en los costes operacionales debido a la gestión y conectividad de múltiples redes solapadas.

Un grupo de trabajo del CSA (*SDP working group*) ha desarrollado un modelo y una especificación que combina autenticación de dispositivo y de usuario para aprovisionar, de forma dinámica, accesos de red a los recursos y mejorar la seguridad. *SDP* incluye tres componentes:

- Un cliente de *SDP* en el activo que inicia la conexión (por ejemplo, un portátil).
- Un controlador de *SDP* para la autenticación y autorización de clientes *SDP* y la configuración de las conexiones con las puertas de enlace *SDP*.
- Una puerta de enlace *SDP* donde termina el tráfico de red del cliente y se hace cumplir las políticas de comunicación con el controlador *SDP*.

De esta forma, las decisiones de seguridad de red pueden tomarse basadas en un rango de criterios más amplio que únicamente usando paquetes IP. Combinado con *SDN*, ofrece potencialmente una mayor flexibilidad y seguridad en topologías de red en evolución.

CSA dispone de más información sobre *SDP* en
https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview

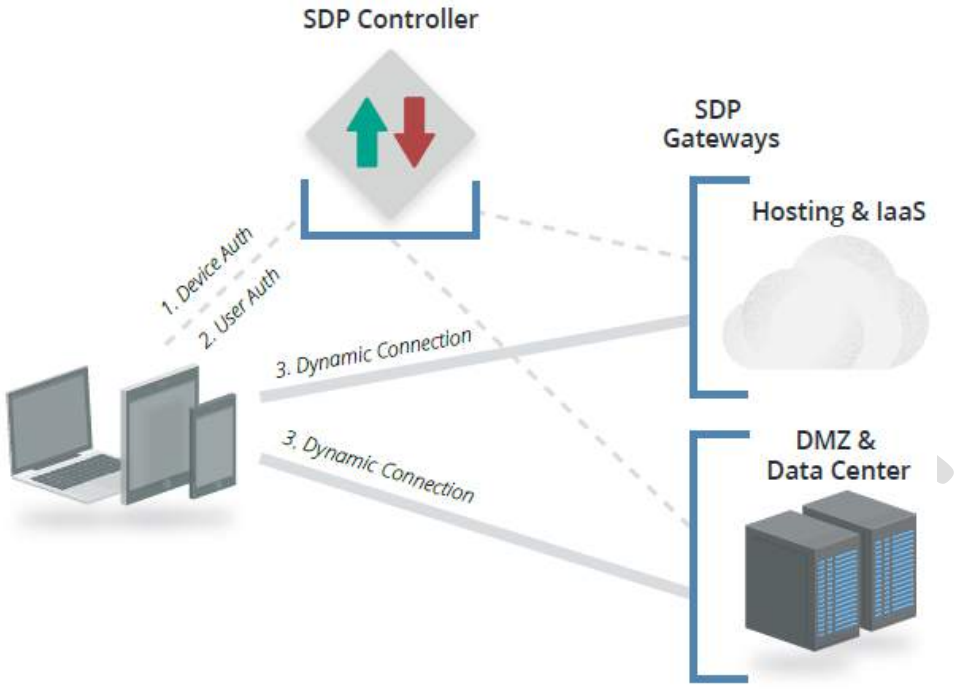


FIGURA *SDP*
Translate
1.- Autentica dispositivo
2.- Autentica Usuario
3.- Conexión dinámica
SDP Controller → controlador *SDP*
SDP Gateway → Puerta de enlace *SDP*
Hosting & IaaS → Hosting & *IaaS*
DMZ & Data Center → MDZ y Centro de Datos.

7.3.4 Consideraciones adicionales para proveedores en la nube o nubes privadas

Los proveedores deben mantener la seguridad básica de las redes físicas/tradicionales sobre las que se construye la plataforma. Un fallo de seguridad en la red física base podría probablemente suponer el compromiso de todos los clientes. Y esta seguridad debe ser gestionada para comunicaciones arbitrarias y múltiples clientes, algunos de los cuales pueden tener políticas contradictorias.

Es absolutamente crítico mantener la segregación y el aislamiento en entornos con múltiples clientes (*tenants*). Así pues, existirán sobrecostes adicionales destinados a mantener, configurar y habilitar de forma apropiada los controles de seguridad de la *SDN*. Aunque una *SDN*, una vez puesta en marcha, es más propensa a ofrecer el aislamiento necesario, es importante emplear el tiempo y los recursos necesarios para tener una configuración apropiada que permita manejar clientes (*tenants*) potencialmente hostiles. No estamos diciendo que los usuarios sean necesariamente hostiles, pero es sensato asumir que, en cierto momento, algún elemento en la red será comprometido y utilizado para profundizar un ataque.

Los proveedores deben ofrecer controles de seguridad a los usuarios de la nube, de forma que estos puedan configurar y gestionar su seguridad de red de forma apropiada.

Por último, los proveedores son responsables de implementar una seguridad perimetral que proteja el entorno, pero minimice el impacto en las cargas de trabajo de los clientes, por ejemplo, protecciones contra ataques de denegación de servicio distribuidos (*DDoS*), e *IPS* básicos que filtren el tráfico hostil antes de que afecte a las nubes de los clientes. Otra consideración a tener en cuenta es que se debe garantizar que cualquier dato sensible es eliminado cuando una instancia virtual se libera, asegurando que ningún otro cliente puede leer dicha información cuando el espacio en disco vuelve a ser aprovisionado.

7.3.5 Consideraciones para nubes híbridas

Como se ha mencionado en el Dominio 1, las nubes híbridas conectan una nube corporativa privada o CPD con la nube pública de un proveedor, habitualmente mediante una *VPN* o un enlace *WAN* (*Wide Area Network*). Idealmente la nube privada soportará direccionamientos de red arbitrarios para poder ayudar a extender de forma transparente la red del usuario en la nube. Si la nube utiliza el mismo rango de red que los activos locales, estos no podrán utilizarse.

La conexión con la nube híbrida puede reducir la seguridad de la red de la nube si la red privada no mantiene un nivel de seguridad equivalente. Si se emplea una red plana en un CPD, sin apenas segregación entre los sistemas de los empleados, un atacante podría comprometer el equipo de un empleado y usarlo para atacar todo el despliegue en la nube a través de la conexión con la nube híbrida. Una conexión híbrida no debería relajar la seguridad de ambas redes. La separación debería forzarse mediante enrutado, controles de acceso o incluso cortafuegos o herramientas de seguridad adicionales entre ambas redes.

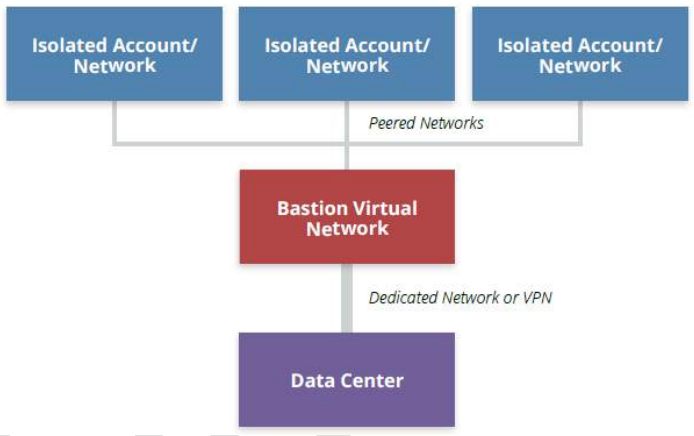
Generalmente es preferible minimizar las conexiones híbridas por motivos de gestión y seguridad. Conectar múltiples redes dispares es complicado, especialmente cuando una de esas redes es definida por software y la otra está basada en hardware. Las conexiones híbridas son a menudo todavía necesarias, pero no hay que asumir que sean obligatorias. Pueden incrementar la complejidad del enrutado, reducir la capacidad de ejecutar múltiples redes en la

nube con rangos de IP que se solapen, y complicar la seguridad en ambos lados debido a la necesidad de armonizar los controles de seguridad.

Una arquitectura emergente para la conectividad de nubes híbridas son las redes virtuales de "bastión" o de "tránsito":

- Este escenario permite conectar varias redes de nubes diferentes a un CPD usando una única conexión híbrida. El usuario de la nube crea una red virtual dedicada para la conexión híbrida y luego conecta cualquier otra red a través de la red bastión designada.

- Las redes de segundo nivel se conectan al CPD a través de la red bastión, pero dado que no están conectadas no pueden hablar entre ellas, quedando así segregadas de forma efectiva. Adicionalmente se pueden desplegar en la red bastión diferentes herramientas de seguridad, reglas de cortafuegos y *ACL* (Listas de Control de Accesos) para una mayor protección del tráfico dentro y fuera de la conexión híbrida.



Redes "bastión" o de "tránsito" para arquitecturas nube híbridas más flexibles

Translate
Isolated Account / Network → Segmento externo independiente

Peered networks → Redes conectadas
Bastion Virtual Network → red bastión
Dedicated Network or *VPN* → conexión punto a punto / *VPN*

Data center → Centro de Datos.

7.4 Seguridad en la computación y carga de trabajo en la nube

Se define la carga de trabajo (*workload*) como una unidad de procesado, que puede estar en una máquina virtual, un contenedor u otra abstracción. Las cargas de trabajo siempre se ejecutan en algún procesador y consumen memoria. Las cargas de trabajo abarcan una amplia gama de tareas de procesado, desde aplicaciones tradicionales corriendo en una máquina virtual bajo un sistema operativo estándar a tareas especializadas basadas en GPU o FPGA. Prácticamente todas estas opciones están soportadas bajo una u otra forma de computación en la nube.

Es importante tener en cuenta que toda carga de trabajo en la nube se ejecuta en una pila hardware, siendo crítico para el proveedor de servicios en la nube mantener la integridad de dicho hardware. Cada pila de hardware además tiene diversas opciones para el aislamiento de la ejecución y el mantenimiento de la cadena de confianza, que pueden incluir entre otros: supervisión basada en hardware, procesos de monitorización que se ejecutan fuera de los procesadores centrales, entornos de ejecución seguros, enclaves de cifrado y gestión de claves, etc. La gama y naturaleza en continuo cambio de estas opciones excede nuestra capacidad de poder ofrecer recomendaciones restrictivas, pero en general, hay potencialmente grandes mejoras en la seguridad eligiendo y aprovechando el hardware con estas capacidades avanzadas.

Existen múltiples tipos de abstracción en computación, cada uno con diferentes grados de aislamiento y segregación:

- Máquinas virtuales (*VM*): Constituyen la forma más conocida de abstracción de computación, y se ofrecen por parte de todos los proveedores de *IaaS*. En la computación en la nube son conocidas comúnmente como instancias ya que son creadas (o clonadas) a partir de una imagen base. El gestor de máquinas virtuales (hipervisor) abstrae un sistema operativo del hardware subyacente. Los hipervisores modernos pueden basarse en las capacidades del hardware disponible actualmente en servidores estándar (y algunas estaciones de trabajo) para reforzar el aislamiento a la vez que soportan operaciones de alto rendimiento.
  Las máquinas virtuales están potencialmente sujetas a ciertos ataques a la memoria, pero estos ataques son cada vez más difíciles de llevar a cabo debido a las mejoras actuales de hardware y software, que mejoran el aislamiento. Las *VMs* en los hipervisores modernos son generalmente un control de seguridad efectivo, y los avances tanto en el aislamiento del hardware como en entornos de ejecución seguros continúan mejorando estas capacidades.

- Contenedores: Los contenedores son entornos de ejecución de código que se ejecutan (por ahora) dentro de un sistema operativo, compartiendo y aprovechando los recursos de dicho sistema. Mientras que una *VM* es una abstracción completa de un sistema operativo, un contenedor es un lugar restringido en el que ejecutar procesos de forma

segregada a la vez que se hace uso del *kernel* y otras capacidades del SO base. Se pueden ejecutar múltiples contenedores en una misma máquina virtual, o se pueden implementar sin usar *VMs*, ejecutándose directamente sobre hardware. El contenedor dispone código que se ejecuta de un entorno restringido, con acceso únicamente a los procesos y capacidades definidas en la configuración del contenedor. Esto permite que los contenedores funcionen increíblemente rápido dado que no necesitan arrancar un sistema operativo o lanzar muchos servicios nuevos (en ocasiones ninguno); el contenedor solo necesita acceder a los servicios ya existentes en el SO anfitrión, pudiendo algunos ejecutarse en milisegundos.

Los contenedores son más recientes que las *VM*, con distintas capacidades de aislamiento que dependen en gran medida de la plataforma. Están, a su vez, evolucionando rápidamente con diferentes sistemas de gestión, sistemas operativos subyacentes y tecnologías específicas. Los contenedores se cubren en profundidad en el Dominio 8.

- Cargas de trabajo basadas en plataformas: Esta es una categoría más compleja ya que cubre cargas de trabajo que se ejecutan en plataformas compartidas que no son ni máquinas virtuales ni contenedores, como procedimientos o lógica de código que se ejecutan en una base de datos compartida. Otros ejemplos pueden ser procedimientos almacenados que se ejecutan en una base de datos multi-usuario (*multi-tenant*), o un *job* de machine-learning ejecutándose en un entorno *PaaS* de machine-learning. La seguridad y el aislamiento son totalmente responsabilidad del proveedor de la plataforma, aunque éste puede ofrecer algunas opciones y controles de seguridad.

- Computación sin servidor (*serverless computing*): Esta amplia categoría hace referencia a cualquier situación en la que el usuario de la nube no gestiona ninguna de las máquinas virtuales o hardware subyacente, accediendo únicamente a una serie de funciones expuestas. Por ejemplo, hay plataformas sin servidor que directamente ejecutan código de aplicación. En el fondo se siguen usando capacidades como contenedores, máquinas virtuales u otras plataformas de hardware especializadas. Desde el punto de vista de la seguridad, las tecnologías sin servidor son meramente un término combinado que cubre los contenedores y las cargas de trabajo basadas en plataformas, donde el proveedor de servicios en la nube gestiona todas las capas inferiores, incluyendo los controles y funciones de seguridad estructurales.

7.4.1 Cómo la nube cambia la seguridad de la carga de trabajo

Dado un procesador y memoria determinados casi siempre estarán ejecutando múltiples cargas de trabajo, normalmente de diferentes usuarios. Es probable que múltiples usuarios compartan un mismo nodo de computación físico, con un rango de capacidades de segregación dependiente de la pila hardware. El peso de mantener el aislamiento de la carga de trabajo

recae sobre el proveedor de servicios en la nube y esta debería ser una de sus mayores prioridades.

En algunos entornos es posible disponer de recursos dedicados o privados, aunque habitualmente a un coste mayor. Si se usa este modelo, las cargas de trabajo elegidas se ejecutan en un procesador físico asignado de forma aislada. El coste para el consumidor se incrementa tanto en nubes públicas, donde se está reservando hardware específico del conjunto de recursos generales, como en nubes privadas, debido al uso menos eficiente de los recursos internos.

Los usuarios de la nube casi nunca controlan el lugar donde físicamente se ejecutan sus cargas de trabajo, independientemente del modelo de despliegue, aunque algunas plataformas soportan la designación de grupos de hardware particulares o localizaciones genéricas para facilitar la disponibilidad, cumplimiento u otros requisitos.

7.4.2 Las cargas de trabajo inmutables mejoran la seguridad

Los contenedores y el auto-escalado, por su naturaleza, trabajan mejor cuando se ejecutan instancias lanzadas dinámicamente a partir de una imagen; estas instancias pueden ser apagadas cuando ya no son necesarias por motivos de capacidad sin romper la pila de la aplicación. Este concepto es clave para la elasticidad de la computación en la nube. Así mismo, no se realizan cambios o aplican parches a una carga de trabajo en ejecución, ya que no afectarían a la imagen base y, por lo tanto, estarían desincronizadas, sea cual sea el cambio realizado, con las nuevas instancias lanzadas. Estas máquinas virtuales se denominan inmutables.
Para cambiar o reconfigurar una instancia inmutable es necesario actualizar la imagen subyacente, y a continuación ir rotando las instancias apagando las viejas y lanzando nuevas en su lugar.

Existen grados de inmutabilidad. La definición pura es la de reemplazar instancias en ejecución con una nueva imagen. Sin embargo, algunas organizaciones solo lanzan nuevas imágenes para actualizar el sistema operativo, empleando técnicas alternativas de despliegue de actualizaciones de código en las máquinas virtuales. Aunque técnicamente no son completamente inmutables ya que la instancia se ve modificada, estos despliegues ocurren de forma completamente automatizada, sin que nadie inicie sesión manualmente en los sistemas en ejecución para realizar cambios en local.

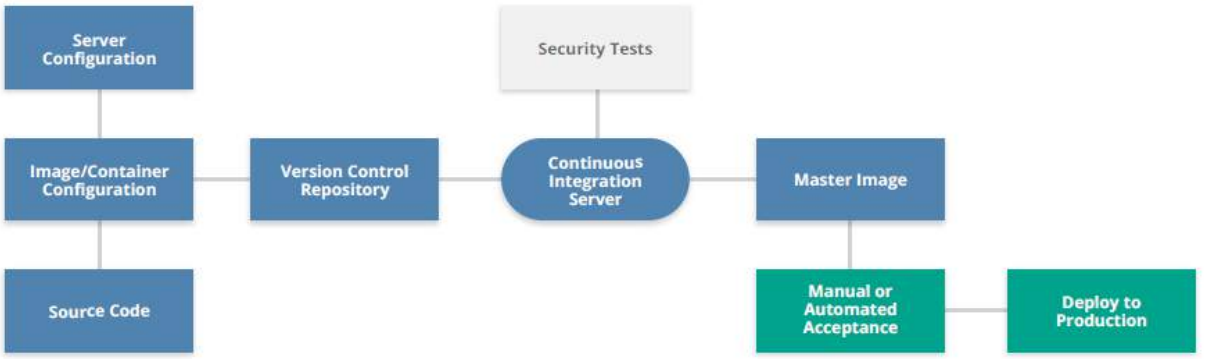
Las cargas de trabajo inmutables ofrecen beneficios de seguridad importantes:

- No es necesario aplicar parches a sistemas en ejecución o preocuparse acerca de dependencias o procesos de parcheo fallidos. Las instancias se reemplazan por una nueva imagen maestra.

- Se puede, y se debería, deshabilitar los inicios de sesión remotos a las cargas de trabajo en ejecución (si llegan a considerarse incluso como una opción). Este suele ser un requisito operacional para prevenir cambios que no sean consistentes a lo largo de toda la pila del sistema, pero que también repercute beneficiosamente en la seguridad.
- Desplegar versiones actualizadas es mucho más sencillo ya que las aplicaciones deben estar diseñadas para gestionar el hecho que algunos nodos puedan caerse (hay que recordar que esta capacidad es fundamental en cualquier esquema de auto-escalado). Se está menos limitado por la complejidad y fragilidad de parchear un sistema en ejecución, e incluso si algo se rompe debería poder ser reemplazado con facilidad.
- Es más fácil deshabilitar servicios o aplicar listas blancas de aplicaciones o procesos ya que la instancia no debería cambiar nunca.
- Gran parte de las pruebas de seguridad pueden realizarse durante la creación de la imagen, lo que reduce la necesidad de evaluar las vulnerabilidades en cargas de trabajo en ejecución, ya que su comportamiento debería de ser completamente conocido en el momento de su creación. Aunque no se eliminan todas las necesidades de pruebas de seguridad en producción, sí que pueden reducirse en gran parte.

Las instancias inmutables añaden algunos requisitos:

- Se necesita un proceso consistente de creación de imágenes, así como la automatización necesaria para la actualización de los despliegues. Estas imágenes deben ser generadas de forma regular para tener en cuenta las actualizaciones debidas a parches y firmas de malware.
- Las pruebas de seguridad deben integrarse en el proceso de creación de imágenes y despliegue, incluyendo análisis de código fuente y, si se emplean máquinas virtuales o contenedores estándar, evaluación de vulnerabilidades.
- La configuración de las imágenes necesita mecanismos para deshabilitar los inicios de sesión y restringir servicios antes de su despliegue y uso en máquinas virtuales en producción.
- En algunas cargas de trabajo se puede necesitar, para resolver algún posible problema, habilitar los inicios de sesión. Podría ser una carga de trabajo extraída del grupo, pero permitiendo que siga ejecutándose de forma aislada. Otra opción (generalmente preferida) es el envío de logs suficientemente detallados a un colector externo, eliminando la necesidad de los inicios de sesión.
- La complejidad de gestionar el catálogo de servicios se incrementa ya que es posible crear docenas o incluso cientos de imágenes un día cualquiera.



Un flujo de implantación para la creación de imágenes para contenedores o máquinas virtuales inmutables.

Server configuration → Configuración de servidor
Security tests → Pruebas de seguridad
Image/Container configuration → Configuración de imágenes/contenedores
Versión control repositorio → Repositorio de control de versiones
Continuous integration server → Servidor de integración continua
Master image → Imagen maestra
Source Code → Código fuente
Manual or Automated acceptance → Validación manual o automática

Deploy to Production → Pase a producción

7.4.3 El impacto de la nube en los controles de seguridad de la carga de trabajo

Algunos controles estándar de cargas de trabajo no son viables en entornos en la nube (por ejemplo, la ejecución de antivirus dentro de algunos tipos de contenedores). Otros controles no son realmente necesarios o necesitan de profundas modificaciones para mantener su efectividad en entornos en la nube:

- Se puede perder la capacidad de ejecutar agentes para cargas de trabajo no basadas en *VM*, como los que se ejecutan en contenedores sin servidor gestionados por el proveedor.
- Los agentes tradicionales tienen un impacto mayor sobre el rendimiento en la nube. Los agentes ligeros con requisitos de computación menores permiten una mejor distribución de la carga de trabajo y un uso eficiente de los recursos. Los agentes que no están diseñados para la computación en la nube pueden asumir una capacidad de cómputo que no se alinea con el diseño del despliegue en la nube. Los desarrolladores de un proyecto podrían asumir que están ejecutando una flota de máquinas virtuales ligeras y de único propósito. Un agente de seguridad que no esté ajustado a este entorno puede

incrementar los costes de proceso, requiriendo tipos de máquinas virtuales más grandes e incrementando los costes.

- Los agentes que operan en entornos en la nube también necesitan soportar cargas de trabajo en la nube dinámicas y patrones de despliegue como el auto-escalado. No puede depender (ni el agente ni el sistema de gestión) de direccionamientos IP estáticos. Aunque algunos activos en la nube se ejecutan en direcciones IP estáticas, es mucho más común que la nube asigne direcciones IP de forma dinámica para mejorar la elasticidad. Por ello, el agente debe tener la capacidad de encontrar el plano de control/gestión y emplearlo para determinar en qué clase de carga se está ejecutando y dónde.
- El plano de gestión del agente debe a su vez operar a la velocidad del auto-escalado y soportar la elasticidad (por ejemplo, siendo capaz de soportar direccionamientos IP increíblemente dinámico como una misma IP usada por múltiples cargas de trabajo durante la misma hora). Las herramientas tradicionales no suelen estar diseñadas para estas velocidades, y suponen el mismo problema ya visto con los cortafuegos y la seguridad de la red.
- Los agentes no deberían incrementar la superficie de ataque debido a comunicaciones/red u otros requisitos. Aunque esta afirmación debería ser siempre cierta, la probabilidad de que un agente en la nube se convierta en un riesgo de seguridad es mayor por las siguientes razones:
    - Se tiene una mayor facilidad para ejecutar sistemas inmutables, y un agente, como cualquier otra pieza de software, incrementa la superficie de ataque, especialmente si toma como entradas cambios en la configuración o firmas que pueden ser empleadas como vector de ataque.
    - Comparado con un servidor físico, en la nube se tiende a que cualquier máquina virtual o contenedor ejecute menos servicios distintos y con un conjunto de puertos de red menor. Algunos agentes necesitan abrir puertos adicionales en el cortafuegos, lo que aumenta la superficie de ataque de red.
    - Esto no significa que los agentes impliquen siempre nuevos riesgos de seguridad, sino que se tiene que valorar los beneficios antes de simplemente asumir una mejora en la seguridad.
- La monitorización de la integridad de ficheros puede ser una manera efectiva de detectar cambios no aprobados en instancias inmutables en ejecución. Las cargas de trabajo inmutables generalmente casi no requieren herramientas de seguridad adicionales, debido a su naturaleza bastionada. Están más protegidas que un servidor estándar y tienen a ejecutar un conjunto de servicios menor. La monitorización de la integridad de ficheros, que tiende a ser muy ligera, puede constituir un buen control de seguridad para cargas inmutables ya que su naturaleza no cambiante implica que se deberían tener esencialmente cero falsos positivos.
- Las *VM* de larga duración que todavía hacen uso de controles de seguridad estándar pueden aislarse dentro de la red, cambiando la forma en la que son gestionadas. Puede ser complicado conectar una herramienta de gestión a una máquina virtual que se ejecuta en una subred privada. Aunque técnicamente es posible ejecutar la herramienta

de gestión dentro de la misma subred, esto puede complicar la gestión e incrementar de forma significativa los costes.

- Las cargas de trabajo en la nube, ejecutándose de forma aislada, generalmente son menos resilientes que en una infraestructura física, debido a la abstracción. Es muy relevante proporcionar opciones de recuperación ante desastres para estas cargas de trabajo.

7.4.4 Cambios en el monitoreo de seguridad de las cargas de trabajo

Los registros/monitoreo de seguridad son más complejos en la computación en la nube:

- Las direcciones IP en un registro (log) no tienen por qué referirse a un flujo de trabajo en particular, ya que varias máquinas virtuales pueden compartir la misma dirección IP en un periodo de tiempo, y algunas cargas de trabajo, como contenedores, o cargas sin servidor, pueden incluso no tener una IP reconocible. Por lo tanto, es necesario emplear otro tipo de identificadores únicos en los registros, para de esta forma saber a qué se hacen referencia realmente. Estos identificadores únicos deben tener cuenta los sistemas efímeros, los cuales pueden estar activos únicamente por un corto periodo de tiempo.
- Los registros deben ser recogidos y descargados con una mayor frecuencia y rapidez debido a la mayor velocidad del cambio de la nube. Los registros de un grupo de auto-escalado pueden perderse con facilidad si no se recolectan antes de que el controlador de la nube apague una instancia que ya no es necesaria.
    - Las arquitecturas de registros deben de tener en cuenta los costes de la red y el almacenamiento en la nube. Por ejemplo, enviar todos los registros de las instancias de una nube pública al *SIEM* local (*Security Information and Event Management*) puede tener un coste prohibitivo debido a las tarifas adicionales de la red y a los costes del almacenamiento interno.

7.4.5 Cambios en la evaluación de vulnerabilidades

Las evaluaciones de seguridad en la computación en la nube deben de tener en cuenta las siguientes limitaciones, tanto contractuales, como de arquitectura:

- El propietario de la nube (ya sea pública o privada) necesitará una notificación de las evaluaciones y podrá limitar la naturaleza de las mismas. Esto es debido a que puede ser imposible distinguir una evaluación de un ataque real si no se dispone de un aviso previo.
- Las redes con políticas de denegación por defecto limitan aún más la efectividad potencial de una evaluación automatizada de la red, tal y como lo haría unos cortafuegos. Se necesita bien abrir agujeros en la red para realizar la evaluación, bien

emplear un agente en la instancia para su ejecución, o bien realizarla teniendo en cuenta que gran parte de las pruebas serán bloqueadas por las reglas del cortafuegos.

- Las evaluaciones pueden realizarse durante la creación de imágenes en el caso de cargas de trabajo inmutables. Dado que no están en producción y que el proceso está automatizado, estas pueden realizarse con menos restricciones de red incrementando el alcance objeto de la evaluación.
- Los test de intrusión se ven menos afectados ya que hacen uso del mismo alcance que un atacante. Se cubrirán en mayor detalle en el Dominio 10.

7.4.6 Seguridad del almacenamiento en la nube

Aunque forman parte de la infraestructura, la seguridad de los datos y el almacenamiento se tratan en profundidad en el Dominio 11.

7.5 Recomendaciones

- Conocer la seguridad de la infraestructura de la plataforma o proveedor:
    - En un modelo de seguridad compartida, el proveedor (o el responsable de mantener la plataforma de nube privada) tiene la responsabilidad de garantizar que las capas subyacentes física, abstracción y orquestación, son seguras.
    - Revisar las certificaciones y declaraciones de cumplimiento.
        - Comprobar periódicamente las certificaciones y declaraciones de cumplimiento, tanto las estándar como las específicas para la industria, para obtener garantías de que el proveedor está siguiendo las mejores prácticas y normativas relativas a la infraestructura en la nube.
- Red:
    - Cuando sea posible es preferible utilizar *SDN*.
    - Usar las capacidades de las *SDN* para crear múltiples redes virtuales o segmentos para incrementar el aislamiento de red.
        - La separación de cuentas y redes virtuales limitará dramáticamente el área de impacto comparado con los CPD tradicionales.
    - Implementar la denegación por defecto en los cortafuegos en la nube.
    - Aplicar cortafuegos en la nube en función de la carga de trabajo, en lugar de por redes.
    - Siempre que sea posible restringir el tráfico entre cargas de trabajo en la misma subred utilizando una política de cortafuegos en la nube (grupo de seguridad).

- Minimizar las dependencias de dispositivos virtuales que restrinjan la elasticidad o causen cuellos de botella en el rendimiento.

- Cómputo / carga de trabajo:

  - Hacer uso de cargas de trabajo inmutables siempre que sea posible.
    - Deshabilitar los accesos remotos.
    - Integrar las pruebas de seguridad en la creación de imágenes.
    - Generar alarmas basadas en la monitorización de la integridad de ficheros.
    - Parchear actualizando imágenes, no instancias en ejecución.
    - Si son necesarios, elegir agentes de seguridad que sean compatibles con la nube y que minimicen el impacto sobre el rendimiento.
  - Mantener controles de seguridad para las cargas de trabajo de larga duración, pero haciendo uso de herramientas compatibles con la nube.
  - Almacenar los registros fuera de las cargas de trabajo.
  - Comprender y cumplir con las limitaciones de los proveedores de servicios en la nube con relación a las evaluaciones de seguridad y los test de intrusión.

Dominio 8 Virtualización y Contendores

8.0 Introducción

La virtualización no es simplemente una herramienta para crear máquinas virtuales: es la tecnología fundamental que permite la computación en la nube. Utilizamos la virtualización en muchos aspectos de la informática, desde las máquinas virtuales completamente operativas, hasta los entornos de ejecución virtuales como la Máquina Virtual de Java, así como también en el almacenamiento, las redes y otras.

La computación en la nube se basa fundamentalmente en la agrupación de recursos, y la virtualización es la tecnología utilizada para convertir la infraestructura fija en estos recursos agrupados. La virtualización proporciona la abstracción necesaria para los grupos de recursos, que luego se gestionan mediante la orquestación.

Como se mencionó, la virtualización cubre una gama muy amplia de tecnologías; en esencia, cada vez que creamos una abstracción, estamos utilizando la virtualización. Para la computación en la nube, tendemos a enfocarnos en los aspectos específicos de la virtualización utilizados para crear nuestros grupos de recursos, especialmente:

- Computación
- Red
- Almacenamiento
- Contenedores

Estas no son las únicas categorías de virtualización, pero son las más relevantes para la computación en la nube.

Es fundamental comprender los impactos de la virtualización en la seguridad para diseñar e implementar correctamente la seguridad en la nube. Los activos virtuales aprovisionados desde un grupo de recursos pueden parecerse a los activos físicos que reemplazan, pero esa apariencia es realmente una herramienta para ayudarnos a comprender y administrar mejor lo que vemos. También es una forma útil de aprovechar las tecnologías existentes, como los sistemas operativos, sin tener que reescribirlos completamente desde cero. Por debajo, estos activos virtuales funcionan de forma completamente diferente a los recursos de los que se abstraen.

8.1 Visión general

En esencia, la virtualización abstrae recursos de sus activos físicos subyacentes. Se puede virtualizar casi cualquier nivel de tecnología, desde computadoras enteras hasta redes e incluso código. Como se mencionó en la introducción, la computación en la nube se basa

fundamentalmente en la virtualización: es la forma en que abstraemos los recursos para crear grupos. Sin virtualización, no hay nube.

Muchos procesos de seguridad se diseñan en base a la existencia de un control físico sobre la infraestructura subyacente. Si bien esto no desaparece con la computación en la nube, la virtualización agrega dos nuevas capas a los controles de seguridad:

- *Seguridad de la propia tecnología de virtualización*, por ejemplo, protegiendo un hipervisor.
- *Controles de seguridad para los activos virtuales.* En muchos casos, deben implementarse de forma diferente de cómo ser haría en sus equivalentes físicos correspondientes. Por ejemplo, como se explica en el Dominio 7, los cortafuegos virtuales no son iguales que los cortafuegos físicos, y la mera abstracción de un cortafuegos físico en una máquina virtual puede que no cumpla con los requisitos de despliegue o seguridad.

La seguridad de la virtualización en la computación en la nube también sigue el modelo de responsabilidad compartida. El proveedor de la nube siempre será responsable de proteger tanto la infraestructura física como la propia plataforma de virtualización. Mientras tanto, el cliente de la nube es responsable de implementar correctamente los controles disponibles de seguridad virtualizados y comprender los riesgos subyacentes, en base a lo que implementa y administra el proveedor de la nube. Por ejemplo, decidir cuándo cifrar el almacenamiento virtualizado, configurar correctamente la red virtual y los cortafuegos, o decidir cuándo utilizar hosting dedicado en lugar de compartido.

Dado que muchos de estos controles afectan a otras áreas de seguridad de la nube, como la seguridad de los datos, trataremos de centrarnos en las preocupaciones específicas de la virtualización en este dominio. Sin embargo, las líneas no siempre son claras y la mayoría de los controles de seguridad en la nube están cubiertos más profundamente en los otros dominios de esta Guía. Dominio 7: Seguridad de la Infraestructura, se centra, de manera extensa, en redes virtuales y cargas de trabajo.

8.1.1 Principales categorías de virtualización relevantes para la computación en la nube

8.1.1.1 Capacidad de computación

La virtualización en la computación abstrae la ejecución del código (incluidos los sistemas operativos) del hardware subyacente. En lugar de ejecutarse directamente en el hardware, el código se ejecuta sobre una capa de abstracción que permite un uso más flexible, como ejecutar múltiples sistemas operativos en el mismo hardware (máquinas virtuales). Esto es una simplificación, y recomendamos investigación adicional sobre los gestores e hipervisores de máquinas virtuales si está interesado en profundizar en este tema.

La computación se refiere generalmente a máquinas virtuales, pero esto está cambiando rápidamente, en gran parte debido a la evolución continua de la tecnología y la adopción de contenedores.

Los contenedores y ciertos tipos de infraestructura sin servidor son también ejemplos de abstracciones de computación. Se trata de diferentes abstracciones para crear entornos de ejecución de código, pero no abstraen un sistema operativo completo como hacen el caso de una máquina virtual. (Se profundizará en los contenedores más adelante).

Responsabilidades del proveedor de nube

Las principales responsabilidades de seguridad del proveedor de la nube con relación a la computación virtualizada son forzar el *aislamiento* y mantener una *infraestructura de virtualización segura*.

- El *aislamiento* asegura que los procesos o la memoria en una máquina virtual / contenedor no deberían ser visibles para otra. Esta es la forma en que separamos a los diferentes usuarios (*tenants*), incluso cuando están ejecutando procesos en el mismo hardware físico.
- El proveedor de la nube es también responsable de proteger la *infraestructura subyacente y la tecnología de virtualización* de ataques externos o mal uso interno. Esto significa el uso de hipervisores parcheados y actualizados que están configurados y respaldados adecuadamente con procesos para mantenerlos actualizados y seguros a lo largo del tiempo. La incapacidad de parchear los hipervisores a través de una implementación en la nube, en el caso de descubrirse una nueva vulnerabilidad, podría crear una nube completamente insegura.

Los proveedores de la nube también deberían soportar el uso seguro de la virtualización para los usuarios. Esto significa crear una cadena segura de procesos, a partir de la imagen (u otra fuente) utilizada para ejecutar completamente la máquina virtual, mediante un proceso de arranque seguro e íntegro. Esto garantiza que los usuarios no puedan iniciar máquinas basadas en imágenes a las que no deberían tener acceso, como las pertenecientes a otro usuario, y que una máquina virtual en ejecución (u otro proceso) es la que el cliente espera que se ejecute.

Además, los proveedores de la nube deberían asegurar a los clientes que la memoria volátil no se puede monitorizar sin autorización, ya que podrían mostrarse datos importantes si otro usuario, un empleado malintencionado o incluso un atacante, pudiera acceder a la memoria en ejecución.

Responsabilidades del usuario en la nube

Por otro lado, la responsabilidad principal del usuario de la nube es implementar correctamente la seguridad de lo que sea que despliegue dentro del entorno virtualizado. Dado que la responsabilidad de la seguridad de la virtualización reside en el proveedor, el cliente tiende a aplicar solo unas pocas opciones de seguridad relacionadas directamente con la virtualización de la carga de trabajo. Hay bastante más opciones para asegurar las cargas de trabajo, como se indica en el Dominio 7.

Dicho esto, existen todavía diferencias específicas de virtualización que el usuario de la nube puede utilizar a la hora de implementar su seguridad. En primer lugar, el usuario de la nube debe aprovechar los controles de seguridad para gestionar su infraestructura virtual, que variarán según la plataforma de la nube y que con frecuencia incluyen:

- *Configuraciones de seguridad, como gestión de identidades, sobre los recursos virtuales*. No se trata de la gestión de identidades dentro del recurso, como las credenciales de inicio de sesión del sistema operativo, sino la gestión de identidades de quién puede acceder a la administración en la nube del recurso, por ejemplo, detener o cambiar la configuración de una máquina virtual. Para obtener información específica sobre la seguridad del plano de administración, consulte el dominio 6.
- *Monitoreo y registro*. El dominio 7 cubre la monitorización y el registro de las cargas de trabajo, incluida la forma de manejar los registros de sistema de las máquinas virtuales y los contenedores, pero es probable que la plataforma en la nube ofrezca capacidades adicionales de registro y monitorización a nivel de virtualización. Esto puede incluir aspectos como el estado de una máquina virtual, eventos de gestión, rendimiento, etc.
- *Gestión de activos de imagen*. Las implementaciones en la nube se basan en imágenes maestras, ya sea una máquina virtual, un contenedor u otro código, que luego se ejecutan en la nube. Generalmente se realiza de manera automatizada generando una mayor cantidad de imágenes, en comparación con las imágenes en computación tradicional. Esta gestión es una responsabilidad muy importante desde el punto de vista de la seguridad, incluso los que cumplen con los requisitos de seguridad, dónde pueden implementarse y quién tiene acceso a ellos.
- *El uso de alojamiento dedicado*, si está disponible, basado en el contexto de seguridad del recurso. En algunas situaciones, se puede especificar que los activos se ejecuten en hardware dedicado (a un coste mayor), incluso en una nube multiusuario. Esto puede ayudar a cumplir con los requisitos de cumplimiento, o satisfacer las necesidades de seguridad, en aquellos casos especiales donde e compartir hardware con otro usuario se considera un riesgo.

En segundo lugar, el usuario de la nube también es responsable de los controles de seguridad dentro del recurso virtualizado:

- Incluye la seguridad estándar para las cargas de trabajo, ya sea una máquina virtual, un contenedor o código de aplicación y están bien cubiertos por la seguridad estándar, las mejores prácticas y la orientación adicional descrita en el Dominio 7.

- Es crítico garantizar el despliegue de solamente las configuraciones seguras (por ejemplo, una imagen de máquina virtual actualizada y parcheada). Debido a la gran automatización en la nube, es fácil desplegar configuraciones más antiguas que pueden no estar parcheadas o aseguradas adecuadamente.

Otras preocupaciones en este ámbito incluyen:

- Los recursos virtualizados tienden a ser más efímeros y cambian a un ritmo más rápido. Cualquier control de seguridad, como la monitorización, debe mantener este ritmo. Estos detalles se cubren con más profundidad en el Dominio 7.
- El monitoreo / registro a nivel de host puede no estar disponible, especialmente para implementaciones sin servidor. Es posible que se necesiten implementar métodos de registro alternativos. Por ejemplo, en una implementación sin servidor, es poco probable que se pueda acceder a los registros del sistema de la plataforma subyacente lo que debería compensarse mediante el desarrollo, a nivel de código, de capacidades de registro más robustas en las aplicaciones.

8.1.2 Red

Existen múltiples tipos de redes virtuales, desde redes VLAN básicas, hasta redes completamente definidas por software (*SDN*). Como parte central de la seguridad de la infraestructura en la nube, estos aspectos se cubren tanto en este Dominio 8 como en el anterior.

En la mayoría de las arquitecturas de computación en la nube actuales utilizan *SDN* para virtualizar redes. (Las VLAN normalmente no son adecuadas para las implementaciones en la nube, ya que carecen capacidades de aislamiento suficientes para entornos multi-usuario).

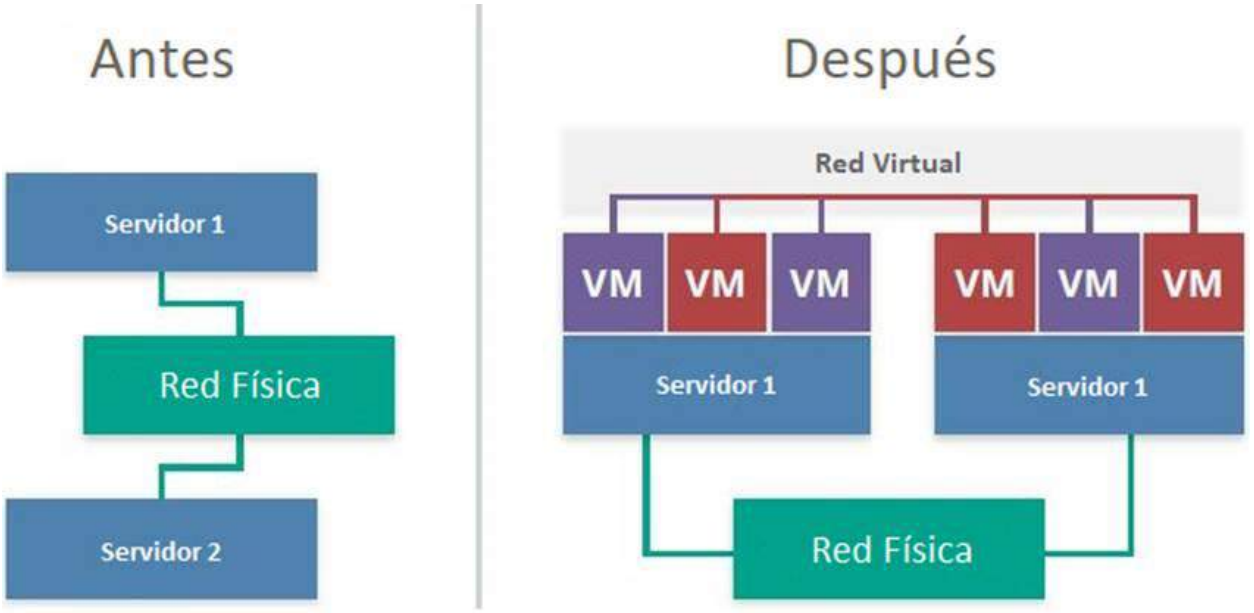
SDN abstrae el plano de administración de red de la infraestructura física subyacente, eliminando muchas restricciones de red típicas. Por ejemplo, se puede superponer varias redes virtuales, incluso las que superponen por completo sus rangos de direcciones, sobre el mismo hardware físico, con todo el tráfico adecuadamente segregado y aislado. Las *SDN* se definen también mediante configuración de software y llamadas a la *API* que soportan la orquestación y agilidad.

Las redes virtuales son bastante diferentes a las redes físicas. Se ejecutan sobre redes físicas, pero la abstracción permite modificaciones profundas en el comportamiento de las redes de maneras que impactan en muchos procesos y tecnologías de seguridad.

8.1.2.1 Monitoreo y Filtrado

El monitoreo y el filtrado (incluidos los cortafuegos), de manera especial, cambian mucho debido a las diferencias en la forma en que los paquetes se mueven alrededor de la red virtual. Los recursos pueden comunicarse en un servidor físico sin que el tráfico cruce la red física. Por ejemplo, si hay dos máquinas virtuales ubicadas en la misma máquina física, no hay ninguna

razón para desviar el tráfico de red desde la máquina a la red. Por lo tanto, pueden comunicarse directamente, y las herramientas de monitoreo y filtrado en línea de la red (o conectadas al hardware de enrutamiento / conmutación) nunca verán el tráfico.



Las redes virtuales mueven paquetes a nivel software y la monitorización no puede depender de la red física

Para compensarlo, se puede enrutar el tráfico a una herramienta de monitoreo o filtrado de red virtual en el mismo hardware (incluida una versión para máquina virtual de un producto de seguridad de red). También puede volver a conectar todo el tráfico a la red o enrutarlo a un dispositivo virtual en la misma red virtual. Cada uno de estos enfoques tiene inconvenientes ya que crean cuellos de botella y un enrutamiento menos eficiente.

Es posible que la plataforma / proveedor en la nube no admita el acceso para la monitorización de red directa. Los proveedores de nube pública raramente permiten el monitoreo completo de la red de paquetes a los clientes, debido a la alta complejidad (y coste). Por lo tanto, no se puede asumir que se tendrá acceso a los datos de paquetes en crudo, a menos que los recopile usted mismo en el host o utilizando un dispositivo virtual.

Con la nube pública en particular, algunas comunicaciones entre servicios en la nube tendrán lugar en la red del proveedor; la monitorización y el filtrado de ese tráfico no es posible para el cliente (y crearía un riesgo de seguridad para el proveedor). Por ejemplo, si se conecta una aplicación sin servidor al almacenamiento de objetos, plataforma de base de datos, cola de mensajes u otro producto *PaaS* del proveedor de la nube, este tráfico se ejecutará de forma nativa en la red del proveedor, no necesariamente dentro de la red virtual gestionada por el cliente. A medida que nos alejamos de la virtualización de infraestructura simple, el concepto de una red gestionada por el cliente comienza a desvanecerse.

Sin embargo, todas las plataformas en la nube modernas ofrecen cortafuegos integrados, que pueden ofrecer ventajas sobre los cortafuegos físicos correspondientes. Se trata de cortafuegos basados en software que pueden operar dentro de la *SDN* o el hipervisor. Por lo general, ofrecen menos funciones que un cortafuegos moderno y dedicado de nueva generación, pero estas capacidades pueden no siempre son necesarias debido a otros aspectos de seguridad inherentes proporcionados por el proveedor de nube.

8.1.2.2 Infraestructura de gestión

Las redes virtuales para computación en la nube siempre soportan la administración remota y, como tal, asegurar el plano de gestión / meta-estructura es fundamental. A veces es posible crear y destruir redes complejas enteras con un puñado de llamadas *API* o unos pocos clics en una consola web.

Responsabilidades del proveedor de nube

El proveedor de la nube es el principal responsable de construir una infraestructura de red segura y configurarla adecuadamente. La máxima prioridad de seguridad es la segregación y el aislamiento del tráfico de red para evitar que los usuarios vean el tráfico de otros. Este es el control de seguridad más fundamental para cualquier red multiusuario.

El proveedor debe deshabilitar el rastreo (*sniffing*) de paquetes u otras "filtraciones" de metadatos que podrían exponer datos o configuraciones entre los usuarios. El rastreo de paquetes, incluso dentro de las propias redes virtuales de un usuario, también debe deshabilitarse para reducir la capacidad de un atacante de comprometer un solo nodo y usarlo para monitorear la red, como es común en redes no virtualizadas. El etiquetado, u otros metadatos a nivel de *SDN*, tampoco deberían exponerse fuera del plano de gestión, o un host comprometido podría utilizarse para profundizar en la propia *SDN*.

Todas las redes virtuales deben habilitar capacidades de cortafuegos integradas para los usuarios de la nube, sin necesidad de cortafuegos o productos externos. El proveedor es también responsable de detectar y prevenir ataques en la red física subyacente y en la plataforma de virtualización. Esto incluye la seguridad perimetral de la propia nube.

Responsabilidades del usuario en la nube

Los usuarios de la nube son los principales responsables de configurar correctamente las implementaciones de la red virtual, especialmente cualquier cortafuegos virtual.

La arquitectura de red puede desempeñar un papel más importante en la seguridad de la red virtual, ya que no estamos limitados por las conexiones físicas y el enrutamiento. Dado que las redes virtuales están basadas en software, el uso de múltiples redes virtuales separadas puede ofrecer amplias ventajas de compartimentación que no son posibles en una red física tradicional. Se puede ejecutar cada pila de aplicaciones en su propia red virtual, lo que reduce

drásticamente la superficie de ataque si un actor malintencionado gana un punto de apoyo. Una arquitectura equivalente en una red física tiene un coste prohibitivo.

Las redes *inmutables* se pueden definir en algunas plataformas en la nube mediante el uso de plantillas de software, lo que puede ayudar a forzar configuraciones correctas por defecto. La completa definición del estado correcto de la red se puede definir en una plantilla, en lugar de tener que configurarlo manualmente. Además de la capacidad de crear múltiples redes con una línea base segura, también se pueden usar para detectar, y en algunos casos revertir, desviaciones de situaciones normales.

El usuario de la nube es, una vez más, responsable de la correcta gestión de los derechos de acceso y la configuración de los controles expuestos en el plano de gestión. Cuando los cortafuegos virtuales y / o el monitoreo no cumplen las necesidades de seguridad, el cliente puede necesitar compensarlo con un dispositivo de seguridad virtual o un agente de seguridad de host. Esto cae dentro de la seguridad de la infraestructura de la nube y está cubierto en profundidad en el Dominio 7.

8.1.2.3 Redes superpuestas en la nube

Las redes superpuestas en nube (*cloud overlay networks*) son un tipo especial de tecnología de virtualización *WAN* para redes que abarcan múltiples redes "base". Por ejemplo, una red de superposición podría abarcar ubicaciones físicas y en la nube, o múltiples redes en la nube, tal vez incluso de diferentes proveedores. No es objetivo de esta Guía profundizar en este tema, si bien aplicarían las mismas recomendaciones de básicas de seguridad.

8.1.3 Almacenamiento

La virtualización del almacenamiento es ya común en la mayoría de las organizaciones: *Storage Area Network* (*SAN*) y *Network-Attached Storage* (*NAS*) son formas comunes de virtualización de almacenamiento, y la seguridad en el almacenamiento se analizará con más detalle en el Dominio 11.

La mayoría del almacenamiento virtualizado es de larga duración y se mantienen múltiples copias de datos en diferentes ubicaciones, por lo que es menos probable que fallos en las unidades ocasionen pérdidas de datos. Cifrar estas unidades reduce la preocupación de que, al cambiar una unidad, actividad bastante frecuente, se pueda exponer ciertos datos.

Sin embargo, este cifrado no protege los datos en ninguna capa virtualizada; solo protege los datos en el almacenamiento físico. Dependiendo del tipo de almacenamiento, el proveedor de la nube también puede (o en su lugar) cifrarlo a nivel de capa de virtualización, pero esto puede no proteger los datos del cliente de la exposición al proveedor de la nube. Por lo tanto, cualquier protección adicional debe aplicarse siguiendo las recomendaciones del Dominio 11.

8.1.4 Contenedores

Los contenedores son entornos de ejecución de código altamente portátiles. Para simplificar, una máquina virtual es un sistema operativo completo, desde el interfaz de usuario hasta, el *kernel*. Un contenedor, en cambio, es un entorno de ejecución virtual que presenta un espacio de usuario aislado, pero utiliza un *kernel* compartido. No es objeto de esta Guía profundizar mucho más allá; puede consultarse más información sobre contenedores de software en esta entrada de Wikipedia[2].

Los contenedores pueden construirse directamente sobre servidores físicos o ejecutarse en máquinas virtuales. Las implementaciones actuales se basan en un *kernel* / sistema operativo existente, que es la razón por la que pueden ejecutarse dentro de una máquina virtual, incluso si el hipervisor no admite la virtualización anidada. (Los contenedores de software dependen de una tecnología completamente diferente que los hipervisores).

Los sistemas de contenedor de software siempre incluyen tres componentes clave:

- El entorno de ejecución (el contenedor).
- Un controlador de orquestación y planificación (que puede ser una colección de múltiples herramientas).
- Un repositorio de las imágenes del contenedor o código para ejecutar.
- Al juntar todos los elementos tenemos tanto el lugar para ejecutar las cosas, las cosas que se deben ejecutar y el sistema de gestión para unirlas.

Independientemente de la plataforma tecnológica, la seguridad del contenedor incluye:

- *Garantizar la seguridad de la infraestructura física subyacente (computación, red, almacenamiento).* Esto no es diferente a cualquier otra forma de virtualización, pero ahora se extiende al sistema operativo subyacente donde se ejecuta el entorno de ejecución del contenedor.
- *Garantizar la seguridad del plano de administración*, que en este caso son el orquestador y el planificador.
- *Asegurar adecuadamente el repositorio de imágenes*. El repositorio de imágenes debe estar en una ubicación segura protegido con controles de acceso adecuados. Esto es tanto para evitar la pérdida o la modificación no autorizada de imágenes de contenedores y archivos de definición, como para evitar filtraciones de datos confidenciales a través del acceso no aprobado a los archivos. Los contenedores se ejecutan tan fácilmente que es también importante controlar que las imágenes solo puedan desplegarse en el contexto de seguridad correcto.
- *La seguridad en las tareas / código que se ejecuta dentro del contenedor*. Sigue siendo posible ejecutar software vulnerable dentro de un contenedor y, en algunos casos, esto podría exponer el sistema operativo compartido o los datos de otros contenedores. Por ejemplo, es posible configurar algunos contenedores para permitir además del acceso a

[2] https://es.wikipedia.org/wiki/Virtualización_a_nivel_de_sistema_operativo

los datos del contenedor en el sistema de archivos, también el acceso al sistema de archivos raíz. También es posible permitir demasiado acceso a la red. Todos estos aspectos son específicos de la plataforma del contenedor en particular y, por lo tanto, requieren configurar de forma segura tanto el entorno del contenedor, como las propias configuraciones de imágenes / contenedores.

Los contenedores evolucionan rápidamente, lo que complica algunos aspectos de la seguridad, pero no significa que sean inherentemente inseguros.

Los contenedores no proporcionan necesariamente un aislamiento completo de seguridad, pero si facilitan la segregación de tareas. Dicho esto, las máquinas virtuales normalmente si proporcionan aislamiento de seguridad. Por lo tanto, se puede colocar tareas de contexto de seguridad equivalente en el mismo conjunto de hosts físicos o virtuales, a fin de proporcionar una mayor segregación de seguridad.

Los sistemas de administración de contenedores y repositorios de imágenes también tienen diferentes capacidades de seguridad, dependiendo que producto se use. La seguridad debe aprender y comprender las capacidades de los productos para poder soportarlos y protegerlos. Los productos deben, como mínimo, soportar controles de acceso basados en roles y autenticación fuerte. También deberían soportar configuraciones seguras, como el aislamiento del sistema de archivos, de proceso y de acceso a red.

Un entendimiento a fondo de la seguridad de los contenedores depende de una comprensión profunda de las partes internas del sistema operativo, como los espacios de nombres (*namespace*), la asignación de puertos de red, la memoria y el acceso al almacenamiento.

Diferentes sistemas operativos host y tecnologías de contenedores ofrecen diferentes capacidades de seguridad. En cualquier proceso de selección de una plataforma de contenedores debería incluirse una evaluación de las capacidades de seguridad.

Un área clave para proteger es qué imágenes/tareas/código se permiten en un entorno de ejecución particular. Eso será posible con un repositorio seguro que cuente con una gestión y planificación adecuada del contenedor.

8.2 Recomendaciones

Los proveedores de la nube deberían:

- Asegurar, de manera inherente, cualquier infraestructura física subyacente utilizada para la virtualización.
- Centrarse en garantizar el aislamiento de seguridad entre los usuarios.
- Proporcionar las capacidades suficientes de seguridad en las capas de virtualización para permitir a los usuarios de la nube proteger sus activos de forma adecuada.
- Proteger firmemente la infraestructura física y las plataformas de virtualización frente a ataques externos o internos.

- Implementar todas las características de virtualización gestionadas por el cliente con una configuración segura por defecto.
- Prioridades específicas:
    - Capacidad de cálculo
        - Utilizar hipervisores seguros e implantar un proceso de gestión de parches para mantenerlos actualizados.
        - Configurar los hipervisores para aislar máquinas virtuales entre sí.
        - Implementar procesos internos y controles de seguridad técnica para evitar el acceso de administradores o no usuarios a máquinas virtuales en ejecución o a la memoria volátil.
    - Red
        - Implementar defensas de seguridad perimetrales esenciales para proteger las redes subyacentes de ataques y, cuando sea posible, para detectar y prevenir ataques contra los consumidores a nivel físico, así como en cualquier capa de red virtual que no puedan proteger directamente.
        - Asegurar el aislamiento entre redes virtuales, incluso si estas redes están todas controladas por el mismo cliente.
            - A menos que el cliente conecte a propósito las redes virtuales separadas.
        - Implementar controles y políticas de seguridad internas para evitar tanto la modificación de las redes de clientes, como la monitorización del tráfico sin aprobación o sin acuerdos contractuales.
    - Almacenamiento
        - Cifrar cualquier almacenamiento físico subyacente, si no ha sido cifrado a otro nivel, para evitar la exposición de datos durante el reemplazo de unidades.
        - Aislar el cifrado de las funciones de administración de datos para evitar el acceso no autorizado a datos de clientes.

Los usuarios de la nube deberían:

- Asegurarse de que entienden las capacidades ofrecidas por los proveedores de la nube, así como también cualquier brecha de seguridad.
- Configurar adecuadamente los servicios de virtualización de acuerdo con las guías del proveedor de la nube y otras mejores prácticas de la industria.
    - La mayor parte de los aspectos fundamental de la seguridad de virtualización recaen en el proveedor de la nube, por lo que la mayoría de las recomendaciones de seguridad para los usuarios de la nube están cubiertas en los otros dominios de esta Guía.
- Para contenedores:

- Comprender las capacidades de aislamiento de seguridad tanto de la plataforma de contenedor elegida, como del sistema operativo subyacente, para poder elegir la configuración adecuada.
- Utilizar máquinas físicas o virtuales para proporcionar aislamiento de contenedores y grupos de contenedores con los mismos contextos de seguridad en los mismos hosts físicos y/o virtuales.
- Asegurarse de que solo se pueda desplegar imágenes de contenedores o códigos previamente aprobados, conocidos y seguros.
- Proteger adecuadamente la(s) pila(s) de software de orquestación / gestión y planificación de contenedores.
- Implementar controles de acceso basados en roles apropiados y mecanismos de autenticación fuerte para toda la gestión de contenedores y repositorios.

Dominio 9 Respuesta ante Incidentes

9.0 Introducción

La respuesta ante incidentes (RI) es un aspecto fundamental en todo programa de seguridad de la información. Los controles de seguridad preventivos han demostrado ser incapaces de eliminar, por completo, la posibilidad de comprometer la información crítica. La mayoría de las organizaciones disponen de algún tipo de plan de RI para determinar cómo se investigará un ataque, pero como la nube presenta diversas diferencias, tanto en el acceso, como en la gestión de la información forense, las organizaciones deben considerar cómo adaptar sus procesos de RI.

Este dominio busca identificar las diferencias relevantes, con relación a la RI, debidas a las características específicas de la computación en la nube. Los profesionales de la seguridad pueden utilizar este documento como referencia a la hora de desarrollar planes de respuesta, así como a la hora de llevar a cabo otras actividades durante la fase de preparación del ciclo de vida de RI. Este dominio está organizado de acuerdo con el ciclo de vida de respuesta ante incidentes tal y como está descrito en la Guía, comúnmente aceptada, de Gestión de incidentes (*NIST* 800-61rev2 08/2012) [1] del *NIST* (*National Institute of Standards and Technology*). Otros marcos de estándares internacionales de respuesta ante incidentes incluyen la *ISO/IEC* 27035 y las estrategias de ENISA para la respuesta ante incidentes y la cooperación ante ciber-crisis.

Después de describir el ciclo de vida de la respuesta ante incidentes tal y como se expone en la guía *NIST* 800-61rev2, cada sección aborda una fase del ciclo de vida, explorando las posibles consideraciones a tener en cuenta por el equipo de respuesta cuando trabajan en un entorno en la nube.

9.1 Visión general

9.1.1 Ciclo de vida de la respuesta ante incidentes

El ciclo de vida de la respuesta ante incidentes viene descrito en la guía *NIST* 800-61rev2, e incluye las siguientes fases y actividades principales:

Ciclo de vida de respuesta ante incidentes

- Preparación: “Establecer una capacidad de respuesta ante incidentes de modo que la organización sea capaz de responder ante incidentes”.
    - Procesos para gestionar incidentes.
    - Instalaciones y comunicaciones para los gestores de incidentes.
    - Software y hardware para el análisis de incidentes.
    - Documentación interna (listados de puertos y activos, diagramas de red, datos de referencia actuales del tráfico de red).
    - Identificación de las necesidades formativas.
    - Evaluación de la infraestructura mediante escaneos proactivos, monitorización de red, evaluaciones de seguridad y análisis de riesgos.
    - Subscripciones a servicios externos de inteligencia de amenazas.

- Detección y análisis:
    - Alertas [protección del puesto de trabajo, monitorización de la seguridad de la red, monitorización de servidores, creación de cuentas, escalada de privilegios, *SIEM*, analítica de seguridad (detección basada en puntos de referencia y anomalías), analítica del comportamiento del usuario y otros indicadores de compromiso].
    - Validar alertas (reduciendo los falsos positivos) y escalado.
    - Estimar el alcance del incidente.
    - Designar un Gestor del Incidente que coordine las acciones a seguir.
    - Designar una persona encargada de comunicar el estatus de la contención y recuperación a la alta dirección.
    - Crear una línea temporal del ataque.
    - Determinar el alcance potencial de la pérdida de datos.
    - Actividades de coordinación y notificación.
    - Contención, erradicación y recuperación:
        - Contención: Desconectar equipos. Considerar pérdidas de datos frente a la disponibilidad del servicio. Asegurar que los sistemas no se autodestruyan tras haber sido detectados.
        - Erradicación y recuperación: Limpiar dispositivos comprometidos y restaurar los sistemas a la normalidad. Confirmar que los sistemas funcionan adecuadamente. Desplegar controles que prevengan incidentes similares.
    - Documentar el incidente y recoger evidencias (cadena de custodia).

- Actividades post-incidente:
    - ¿Qué podría haberse hecho mejor? ¿Podría haberse detectado antes el ataque? ¿Qué información adicional habría sido útil para aislar al ataque más rápidamente? ¿Son necesarios cambios en el proceso de RI? De ser así, ¿cuáles?

9.1.2 Cómo afecta la nube a la RI

Cada una de las fases del ciclo de vida se ve afectada, en distinto grado, en un despliegue en la nube. Algunas de las fases son similares a la respuesta ante incidentes en un entorno externalizado, en el que es necesaria la coordinación con un tercero. Otras diferencias son más específicas de la naturaleza abstracta y automatizada de la nube.

9.1.2.1 Preparación

Estas son las consideraciones más importantes a la hora de prepararse para la respuesta ante incidentes en la nube.

- *SLA y gobierno*: Todo incidente que involucre a un proveedor de alojamiento o una nube pública requiere de la comprensión de los acuerdos de nivel de servicio (*SLA*, *Service Level Agreements*), y probablemente de la coordinación con el proveedor de la nube. Hay que tener en cuenta que, dependiendo de la relación con el proveedor, es posible no disponer de puntos de contacto directos, estando limitados a lo que pueda estar disponible a través del soporte estándar. Una nube privada personalizada en un centro de datos de terceros tendrá una relación muy distinta de una aplicación *SaaS* que requiere el registro en un sitio web y la aceptación de un acuerdo de licencia.

Las cuestiones clave incluyen: ¿Qué hace tu organización? ¿De qué es responsable el proveedor de servicios en la nube (*CSP*, *Cloud Service Provider*)? ¿Quiénes son los puntos de contacto? ¿Cuáles son las expectativas de tiempos de respuesta? ¿Cuáles son los procedimientos de escalado? ¿Existen procedimientos de comunicación fuera de banda (en caso de que la red se vea afectada)? ¿Cómo funcionan los traspasos? ¿A qué datos es posible tener acceso?

Es necesario probar los procedimientos con el *CSP* cuando sea posible, así como validar que los roles, responsabilidades y escalados de incidentes son claros. Garantizar que el *CSP* tiene los contactos necesarios para la notificación de los incidentes que detecten, estando dichas notificaciones integradas en los procesos de la organización. En los servicios de registro online, las notificaciones serán a menudo enviadas a la dirección de correo empleada en el registro; dichas direcciones deben ser controladas por la organización y monitorizadas de forma

continua. Se debe asegurar que existen contactos en la organización con el *CSP*, incluyendo medios fuera de banda, y que han sido probados.

- *IaaS/PaaS vs SaaS:* ¿Cómo se proveen los datos específicos de la nube de tu organización en un entorno multiusuario? Para cada servicio principal se debería entender y documentar qué datos y registros estarán disponibles en caso de un incidente. No se debe asumir que se puede contactar con un proveedor después de un incidente y recoger datos que normalmente no están disponibles.
- *"Juego de herramientas para saltar a la nube":* Conjunto de herramientas necesarias para realizar una investigación de forma remota (como suele suceder con recursos basados en la nube). Por ejemplo: ¿se tienen herramientas para recoger registros y metadatos de la plataforma en la nube? ¿Se tienen los conocimientos necesarios para interpretar la información? ¿Cómo se obtienen imágenes de máquinas virtuales en ejecución y a qué tipo de datos se tiene acceso: almacenamiento en disco o memoria volátil?
- *Diseñar el entorno en la nube para una rápida detección, investigación y respuesta (contención y recuperación).* Esto significar asegurar que se tiene una arquitectura y configuración adecuadas para facilitar la respuesta ante incidentes:
    - Habilitar la instrumentación de la información, como los logs de *API* en la nube, y garantizar que son enviados a una localización segura para que los investigadores los tengan disponibles en caso de un incidente.
    - Utilizar el aislamiento para asegurar que los ataques no pueden propagarse y comprometer el entorno por completo.
    - Hacer uso de servidores inmutables cuando sea posible. Si se detecta un problema, mover la carga de trabajo del dispositivo comprometido a una nueva instancia en buen estado. Concentrarse en la gestión de la configuración y en la monitorización de la integridad de los ficheros.
    - Implementar mapas de la pila de aplicación para comprender dónde van a residir los datos, para de esta forma tener en cuenta diferencias geográficas que afecten a la captura de datos y monitorización.
    - La realización de modelado de amenazas y ejercicios sobre el papel puede ser muy útiles a la hora de determinar las estrategias más efectivas de contención de distintos tipos de ataques a diversos componentes de la pila del servicio en la nube.
    - Se deben incluir, en cada caso, las diferencias a la respuesta en *IaaS*, *PaaS* y *SaaS*.

9.1.2.2 Detección y análisis

La detección y el análisis en un entorno en la nube pueden parecer prácticamente la misma (para entornos *IaaS*) o ser muy diferente (en entornos *SaaS*). En cualquier caso, el alcance de la monitorización debe cubrir toda la gestión del servicio en la nube (plano de gestión), no solo los activos desplegados.

De cara a acelerar el proceso de respuesta, es posible aprovechar la monitorización propia de la nube y las alertas capaces de iniciar un flujo automatizado de RI. Algunos proveedores de nube ofrecen estas características dentro de sus plataformas, y también existen disponibles

soluciones de monitorización de terceros. Estas soluciones no tienen por qué ser específicas de seguridad: muchas plataformas en la nube (*IaaS* y posiblemente *PaaS*) ofrecen una variedad de métricas de monitorización en tiempo real o cuasi real por motivos operativos y de rendimiento. Estas métricas pueden ser utilizas desde el punto de vista de seguridad.

Las plataformas en la nube ofrecen también una variedad de registros que pueden ser, en algunos casos, integrados en las operaciones de seguridad y monitorización. Se pueden tener desde registros operacionales, hasta un registro completo de todas las llamadas a *API*, o la actividad de gestión del servicio. Hay que tener en cuenta que no están disponibles en todos los proveedores; es más habitual tenerlos en entornos *IaaS* y *PaaS* que SaaS. Cuando no existen mecanismos de envío de registros, es posible utilizar la consola de la nube para identificar cambios en la configuración o en el entorno.

Las *fuentes de datos* en incidentes en la nube pueden ser bastante distintas de aquellas empleadas en la respuesta ante incidentes tradicional. Aunque hay un solape significativo (como en los registros de sistema), hay diferencias en las formas en las que recopila la información en lo relativo a las nuevas fuentes, como los mecanismos de alimentación de los entornos de gestión en la nube.

Como se ha mencionado, los registros de la plataforma en la nube pueden ser una opción, pero no están disponibles de forma universal. Idealmente, estos registros deberían mostrar toda la actividad del entorno de gestión. Es importante comprender qué información se guarda, así como los vacíos que pudieran afectar al análisis de un incidente ¿Se registran todas las actividades de gestión? ¿Se incluyen todas las actividades automatizadas del sistema (como el auto-escalado) o las actividades de gestión del proveedor de la nube? En el caso de un incidente grave, los proveedores pueden tener acceso a otros registros que habitualmente no están disponibles para los clientes.

Un reto a la hora de la recolección de información puede ser la visibilidad limitada de la red. Los registros de red de un proveedor tienden a ser registros de flujos, no una captura completa de paquetes.

Donde existan vacíos siempre es posible instrumentar la pila de tecnología con mecanismos propios de registro. Esto puede aplicarse a instancias, contenedores y código de aplicación para permitir obtener telemetría vital en una posible investigación. Hay que prestar atención especial a las arquitecturas de aplicación sin servidores y al *PaaS*; es probable que sea necesario añadir registros personalizados a nivel de aplicación.

La inteligencia de amenazas externa puede ser también útil, como en la computación tradicional, a la hora de identificar indicadores de compromiso y conseguir información sobre los adversarios.

Hay que ser consciente de los retos potenciales existentes cuando la información que un *CSP* provee se enfrenta a cuestiones relativas a la cadena de custodia. Hoy en día, no hay precedentes fiables establecidos al respecto.

El soporte para las investigaciones y análisis forenses debe también adaptarse y entendiendo los cambios producidos a las fuentes de datos.

Hay que fijarse siempre en lo que el *CSP* puede proveer y si cumplen los requisitos de cadena de custodia. No todos los incidentes provocan una acción legal, pero es importante trabajar con el equipo legal para entender los límites y dónde se puede terminar teniendo problemas con la cadena de custodia.

Hay una mayor necesidad de automatizar muchos de los procesos forenses y de investigación en la nube, debido a su naturaleza dinámica y de alta velocidad. Por ejemplo, es posible perder evidencias debido a una actividad normal de auto-escalado, o si un administrador decide apagar una máquina virtual involucrada en una investigación. Algunos de los ejemplos de tareas que pueden ser automatizadas incluyen:

- Realizar una instantánea (*snapshot*) del almacenamiento de la máquina virtual.
- Capturar los metadatos en el momento de la alerta, para que el análisis pueda basarse en cómo estaba la infraestructura en dicho momento.
- Si el proveedor lo soporta, “pausar” la máquina virtual, lo que guardará el estado de la memoria del sistema.

Siempre se puede aprovechar las capacidades de una plataforma en la nube para determinar el alcance potencial de un compromiso:

- Analizar flujos de red para comprobar si el aislamiento de red fue eficaz. Es posible usar llamadas *API* para realizar una instantánea del estado de la red y de las reglas del cortafuegos virtual, lo que puede aportar una imagen exacta de toda la pila en el momento del incidente.
- Examinar datos de la configuración para comprobar si otras instancias similares fueron comprometidas en el mismo ataque.
- Revisar registros de acceso a datos (para el almacenamiento basado en la nube, si están disponibles) y del panel de gestión para ver si el incidente ha afectado o alcanzado a la plataforma en la nube.
- Las arquitecturas *PaaS* y sin servidor requerirán una correlación adicional entre la plataforma en la nube y cualquier registro de aplicación autogenerado.

9.1.2.3 Contención, erradicación y recuperación

Siempre hay que empezar garantizando que el panel de control de la nube y su meta-estructura están libres de ataques. Esto incluirá con frecuencia la invocación de procedimientos de urgencia, para tener acceso a las credenciales maestras de la cuenta en la nube, para confirmar de esta manera, que la actividad del atacante no está siendo ocultada o enmascarada a la vista de cuentas de menor privilegio que la del administrador. Hay que recordar que no es posible contener un ataque si los atacantes mantienen acceso al panel de gestión. Los ataques a activos en la nube, como las máquinas virtuales, pueden en ocasiones revelar credenciales del panel de gestión que luego son usadas como un puente a un ataque más amplio y serio.

La nube ofrece, a menudo, mucha más flexibilidad en esta fase de la respuesta, especialmente en *IaaS*. La infraestructura definida por software permite una rápida reconstrucción desde cero en un entorno limpio, y para ataques más aislados, las características inherentes de la nube – grupos de auto-escalado, llamadas a *APIs* para cambiar la configuración de redes o máquinas virtuales y las instantáneas – pueden acelerar los procesos de cuarentena, erradicación y recuperación. Por ejemplo, en muchas plataformas es posible poner en cuarentena, de forma instantánea, una máquina virtual moviéndola fuera del grupo de auto-escalado, aislándola con un cortafuegos virtual y reemplazándola.

Esto implica, a su vez, que no hay una necesidad inmediata de “erradicar” al atacante antes de identificar sus mecanismos de explotación y el alcance de la brecha, ya que como la nueva infraestructura o instancia están limpias, es posible, en su lugar, simplemente aislarlo. De todas formas, sigue siendo necesario asegurar que el camino de explotación utilizado está cerrado y no puede ser usado para infiltrarse, de nuevo, en otros activos en producción. Si existe alguna duda de que el panel de administración ha sido comprometido, hay que estar seguro de que las plantillas o configuraciones para las nuevas infraestructuras o aplicaciones no han sido comprometidas a su vez.

Dicho esto, estas capacidades no son siempre universales: con *SaaS* y algunos *PaaS* se puede estar muy limitado y por ello depender, en mayor medida, del proveedor de la nube.

9.1.2.4 Actividades post-incidente

Como con cualquier ataque, hay que trabajar con el equipo de respuesta interno y el proveedor para analizar qué funcionó bien y qué no funcionó para identificar los puntos de mejora. Se debe prestar especial atención a las limitaciones de los datos recogidos y averiguar cómo resolver los problemas encontrados.

Es complicado cambiar los *SLAs*, pero si los tiempos de respuesta, datos o cualquier otro apoyo acordado fueron insuficientes, hay que intentar renegociarlos.

9.1 Recomendaciones

- Los aspectos más importantes de la respuesta ante incidentes en entornos en la nube son los *SLA* y el establecimiento de las expectativas sobre qué tiene que hacer el cliente vs. qué tiene que hacer el proveedor. Una comunicación clara de roles y responsabilidades y la práctica tanto de la respuesta, como de los trasvases de información son críticas.
- Los clientes deben establecer canales de comunicación claros con el proveedor que puedan ser empleados en el caso de un incidente. Los estándares abiertos existentes pueden facilitar la comunicación del incidente.
- Los clientes deben comprender el contenido y formato de los datos que el proveedor de la nube puede proporcionar para su análisis, y evaluar si los datos forenses satisfacen los requisitos legales de la cadena de custodia.
- Los clientes en la nube deberían adoptar esquemas de monitorización continua y de recursos en la nube para detectar los problemas de forma más temprana que en centros de datos tradicionales.
    - Las fuentes de datos deberían de ser almacenadas o copiadas en localizaciones que mantengan la disponibilidad durante incidentes.
    - Si fuera posible y necesario, deberían de ser manejadas de forma que se mantenga una cadena de custodia apropiada.
- Las aplicaciones basadas en la nube deberían aprovecharse de la automatización y la orquestación para optimizar y acelerar la respuesta, incluyendo la contención y la recuperación.
- Para cada proveedor de servicios utilizado, la aproximación para detectar y gestionar incidentes que afecten a los recursos alojados en dicho proveedor, debe ser planificada y descrita en el plan de respuesta ante incidentes corporativo.
- Los *SLAs* de cada proveedor de servicios en la nube deben garantizar el soporte a las tareas de gestión de incidentes requeridas para una ejecución efectiva del plan de respuesta ante incidentes corporativo. Se debe cubrir cada etapa del proceso de gestión del incidente: detección, análisis, contención, erradicación y recuperación.
- Las pruebas deben llevarse a cabo anualmente, o cada vez que se produzcan cambios significativos en la arquitectura de la aplicación. Los clientes deberán integrar sus procedimientos de prueba con los de sus proveedores (y otros asociados) en la mayor medida posible.

Dominio 10 Seguridad de Aplicaciones

10.0 Introducción

La seguridad de las aplicaciones abarca un conjunto de conocimientos increíblemente amplio y complejo: todo, desde el diseño inicial y la detección de amenazas, hasta el mantenimiento y la protección de las aplicaciones en producción. La seguridad de las aplicaciones también está evolucionando a un ritmo increíblemente rápido a medida que la práctica del desarrollo de aplicaciones continúa avanzando y abarca nuevos procesos, patrones y tecnologías. La computación en la nube es uno de los mayores impulsores de estos avances y esto se traduce en una presión correspondiente para evolucionar el estado de la seguridad de las aplicaciones, a fin de garantizar que este progreso continúe de la manera más segura posible.

Esta sección de la guía está destinada a equipos de desarrollo de software y TI que quieran construir y desarrollar aplicaciones de forma segura en entornos de computación en la nube, específicamente *PaaS* e *IaaS*. (Muchas de las técnicas en esta sección son usadas para respaldar aplicaciones de *SaaS* seguras). Nos centraremos en:

- Cómo difiere la seguridad de la aplicación en la nube
- Revisar los aspectos básicos de desarrollo de software seguro y cómo estos cambian en la nube.
- Aprovechar las capacidades de la nube para desarrollar aplicaciones en la nube más seguras.

No podemos cubrir todas las opciones posibles de desarrollo e implementación, incluso aquellas directamente relacionadas con la computación en la nube, por lo que el objetivo es centrarse en áreas relevantes que deberían ayudar a guiar la seguridad en la mayoría de las situaciones. Este dominio también presenta los fundamentos de seguridad para *DevOps*, que está emergiendo rápidamente como una fuerza dominante en el desarrollo de aplicaciones basadas en la nube.

La computación en la nube, generalmente, aporta beneficios de seguridad a las aplicaciones, pero al igual que con la mayoría de las áreas de tecnología en la nube, se requiere cambios acordes a las prácticas, procesos y tecnologías existentes que no fueron diseñados para operar en la nube. A alto nivel, este equilibrio de oportunidades y desafíos incluye:

Oportunidades

- *Línea base de seguridad mayor*. Los proveedores de la nube, especialmente los principales proveedores de *IaaS* y *PaaS*, tienen incentivos económicos significativos para mantener una línea base de seguridad más alta que la mayoría de las organizaciones. En un entorno de nube, los fallos graves de líneas base de seguridad, rompen por completo la confianza que un proveedor de nube pública necesita para mantener las relaciones con sus clientes. Los proveedores de la nube también están

sujetos a un amplio rango de requerimientos de seguridad con el fin de cumplir con todas las regulaciones y requerimientos sectoriales de sus clientes. Esto motiva fuertemente a los proveedores de la nube a mantener niveles extremadamente altos de seguridad.

- *Capacidad de reacción*. Las *APIs* y la automatización proporcionan una amplia flexibilidad para crear programas de seguridad con mayor capacidad de reacción a un coste menor que en la infraestructura tradicional. Por ejemplo, cambiar las reglas del cortafuegos, o implementar nuevos servidores con código actualizado, se puede realizar con unas pocas llamadas a *APIs* o mediante la automatización.

- *Entornos aislados*. Las aplicaciones en la nube también pueden aprovechar redes virtuales y otras estructuras, incluido *PaaS*, para entornos hiper-segregados. Por ejemplo, es posible implementar, sin coste adicional, múltiples pilas de aplicaciones en redes virtuales completamente separadas, eliminando la posibilidad de que un atacante use una aplicación comprometida para atacar a otras detrás de los cortafuegos perimetrales.

- *Máquinas virtuales independientes*. El uso de arquitecturas de microservicios permite mejorar aún más la seguridad. Dado que la nube no requiere que el consumidor optimice el uso de servidores físicos, un requisito que a menudo resulta en la implementación de múltiples componentes de aplicaciones y servicios en un solo sistema (tradicional), los desarrolladores pueden implementar más máquinas virtuales y más pequeñas, cada una dedicada a una función o servicio. Esto reduce el rango de ataque de las máquinas virtuales individuales y soporta controles de seguridad más granulares.

- *Elasticidad*. La elasticidad permite un uso mayor de la infraestructura inmutable. Cuando se utilizan herramientas de elasticidad como los grupos de auto-escalado, cada sistema en producción se inicia dinámicamente en función de una imagen base, y puede ser "desaprovisionado" automáticamente sin interacción humana. Por lo tanto, los requisitos operativos básicos implican que nunca se permita a un administrador iniciar sesión en un sistema y realizar cambios, ya que se perderán durante una actividad normal de auto-escalado. Esto permite el uso de servidores inmutables, donde la administración remota está completamente deshabilitada. Los servidores e infraestructura inmutables se describen con más detalle en el Dominio 7.

- *DevOps*. *DevOps* es una nueva metodología y filosofía de desarrollo de aplicaciones centrada en la automatización del desarrollo y la implantación de aplicaciones. *DevOps* abre muchas oportunidades en seguridad para mejorar el fortalecimiento de código (*hardening*), la administración de cambios, la seguridad de las aplicaciones de producción, e incluso para mejorar las operaciones de seguridad en general.

- *Interfaz unificada*. Un interfaz unificado (interfaz de administración y *APIs*) para infraestructura y servicios de aplicaciones (cuando se usa *PaaS*) proporciona una vista más completa y una mejor administración en comparación con los sistemas y dispares dispositivos tradicionales (balanceadores de carga, servidores, dispositivos de red, cortafuegos, ACL, etc.), que a menudo son administrados por diferentes grupos. Esto permite reducir los fallos de seguridad debido a la falta de comunicación o visibilidad completa.

Desafíos

- *Visibilidad detallada limitada*. La visibilidad y la disponibilidad de monitoreo se ven afectadas, lo que requiere nuevos enfoques para recopilar datos relacionados con la seguridad. Esto ocurre especialmente cuando se usa *PaaS*, donde los registros disponibles normalmente, como los registros del sistema o de red, a menudo ya no son accesibles para el usuario de la nube.

- *Mayor número de componentes de la aplicación*. La seguridad del plano de gestión /meta-estructura afecta directamente a la seguridad de cualquier aplicación asociada con esa cuenta en la nube. Los desarrolladores y los operadores probablemente necesiten también acceder al plano de administración, en lugar de pasar siempre por un equipo diferente. Los datos y la información sensible también son potencialmente visibles desde el plano de gestión. Por último, las aplicaciones modernas en la nube a menudo se conectan con el plano de gestión para activar una serie de acciones automáticas, especialmente cuando se trata de *PaaS*. Por todos estos motivos, la seguridad del plano de gestión se considera dentro del alcance de la seguridad de la aplicación ya que un fallo en cualquiera de los lados podría impactar a la otra.

- *Cambio del modelo de amenazas*. La relación con el proveedor de la nube y el modelo de seguridad compartido deberán incluirse en el modelo de amenazas, así como en cualquier plan de respuesta operacional y de incidentes. Los modelos de amenazas también deben adaptarse para reflejar las diferencias técnicas del proveedor o plataforma utilizados en la nube.

- *Transparencia reducida*. Puede haber menos transparencia en cuanto a lo que está sucediendo dentro de la aplicación, especialmente cuando se integra con servicios externos. Por ejemplo, rara vez se conoce el conjunto completo de controles de seguridad para un servicio *PaaS* externo integrado con su aplicación.

En general, habrá cambios en la seguridad de las aplicaciones debido al modelo compartido de seguridad. Algunos de estos están directamente relacionados con el gobierno y la operación, pero hay muchos más en términos de cómo piensas y planificas la seguridad de la aplicación.

10.1 Visión general

Debido a la amplia naturaleza de la seguridad de las aplicaciones y los diferentes conjuntos de habilidades y roles involucrados en un programa efectivo de seguridad de aplicaciones, este dominio se divide en las siguientes áreas principales:

- *El ciclo de vida de desarrollo de software seguro* (SSDLC): cómo la computación en la nube afecta a la seguridad de las aplicaciones, desde el diseño hasta la implementación.

- *Diseño y arquitectura*: Tendencias en el diseño de aplicaciones para computación en la nube que afectan e incluso pueden mejorar la seguridad.

- *DevOps e integración continua / implementación continua (CI/CD): DevOps* y CI/CD se utilizan con mucha frecuencia tanto en el desarrollo como en la implementación de aplicaciones en la nube, y se están convirtiendo rápidamente en los modelos dominantes. Implican nuevas consideraciones de seguridad y, una vez más, oportunidades para mejorar la seguridad frente a desarrollos y patrones de despliegue más manuales, como el modelo en cascada.

10.1.1 Introducción al ciclo de vida de desarrollo de software seguro y computación en la nube

El SSDLC describe una serie de actividades de seguridad durante todas las fases de desarrollo, despliegue y operaciones de aplicaciones. Hay múltiples marcos de trabajo utilizados en la industria, incluyendo:

- Ciclo de vida de desarrollo seguro de Microsoft
- *NIST* 800-64
- ISO/IEC 27034
- Otras organizaciones, incluido Proyecto de Seguridad de Aplicaciones Web Abiertas (*OWASP*, *Open Web Application Security Project*) y una variedad de proveedores de seguridad de aplicaciones, también publican sus propias guías de ciclo de vida y aspectos de seguridad.

Debido a la variedad de marcos de trabajo y las diferencias en la terminología, Cloud Security Alliance los divide en grandes "metafases" para ayudar a describir el conjunto, relativamente estándar, de actividades que se observan en estos marcos. Estas “metafases” no pretenden reemplazar las metodologías formales, sino que simplemente proporcionan un modelo descriptivo que podemos utilizar para abordar las principales actividades, independiente del ciclo de vida que la organización utilice.

- *Diseño y desarrollo seguro*: desde la formación y estándares corporativos de desarrollo hasta la programación y pruebas del código.
- *Despliegue seguro*: las actividades y pruebas de seguridad al pasar el código de un entorno de desarrollo aislado a la producción.
- *Operaciones seguras*: asegurar y mantener las aplicaciones de producción, incluidas las defensas externas, como los cortafuegos de aplicaciones web (*WAF*), y las continuas evaluaciones de vulnerabilidades.

La computación en la nube afecta todas las fases del SSDLC, independientemente del método SSDLC particular que se utilice. Este es resultado directo de la abstracción y la

automatización de la computación en la nube, combinada con (en la nube pública) una mayor dependencia de un proveedor externo. Específicamente:

- El modelo de responsabilidad compartida significa que siempre hay una cierta dependencia del proveedor de la nube para algunos aspectos de la seguridad, incluso en una aplicación basada en *IaaS*. Cuanto más se adopte PaaS y las características específicas del proveedor, mayor será la división en responsabilidades de seguridad. Podría ser tan simple como usar un balanceador de carga en la nube, que el proveedor es completamente responsable de mantener seguro, pero el usuario de la nube es responsable de configurarlo y usarlo correctamente.
- Hay grandes cambios en la visibilidad y el control, como se explica en casi todos los ámbitos de esta Guía. En el caso de *IaaS*, podría tratarse de una falta de registros de red, pero a medida que nos movemos hacia *PaaS* podemos ir perdiendo registros de servidor y servicio. Y, todo variará según el proveedor y la tecnología.
- Los proveedores de la nube tienen capacidades diferentes en términos de características, servicios y seguridad, que deben tenerse en cuenta en el plan general de seguridad de aplicaciones.
- El plano de gestión y la meta-estructura pueden estar dentro del alcance de seguridad de la aplicación, especialmente cuando los componentes de la aplicación se comunican directamente con el servicio en la nube.
- Hay nuevas y diferentes opciones de arquitecturas, especialmente, a medida que profundizamos en *PaaS*.
- El aumento e impacto de *DevOps*, que cubriremos más adelante en este Dominio.

10.1.2 Desarrollo y diseño seguro

Hay cinco fases principales en el desarrollo y diseño seguro de aplicaciones, todas ellas impactadas por la computación en la nube:

Fases de desarrollo y diseño seguro de aplicaciones.

Cambiar “modelamiento” por “modelado”

Formación: Hay tres roles diferentes que requerirán de dos nuevas categorías de formación. Desarrollo, operaciones y seguridad deberían todos recibir formación adicional sobre los fundamentos de la seguridad en la nube (que no son específicos del proveedor), así como formación apropiada de seguridad de cualquier proveedor específico y plataformas de nube utilizadas en los proyectos. Normalmente hay una mayor participación de desarrollo y operaciones en la arquitectura y administración directas de la infraestructura en la nube, por lo que es esencial la capacitación de seguridad básica específica de las herramientas que utilizarán.

Definición: El usuario de la nube determina las arquitecturas o características/herramientas aprobadas para el proveedor, los estándares de seguridad y otros requisitos. Esto podría estar estrechamente relacionado con los requisitos de cumplimiento, como, por ejemplo, qué tipo de datos se permiten en qué servicios en la nube (incluidos los servicios individuales dentro de un proveedor más grande). Los procesos de despliegue también deben definirse en este paso, aunque a veces se finalizan más adelante. Los estándares de seguridad deben incluir los derechos iniciales de acceso para determinar quién puede administrar qué servicios en el proveedor de la nube, que suele ser independiente de la arquitectura de la aplicación. También debe incluir herramientas, tecnologías, configuraciones e incluso patrones de diseño previamente aprobados.

Diseño: Durante el proceso de diseño de aplicaciones, especialmente cuando se trata de *PaaS*, las prioridades de seguridad en la nube están en la arquitectura, las capacidades estándar y características del proveedor de la nube, la automatización y administración de seguridad para el despliegue y las operaciones. A menudo nos encontramos que hay importantes ventajas de seguridad al integrar la seguridad en la arquitectura de aplicaciones, ya que se puede aprovechar las capacidades de seguridad propias del proveedor. Por ejemplo, insertar un balanceador de carga sin servidor o cola de mensajes, podría bloquear por completo ciertas rutas de ataque por red. Aquí también es donde realiza el modelado de amenazas, que también debe específico del proveedor/plataforma y la nube.

Desarrollo: los desarrolladores pueden necesitar un entorno de desarrollo con acceso de administración al plano de gestión de la nube, para poder configurar redes, servicios y otros aspectos. Esto nunca debe realizarse en entornos de producción ni contener datos de producción. Es probable que los desarrolladores también utilicen un canal CI/CD, que debe ser protegido, especialmente el repositorio de código. Si se usa *PaaS*, los desarrolladores deben construir el registro en las aplicaciones para compensar, en la medida de lo posible, cualquier pérdida de red, sistema o registros de servicio.

Prueba: las pruebas de seguridad deben integrarse en el proceso y canal de despliegue. Las pruebas suelen abarcar, además, la fase de despliegue seguro, pero se inclinan hacia pruebas unitarias de seguridad, pruebas funcionales de seguridad, pruebas estáticas de seguridad de aplicaciones (*SAST*) y pruebas dinámicas de seguridad de aplicaciones (*DAST*). Debido a este solapamiento, cubrimos las consideraciones de la nube con más profundidad en la siguiente sección. Las organizaciones también deberían confiar más en las pruebas automatizadas en la nube. La infraestructura está incluida más a menudo en el alcance de las pruebas de

aplicaciones, debido a que al definirse como "infraestructura como código", la infraestructura se ha definido e implementado a través de plantillas automatizadas. Como parte de estas pruebas, considere la necesidad de marcado para aquellas capacidades sensibles a la seguridad que puedan requerir una revisión más profunda, como la autenticación y el cifrado de código.

10.1.3 Despliegue seguro

Dado que el despliegue automático tiende a ser mayor en entornos de nube, incluye a menudo ciertas actividades de seguridad que también podrían implementarse en las fases de Diseño y Desarrollo. Las pruebas de seguridad automatizadas se integran, frecuentemente, en el flujo de despliegue y se realizan fuera del control directo de los desarrolladores. Esto es, en sí mismo, una desviación de muchos de los esfuerzos de desarrollo tradicionales, pero las pruebas también necesitan adaptarse a la nube.

Existen múltiples tipos de pruebas de seguridad de aplicaciones que podrían potencialmente integrarse en las etapas de desarrollo y de despliegue:

Revisión de código: Se trata de una actividad manual que no está necesariamente integrada durante las pruebas automatizadas, sin embargo, el flujo de integración y despliegue continuo (CI/CD) podría imponer una prueba manual. La revisión en sí misma no cambia necesariamente para la nube, pero hay áreas específicas que sí requieren atención adicional. Cualquier comunicación de aplicación con el plano de gestión a nivel de administración (por ejemplo, las llamadas de una *API* al servicio en la nube, algunas de las cuales pueden alterar la infraestructura) debe ser analizada, especialmente al principio del proyecto. Además de mirar el código en sí, el equipo de seguridad puede enfocarse en asegurar que solo se habilite el principio de mínimos privilegios para esa parte de la aplicación y, a continuación, validarlos con la configuración del plano de gestión. También es importante revisar de manera adicional cualquier elemento relacionado con la autenticación y/o el cifrado. El proceso de despliegue puede automatizarse para incluir notificaciones de seguridad cuando haya modificaciones en estas secciones de código que pueden requerir de una aprobación manual, o simplemente de una revisión de cambios a posteriori.

Pruebas unitarias, *de regresión y funcionales*: Éstas son las pruebas estándar utilizadas por los desarrolladores en sus procesos de desarrollo. Las pruebas de seguridad pueden y deben integrarse en éstas para garantizar que las características de seguridad en la aplicación continúan funcionando tal y como se esperaba. Las pruebas en sí probablemente deben actualizarse para que funcionen en la nube, incluidas algunas de las llamadas a las *APIs*.

Pruebas de análisis estático de código o "caja blanca" (SAST: Static Application Security Testing): Deberían incorporar, además de las pruebas habituales, controles de llamadas *APIs* al servicio en la nube. También deben buscar cualquier componente estático de credenciales integrado en las llamadas a *APIs*, siendo éste un problema creciente.

Pruebas de análisis dinámico de código o "caja negra" (DAST: Dynamic Application Security Testing): DAST realiza pruebas en las aplicaciones en ejecución e incluye pruebas como detección de vulnerabilidades web y *fuzzing*. Debido a los términos del servicio con el

proveedor de la nube, *DAST* puede estar limitado y/o requerir gestionar permisos previos para poder realizarse. Con los flujos de despliegue automáticos y la nube es posible establecer entornos de pruebas completamente funcionales, utilizando infraestructura como código, para luego realizar evaluaciones profundas antes de aprobar los cambios a producción.

10.1.3.1 Impacto en la evaluación de vulnerabilidades

La evaluación de vulnerabilidades puede ser incorporada en el proceso de integración y despliegue continuo (CI /CD) del desarrollo del software, y se puede implementar en la nube de manera sencilla, pero casi siempre requiere cumplir con los términos del servicio acordados con el proveedor.

Generalmente nos encontramos con dos patrones específicos. El primero es ejecutar evaluaciones completas contra imágenes o contenedores, como parte del flujo, en un área especial para pruebas de la nube (un segmento de una red virtual) que está defina para este propósito. La imagen solo será aprobada para ser desplegada en producción si pasa esta prueba. Vemos un patrón similar utilizado para probar infraestructuras enteras construyendo un entorno de prueba usando infraestructura como código.

En ambos casos, se realizan menos pruebas, o incluso ninguna, sobre entornos en producción, ya que deben ser inmutables y equivalente al entorno de pruebas (ambos se basan en los mismos archivos de definición). Las organizaciones también pueden utilizar herramientas de evaluación de vulnerabilidades basadas en host, que se ejecutan localmente en una máquina virtual y, por lo tanto, no requieren coordinación ni permiso del proveedor de la nube.

10.1.3.2 Impacto del test de Intrusión

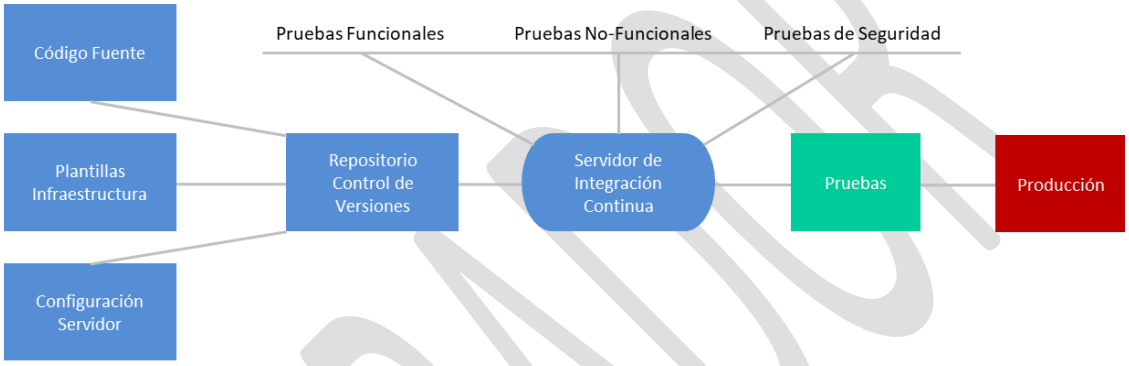
Al igual que con la evaluación de vulnerabilidades, es casi seguro que habrá límites para realizar pruebas de intrusión sin el permiso del proveedor de la nube. El CSA recomienda adaptar las pruebas de intrusión para la nube usando las siguientes pautas:

- Utilice una empresa para realizar las pruebas que tenga experiencia en la ejecución intrusiones en el proveedor de la nube donde se implementa la aplicación.
- Incluir desarrolladores y administradores de la nube en el alcance de la prueba. Muchas de las nubes son atacadas con brechas en quienes mantienen la nube y no directamente a las aplicaciones. Esto incluye el nivel de gestión de la nube.
- Si la aplicación es una aplicación multiusuario, permita que el equipo de testeo tenga acceso autorizado para ver si pueden comprometer el aislamiento definido para el cliente y acceder al entorno o datos de otro cliente.

10.1.3.3 Seguridad en el proceso de despliegue

El proceso de desarrollo de software con integración y despliegue continuo (CI/CD) puede mejorar la seguridad mediante la infraestructura inmutable (menos cambios manuales en los entornos de producción), la automatización de las pruebas de seguridad, el registro añadido de cambios en la aplicación y en la infraestructura cuando estos cambios se ejecutan a través del proceso de despliegue. Con una correcta configuración, los archivos de registros pueden permitir rastrear cada pieza de código, infraestructura y cambio de configuración y vincularlo con el que lo hizo y con el que lo aprobó; podrán incluir también los resultados de las pruebas.

El proceso/flujo en sí necesita estar altamente protegido. Considere aislar estos procesos/flujos en entorno dedicado en la una nube con acceso muy limitado a la nube y/o a la infraestructura que aloja a los componentes del proceso/flujo.



Un proceso de despliegue continuo

10.1.3.4 Impacto de la infraestructura como código e infraestructura inmutable

Nos referimos a la infraestructura como código en varios sitios de esta guía. Debido a la naturaleza virtual y definida por software de la nube, es posible definir, a menudo, entornos completos utilizando plantillas que son traducidas por herramientas (ya sea del proveedor o de terceros) en llamadas a *APIs* que construye automáticamente los entornos. Un ejemplo sencillo es crear la configuración de un servidor a partir de una plantilla. Las implementaciones más complejas pueden construir pilas completas de aplicaciones en la nube, hasta la configuración de red y gestión de identidades.

Dado que estos entornos se crean automáticamente a partir de un conjunto de definiciones de archivos fuente, también pueden ser inmutables. Si el sistema o entorno se crea automáticamente a partir de una plantilla, probablemente con un proceso CI/CD, cualquier cambio realizado en producción será sobrescrito por el próximo cambio de código o plantilla. El entorno de producción puede protegerse, de manera mucho más estricta de lo posible en un despliegue de aplicaciones tradicional (no en la nube), donde gran parte de la infraestructura está configurada manualmente de acuerdo con especificaciones. Cuando la seguridad está adecuadamente incorporada, el uso de la infraestructura como código y despliegues inmutables pueden mejorar significativamente la seguridad.

10.1.4 Operaciones seguras

Cuando una aplicación se implementa en producción, las actividades de seguridad continúan. Muchas de éstas son cubiertas en otras áreas a lo largo de esta Guía, especialmente en el Dominio 7 (Infraestructura), Dominio 8 (Contenedores), Dominio 11 (Datos) y Dominio 12 (Gestión de accesos e identidades). Esta sección contiene recomendaciones adicionales que se aplican más directamente a las aplicaciones:

- El plano de gestión para entornos en producción debe estar mucho más controlada que para los entornos de desarrollo. Como se mencionó anteriormente, si la aplicación directamente accede al nivel de administración del entorno donde está alojado, entonces, los privilegios deben ser los mínimos necesarios. Recomendamos utilizar conjuntos de credenciales diferenciados para cada servicio de aplicación con el fin de segregar aún más los accesos.

- Incluso cuando se utiliza una infraestructura inmutable, en el entorno de producción debe ser monitoreado activamente los cambios y desviaciones de las líneas bases aprobadas. Esto se puede y se debe automatizar a través de código (o herramienta) que haga llamadas *API* a la nube para evaluar regularmente el estado de configuración.

En algunas plataformas de la nube, es posible utilizar funciones integradas de gestión de configuración y evaluación. También es posible deshacer automáticamente los cambios no aprobados, dependiendo de la plataforma y la naturaleza del cambio. Por ejemplo, se puede revertir de manera automática cualquier cambio en una regla de un cortafuegos que no haya sido correctamente aprobada.

- Incluso después la implantación, y aunque se utilice infraestructura inmutable, se debe continuar con las pruebas y evaluación de aplicaciones. En escenarios de nubes públicas, probablemente requerirá la coordinación con el proveedor de la nube para evitar no cumplir con los términos de servicio, al igual que con cualquier evaluación de vulnerabilidades.

- La gestión del cambio no solo incluye la aplicación, sino también cualquier infraestructura e interfaz de gestión de la nube.

Para obtener información sobre respuesta a incidentes, ver el dominio 9; para información sobre la continuidad del negocio y seguridad del nivel de gestión, revisar el dominio 6.

10.1.5 Cómo afecta la nube al diseño y arquitecturas de las aplicaciones

La naturaleza misma de la nube está creando cambios en los diseños de aplicaciones, en las arquitecturas y patrones. Algunos de estos no tienen nada que ver directamente con la seguridad, pero las siguientes tendencias ofrecen oportunidades para reducir problemas comunes de seguridad:

- *Segregación por defecto*: las aplicaciones se pueden ejecutar fácilmente en sus propios entornos aislados de nube. Dependiendo del proveedor, esto podría ser una red virtual o cuenta/subcuenta separada. El uso de cuentas o estructuras de subcuentas ofrece la

ventaja de habilitar segregación a nivel de gestión. La organización puede habilitar derechos de acceso más amplios en cuentas de desarrollo mientras en producción cuentas más restrictivas.

- *Infraestructura inmutable*: como se mencionó, la infraestructura inmutable se está volviendo cada vez más común en la nube, por razones operativas. La seguridad puede extender estos beneficios al deshabilitar inicios de sesión remotos a servidores/contenedores inmutables, agregando monitoreo de la integridad de los archivos, e integrando técnicas inmutables en planes de recuperación ante incidentes.

- *Mayor uso de los microservicios*: en la computación en la nube, es más fácil segregar diferentes servicios en diferentes servidores (o contenedores), debido a que, por un lado, ya no es necesario maximizar la utilización de servidores físicos y, por otro, los grupos de auto-escalado pueden asegurar la escalabilidad de la aplicación incluso cuando se usan granjas de recursos de computación de menor tamaño para ejecutar las cargas de trabajo. Ya que cada nodo hace menos, es más fácil bloquear y minimizar los servicios que se ejecutan en él. Mientras esto mejora la seguridad de cada carga de trabajo (cuando se usa correctamente), implica algunos gastos en asegurar las comunicaciones entre todos los micro servicios y garantizar que cualquier descubrimiento de servicios, planificación y enrutado también sea configurado de forma segura.

- *PaaS y arquitecturas "sin servidor":* con *PaaS* y configuraciones "sin servidor" (ejecutando cargas de trabajo directamente en la plataforma del proveedor de la nube, donde no administras los servicios subyacentes ni el funcionamiento sistema) existe un gran potencial para reducir considerablemente la superficie de ataque. Esto es solo si el proveedor de la nube asume la responsabilidad de la seguridad de la configuración de la plataforma/servidor y cumple con nuestros requisitos.

El trabajar sin servidores puede ofrecer algunas ventajas. En primer lugar, existen grandes incentivos económicos para que el proveedor mantenga niveles de seguridad extremadamente altos y el entorno actualizado. Esto elimina al usuario de la nube la responsabilidad en el día a día de mantener estos controles, sin olvidar que sigue siendo el responsable de la seguridad de su aplicación. Por lo tanto, resulta crítico trabajar con un proveedor de la nube confiable y con una sólida trayectoria.

Continuando, las plataformas sin servidor se pueden ejecutar en la red del proveedor con comunicaciones a las componentes del usuario a través de *APIs* o tráfico HTTPS. Esto elimina el vector de ataque directo a la red, incluso si un atacante compromete un servidor o contenedor. El atacante está limitado a intentar llamadas *API* o tráfico HTTPS y no puede escanear puertos, identificar otros servidores o utilizar otras técnicas comunes.

- *Seguridad definida por software*: los equipos de seguridad pueden aprovechar todas las mismas herramientas y tecnologías para automatizar muchas operaciones de seguridad, incluso integrándolas con la pila de aplicaciones. Algunos ejemplos incluyen la automatización de la respuesta a incidentes en la nube, la automatización de cambios dinámicos en permisos y la resolución de cambios de infraestructura no aprobados.

- *Seguridad basada en eventos*: algunos proveedores de la nube soportan la ejecución de código basado en eventos. En estos casos, el interfaz de administración detecta

diversas actividades -como que un archivo se cargue en una ubicación designada de almacenamiento de objetos, o un cambio de configuración en la red, o de gestión de identidades- que a su vez pueden activar la ejecución del código a través de un mensaje de notificación, o mediante un código alojado “sin servidor”. Se puede definir eventos para acciones de seguridad y usar las capacidades basadas en eventos para desencadenar la notificación automatizada, evaluación, remediación u otros procesos de seguridad.

10.1.6 Consideraciones adicionales para proveedores de servicios de nube

Los proveedores de la nube de todos los modelos de servicio deben prestar especial atención a ciertos aspectos de sus servicios dado que podrían causar problemas muy importantes para sus clientes si existen fallos de seguridad:

- Las *APIs* y los servicios web deben ser fuertemente protegidos (*hardening*) y asumir que habrá ataques tanto de adversarios autenticados como no autenticados. Esto incluye el uso de autenticación estándar de la industria, diseñada específicamente para *APIs*.
- Las *APIs* deben monitorizarse frente abuso y actividad inusual.
- El servicio debe someterse a un diseño y pruebas exhaustivos para prevenir ataques o accesos inapropiados/accidentales entre usuarios de la nube.

10.1.7 El nacimiento y papel de *DevOps*

DevOps se refiere a la integración más profunda entre los equipos de desarrollo y operaciones a través de una mejor colaboración y comunicación, con un fuerte enfoque en la automatización de la implantación de aplicaciones y operaciones de infraestructura. Hay múltiples definiciones, pero la idea general consiste en una cultura, filosofía, procesos y herramientas.

En el núcleo está la combinación de CI/CD a traves de procesos de implantación automatizada y el uso de herramientas de automatización para administrar mejor la infraestructura. *DevOps* no es exclusivo de la nube, pero como comentamos está muy en sintonía con la nube y desarrollándose para convertirse en el modelo dominante de entrega de aplicaciones en la nube.

10.1.7.1 Implicaciones y ventajas en seguridad

- *Estandarización*: con *DevOps*, todo lo que entra en producción es creado por el proceso CI/CD mediante código aprobado y plantillas de configuración. Los entornos de desarrollo, pruebas y producción se basan en exactamente los mismos archivos de origen, lo que elimina cualquier desviación de estándares bien conocidos.
- *Pruebas automatizadas*: tal y como comentamos, se puede integrar una amplia variedad de pruebas de seguridad en el proceso CI/CD, con pruebas manuales adicionales según sea necesario complementar.

- *Inmutables*: los procesos de CI/CD pueden producir imágenes maestras para máquinas virtuales, contenedores y pilas de infraestructura de manera rápida y confiable. Esto permite implementaciones automatizadas e infraestructura inmutable.

- *Mejoras en auditoría y gestión del cambio*: los procesos de CI/CD pueden rastrearlo todo, hasta cambios de caracteres individuales en los archivos de origen que están vinculados a la persona que envía el cambio, con el historial completo de la pila de aplicaciones (incluida la infraestructura) almacenado en el repositorio de control de versiones. Esto ofrece considerables beneficios de auditoría y control de cambios.

- *SecDevOps/DevSecOps y DevOps robusto (rugged DevOps)*: estos términos están apareciendo para describir la integración de las actividades de seguridad en *DevOps*. *SecDevOps/DevSecOps* a veces se refiere al uso de técnicas de automatización *DevOps* para mejorar las operaciones de seguridad. *DevOps* robusto se refiere a la integración de pruebas de seguridad en el proceso de desarrollo de aplicaciones para producir aplicaciones más resistentes, más seguras y más resilientes.

10.2 Recomendaciones

- Comprender las capacidades de seguridad de sus proveedores de la nube. No solo su línea base, sino las diversas plataformas y servicios.

- Construir la seguridad desde el proceso de diseño inicial. Las implementaciones en la nube se diseñan muy a menudo desde cero, creando nuevas oportunidades para involucrar a seguridad desde el inicio.

- Incluso si no tiene un SDLC formal, considere pasar a la implantación continua y automatizar la seguridad en el proceso de implantación.

- Los modelos de amenazas, *SAST* y *DAST* (con *fuzzing*) deberían estar todos integrados. Las pruebas deben ser configuradas para trabajar en el entorno de la nube, pero también para revisar las preocupaciones específicas de las plataformas de nube, como las credenciales almacenadas en las *API*.

- Comprender las nuevas opciones y requisitos de arquitectura en la nube. Actualizar las políticas y estándares de seguridad para soportarlos, y no simplemente intentar forzar los estándares existentes en un modelo informático completamente diferente.

- Integrar las pruebas de seguridad en el proceso de implementación.

- Utilizar seguridad definida por software para automatizar los controles de seguridad.

- Utilizar seguridad basada en eventos, cuando esté disponible, para automatizar la detección y solución de problemas de seguridad. Usar diferentes entornos de nube para segregar mejor el acceso al nivel de administración y proporcionar a los desarrolladores la libertad que necesitan para configurar los entornos de desarrollo, mientras que también se bloquean los entornos de producción.

Dominio 11 Seguridad y Cifrado de Datos

11.0 Introducción

La seguridad de los datos es una herramienta clave para el gobierno de la información y los datos. Al igual que con todas las otras áreas de la seguridad de la nube, su utilización debería ser basada en riesgo ya que no es apropiado asegurar todo de la misma manera.

Esto es cierto para la seguridad de los datos en general, independiente de si está involucrada la nube o no. Sin embargo, muchas organizaciones no están acostumbradas a confiar grandes volúmenes de sus datos sensibles -- si es que no todos -- a un tercero, o a combinar todos sus datos internos en un repositorio de recursos compartidos. En estos casos, la reacción instintiva puede ser el fijar una política de seguridad global para “cualquier cosa en la nube”, en vez de adherirse a una aproximación basada en riesgo, la cual será mucho más segura y efectiva en costes.

Por ejemplo, cifrar todo lo que está en *SaaS* porque no confías en el proveedor con toda seguridad significa que no deberías estar usando a dicho proveedor en primer lugar. Cifrar todo no es un remedio para todo y puede llevar a una falsa sensación de seguridad, por ejemplo, cifrar el tráfico de datos sin preocuparse de la seguridad de los propios dispositivos.

De acuerdo con algunos puntos de vista la seguridad de la información es la seguridad de los datos, pero para nuestros propósitos este dominio se focalizará en aquellos controles relacionados con asegurar los propios datos, de los cuales el cifrado es uno de los más importantes.

11.1 Visión general

11.1.1 Controles de seguridad de los datos

Los controles de seguridad de los datos tienden a caer en tres categorías. Cubriremos todas ellas en esta sección:

- Controlar qué datos van a la nube (y dónde).

- Proteger y gestionar los datos en la nube. Los controles y procesos clave son:
    - Controles de acceso
    - Cifrado
    - Arquitectura
    - Monitoreo/alertas (de uso, configuración, estado del ciclo de vida, etc.)
    - Controles adicionales, incluyendo aquellos relacionados con el producto/servicio/plataforma específica de su proveedor de nube, prevención de fuga de datos, y gestión de permisos corporativos.

- Imposición de la seguridad de la gestión del ciclo de vida de la información.
    - Gestionar la ubicación/residencia de los datos.
    - Asegurar el cumplimiento, incluyendo artefactos de auditoría (logs, configuraciones).
    - Respaldos y continuidad de negocio, los que son cubiertos en el Dominio 6.

11.1.2 Tipos de almacenamiento de datos en la nube

Debido a que el almacenamiento en la nube está virtualizado, tiende a soportar distintos tipos de almacenamiento de datos que los usados en tecnologías de almacenamiento tradicionales. Bajo la capa de virtualización pueden utilizar mecanismos de almacenamiento conocidos, pero las tecnologías de virtualización de almacenamiento en la nube a las que los usuarios de la nube acceden, serán diferentes. Estas son las más comunes:

Almacenamiento de objetos: El almacenamiento de objetos es similar a un sistema de archivos. Los “objetos” son típicamente archivos, los cuales son almacenados utilizando un mecanismo específico de la plataforma de nube. La mayoría de los accesos son a través de *APIs*, no a través de protocolos estándar para compartir archivos, aunque los proveedores de nube también pueden ofrecer interfaces *front-end* para soportar dichos protocolos.

Almacenamiento de Volúmenes: Esto es esencialmente un disco duro virtual para instancias/máquinas virtuales.

Base de Datos: Las plataformas y proveedores de nube pueden soportar una variedad de distintos tipos de bases de datos, incluyendo opciones comerciales y de código abierto, así como sus propios sistemas propietarios. Las bases de datos propietarias típicamente utilizan sus propias *APIs*. Las bases de datos comerciales o de código abierto son alojadas por el proveedor y utilizan típicamente estándares existentes para las conexiones. Estas pueden ser relacionales o no-relacionales -- estas últimas incluyen NoSQL y otros sistemas de almacenamiento de llave/valor, o bases de datos basadas en sistemas de archivos (p.ej. *HDFS*).

Aplicación/plataforma: Ejemplos de esto sería una red de distribución de contenidos (*CDN* por su nombre en inglés), archivos almacenados en *SaaS*, y otras opciones novedosas.

La mayoría de las plataformas de nube también utilizan mecanismos de almacenamiento duradero y redundante que a menudo utilizan *dispersión de los datos* (a veces también conocido como *data fragmentation* o *bit splitting*). Este proceso toma porciones de datos, las divide, y luego almacena múltiples copias en distintos almacenamientos físicos para proveer alta durabilidad. Los datos almacenados de esta manera están físicamente dispersos. Un archivo, por ejemplo, no estaría ubicado en un único disco duro.

11.1.3 Gestionando la migración de datos hacia la nube

Antes de asegurar los datos en la nube, la mayoría de las organizaciones quiere algún mecanismo para gestionar qué datos son almacenados en proveedores de nube privados y públicos. A menudo esto es esencial para el cumplimiento tanto o más que para la seguridad.

Para comenzar, defina sus políticas para qué tipos de datos serán permitidos y dónde serán permitidos, luego asocie estos a sus requerimientos de seguridad de línea base. Por ejemplo, "Datos de Carácter Personal (PII por su nombre en inglés) serán permitidos en *x* servicios, asumiendo que cumplen con los requerimientos de cifrado y controles de acceso."

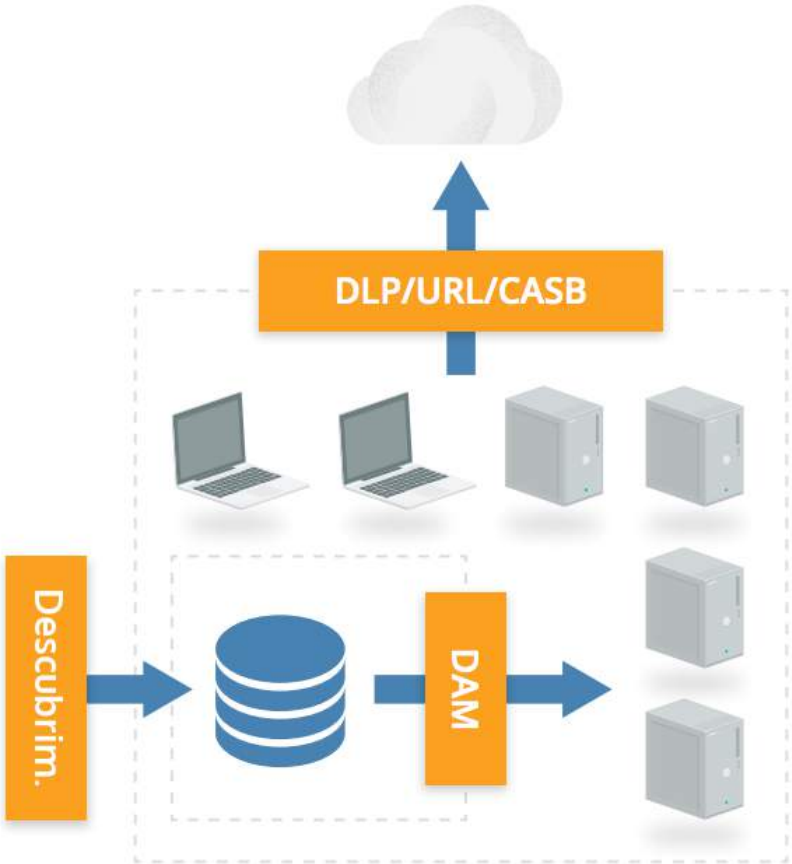
Luego identifique sus repositorios clave de datos. Monitoree la ocurrencia de grandes migraciones/actividades, utilizando herramientas tales como Monitorización de Actividad de Base de Datos y Monitorización de Actividad de Archivos. Esencialmente se trata de construir un "sistema de alerta temprana" para grandes transferencias de datos, pero también es un importante control de seguridad de los datos para detectar todo tipo de escenarios de grandes fugas o de mala utilización.

Para detectar migraciones reales, monitoree la utilización de la nube y cualquier tipo de transferencia de datos. Puede hacer esto con la ayuda de las siguientes herramientas:

***CASB*:** *Cloud Access and Security Brokers* (también conocidos como *Cloud Security Gateways*) sirve para descubrir el uso interno de servicios de nube utilizando diversos mecanismos tales como monitoreo de red, integrándose con una puerta de enlace de red o herramienta de monitoreo existente, o incluso monitoreando las consultas *DNS*. Después de descubrir a qué servicio se están conectando sus usuarios, la mayoría de estos productos ofrecen monitorear la actividad de los servicios permitidos a través de conexiones *API* (cuando estén disponibles) o interceptación en línea (monitoreo de hombre en el medio). Muchos soportan *DLP* y otras alertas de seguridad e incluso ofrecen controles para gestionar de mejor forma el uso de datos sensibles en servicios de nube (*SaaS*/*PaaS*/e *IaaS*).

Filtrado de *URL*: Pese a no ser tan robusto como *CASB*, el filtrado de *URL*s/puerta de enlace web puede ayudarle a entender qué servicios de nube están utilizando sus usuarios (o tratando de usar).

***DLP*:** Si monitorea su tráfico web (y mira dentro de sus conexiones *SSL*) una herramienta de Data *Loss Prevention* (*DLP*) también puede ayudar a detectar migraciones de datos hacia servicios de nube. Sin embargo,



algunos *SDKs* y *API* de nube pueden cifrar parte de los datos y el tráfico, los que el *DLP* no podrá escrutar, y no podrá ser capaz de analizar y entender su contenido.

11.1.3.1 Asegurando las transferencias de datos en la nube

Asegurar que está protegiendo sus datos cuando los mueve hacia la nube. Esto requiere entender los mecanismos de migración de datos de su proveedor, ya que aprovechar dichos mecanismos es a menudo más seguro y efectivo en costes que métodos “manuales” de transferencia de datos tales como el Protocolo Seguro de Transferencia de Archivos (SFTP por su nombre en inglés). Por ejemplo, enviar datos al almacenamiento de objetos de un proveedor utilizando su *API* es probablemente mucho más confiable y seguro que configurar su propio servidor SFTP en una máquina virtual en el mismo proveedor.

Hay algunas opciones para el cifrado en tránsito de los datos, éstas dependen de lo que soporte la plataforma de nube. Una forma de hacerlo es cifrar antes de enviar a la nube (cifrado en el lado del cliente). Otra opción es el cifrado de red (TLS/SFTP/etc.). La mayoría de las *APIs* de los proveedores de nube utilizan Seguridad de Capa de Transporte (TLS por su nombre en inglés) por defecto; si es que no lo hace, elija un proveedor distinto, ya que ésta es una capacidad de seguridad esencial. El cifrado basado en proxy puede ser una tercera opción, en la que se instala un proxy de cifrado en un área de confianza entre el usuario de nube y el proveedor de nube y el proxy gestiona el cifrado antes de transferir los datos hacia el proveedor.

En algunos casos puede tener que aceptar datos públicos o que no son de confianza. Si permite que asociados o el público le envíen datos, asegúrese de tener los mecanismos de seguridad adecuados para “*sanitizar*” los datos antes de procesarlos o mezclarlos con sus datos existentes. Siempre aísle y revise estos datos antes de incorporarlos.

11.1.4 Asegurando los datos en la nube

Los controles de acceso y el cifrado son los controles principales de seguridad de datos en diversas tecnologías.

11.1.4.1 Controles de acceso a los datos en nube

Los *controles de acceso* deberían ser implementados con un mínimo de tres capas:

- *Plano de Gestión:* Estos son los controles para gestionar el acceso de usuarios que acceden directamente al plano de gestión de la plataforma de nube. Por ejemplo, iniciar sesión en la consola web de un servicio *IaaS* le permitirá a ese usuario acceder a los datos en el almacenamiento de objetos. Afortunadamente, la mayoría de las plataformas y proveedores de nube comienzan por defecto con políticas de control de acceso de denegación.

- *Controles de Compartición Interna y Pública:* Si los datos son compartidos externamente al público o a asociados que no tienen acceso directo a la plataforma de nube, deberá existir una segunda capa de controles para este acceso.
- *Controles a nivel de aplicación:* En la medida que construya sus propias aplicaciones en la plataforma de nube, deberá diseñar e implementar sus propios controles para gestionar el acceso.

Las opciones de control de acceso variarán basados en el modelo de servicio de nube y en las características específicas de cada proveedor. Una matriz de asignación de derechos documenta qué usuarios, grupos y roles deberían tener acceso a qué recursos y funciones.

Asignación de derechos	Super Administrador	Administrador del Servicio	Administrador del Almacenamiento	Desarrollador	Auditor de Seguridad	Administrador de Seguridad
Describir el Volumen	X	X		X	X	X
Describir los Objetos	X		X	X	X	X
Modificar el Volumen	X	X		X		X
Leer los logs	X				X	X

Valide frecuentemente (idealmente en forma continua) que sus controles cumplen con sus requerimientos, poniendo particular atención a cualquier recurso compartido públicamente. Considere la configuración de alertas ante la creación de cualquier nuevo recurso compartido públicamente o ante cambios en los permisos que otorguen el acceso público.

Controles de acceso finos y asignaciones de derechos

La profundidad de los derechos potenciales variará mucho de una tecnología a otra. Algunas bases de datos pueden admitir seguridad a nivel de fila, otras poco más que un acceso amplio. Algunas permitirán ligar los derechos a los mecanismos de identidad y aplicación incorporados en la plataforma de la nube, mientras que otras confían completamente en la plataforma de almacenamiento en sí misma ejecutándose meramente en máquinas virtuales.

Es importante comprender sus opciones, mapearlas y construir su matriz. Esto aplica más que solo al acceso a archivos, por supuesto; también se aplica a bases de datos y todos sus almacenes de datos en la nube.

11.1.4.2 Cifrado (en reposo) del almacenamiento y uso de *Tokens*

Las opciones de cifrado varían ampliamente dependiendo del modelo de servicio, del proveedor, y de aspectos específicos de la aplicación/desarrollo. La gestión de claves es tan esencial como el cifrado, y por ello es cubierto en una sección posterior.

El cifrado y el uso de *tokens* son dos tecnologías separadas. El cifrado protege los datos aplicando un algoritmo matemático que "revuelve" los datos, los cuales luego solo pueden ser recuperados al pasarlos por un proceso de ordenamiento (descifrado) con la clave correspondiente. El resultado es un montón de texto cifrado. El uso de *tokens*, por otra parte, toma los datos y los reemplaza con valores al azar. Luego almacena las versiones original y aleatoria en una base de datos segura para poder ser recuperados posteriormente.

El uso de *token* es frecuente cuando el *formato* de los datos es importante (p.ej. reemplazando números de tarjeta de crédito en un sistema existente que requiere el formato de texto en la cadena de caracteres). El cifrado con conservación de formato cifra los datos con una clave, pero también mantiene la misma estructura de formato al igual que el uso de *tokens*, pero puede que no sea criptográficamente seguro debido a los compromisos.

Existen tres componentes en un sistema de cifrado: los datos, el motor de cifrado, y el gestor de claves. Los datos son, por supuesto, la información que se está cifrando. El motor es lo que realiza el proceso matemático de cifrado. Finalmente, el gestor de claves maneja las claves para el cifrado. El diseño general del sistema se focaliza en dónde poner cada uno de estos componentes.

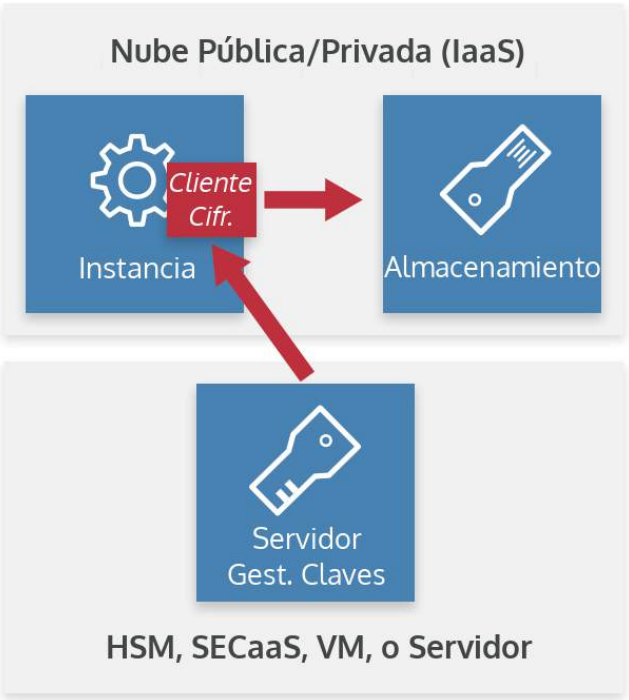
Cuando se esté diseñando un sistema de cifrado, se debería comenzar con un modelo de amenazas. Por ejemplo, ¿confía en su proveedor de nube para gestionar sus claves? ¿Cómo podrían ser expuestas las claves? ¿Dónde debería ubicar el motor de cifrado para gestionar las amenazas que le preocupan?

Cifrado IaaS

Los volúmenes *IaaS* pueden ser cifrados utilizando métodos diferentes, dependiendo de los datos.

Cifrado de Almacenamiento en Volúmenes

- *Cifrado gestionado por instancia:* El motor de cifrado se ejecuta dentro de la instancia, y la clave se almacena en el volumen, pero protegida por una contraseña o un par de claves.
- *Cifrado gestionado externamente:* El motor de cifrado se ejecuta en la instancia, pero las claves son gestionadas externamente y son



Cifrado de volúmenes gestionado externamente

provistas a la instancia a pedido.

Almacenamiento de Objetos y Archivos

- *Cifrado del lado del cliente:* Cuando se utiliza el almacenamiento de objetos como el *back-end* para una aplicación (incluyendo aplicaciones móviles), cifre los datos utilizando un motor de cifrado embebido en la aplicación o cliente.
- *Cifrado del lado del servidor:* Los datos son cifrados en el lado del servidor (nube) después de haber sido transferidos. El proveedor de nube tiene acceso a la clave y ejecuta el motor de cifrado.
- *Cifrado por proxy:* En este modelo, se conecta el volumen a una instancia especial o a un *appliance*/aplicativo, y luego se conecta la instancia a la instancia de cifrado. El proxy maneja todas las operaciones de cifrado y puede tener las llaves dentro o fuera.

Cifrado PaaS

El cifrado *PaaS* varía mucho dependiendo de las distintas plataformas *PaaS*.

- *Cifrado en capa de aplicación:* Los datos son cifrados en la aplicación *PaaS* o en el cliente que se utiliza para acceder a la plataforma.
- *Cifrado en base de datos:* Los datos son cifrados en la base de datos utilizando los mecanismos nativos y es soportado por una plataforma de base de datos como Cifrado de Base de Datos Transparente (TDE por su nombre en inglés) o a nivel de campos.
- *Otro:* Estas son capas gestionadas por el proveedor en la aplicación, tales como la cola de mensajes. También existen opciones de *IaaS* cuando son utilizadas para el almacenamiento subyacente.

Cifrado SaaS

Los proveedores de *SaaS* pueden utilizar cualquiera de las opciones previamente mencionadas. Se recomienda que utilicen claves distintas para cada cliente cuando sea posible, para imponer de mejor manera el aislamiento multi-cliente. Las siguientes opciones son para clientes de *SaaS*:

- *Cifrado gestionado por el proveedor:* Los datos son cifrados en la aplicación *SaaS* y generalmente gestionados por el proveedor.
- *Cifrado por proxy:* Los datos pasan a través de un proxy de cifrado antes de ser enviados a la aplicación *SaaS*.

11.1.4.3 Gestión de claves (incluyendo claves gestionadas por el cliente)

Las principales consideraciones para la gestión de claves son rendimiento, accesibilidad, latencia, y seguridad. ¿Se puede llevar la clave correcta al lugar correcto en el momento correcto y al mismo tiempo satisfacer los requerimientos de cumplimiento y de seguridad?

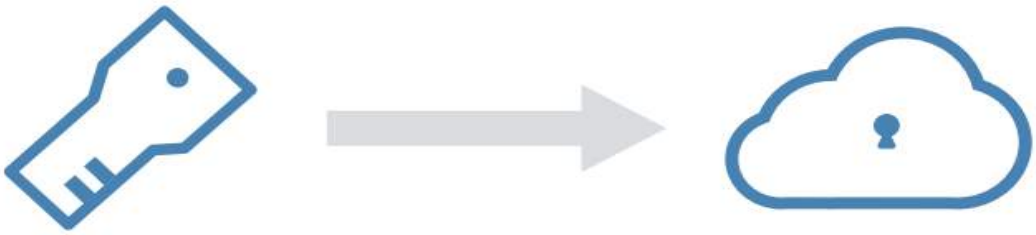
Existen cuatro opciones potenciales para manejar la gestión de claves:

- *HSM/appliance:* Utilizar un módulo de seguridad de hardware (HSM por su nombre en inglés) tradicional o un gestor de claves basado en *appliance*, el cual típicamente requiere estar en instalaciones del cliente, y entregar las claves a la nube sobre una conexión dedicada.

- *Appliance virtual/software:* Instalar un gestor de claves basado en *appliance* virtual o en software, en la nube.
- *Servicio de proveedor de nube:* Este es un servicio de gestión de claves ofrecido por el proveedor de nube. Antes de seleccionar esta opción, asegúrese de comprender el modelo de seguridad y los *SLAs* para entender si sus claves podrían ser expuestas.
- *Híbrido:* También puede utilizar una combinación de opciones, tal como utilizar un HSM como la raíz de confianza para las claves, pero luego entregar claves específicas para cada aplicación a un *appliance* virtual que está ubicado en la nube y solo gestiona claves para un contexto particular.

Claves gestionadas por el cliente

Una clave gestionada por el cliente permite que un cliente de la nube gestione su propia clave de cifrado mientras el proveedor gestiona el motor de cifrado. Por ejemplo, utilizar su propia clave para cifrar los datos de SaaS dentro de la plataforma *SaaS*. Muchos proveedores cifran los datos por defecto, utilizando claves que están completamente en su control. Algunos de ellos pueden permitirle sustituirlas por sus propias claves, las que integrará en su sistema de cifrado. Asegúrese que las prácticas de su proveedor estén alineadas con sus requerimientos.



Claves gestionadas por el cliente

Algunos proveedores pueden solicitarle que utilice un servicio del mismo proveedor para gestionar las claves. Luego, pese a que las claves son gestionadas por el cliente, potencialmente también están disponibles al proveedor. Esto no necesariamente significa que sea inseguro: Ya que los sistemas de gestión de claves y de gestión de almacenamiento de datos pueden ser separados, sería necesaria la colusión de parte de múltiples empleados del proveedor para potencialmente comprometer los datos. Sin embargo, las claves y los datos podrían ser expuestos ante una solicitud del gobierno, dependiendo de las leyes locales. También se puede almacenar las claves en forma externa al proveedor y solo entregarlas a pedido.

11.1.5 Arquitecturas de seguridad de datos

La arquitectura de la aplicación impacta la seguridad de los datos. Las características que su proveedor de nube ofrezca pueden reducir la superficie de ataque, pero asegúrese de exigir una meta-estructura de seguridad fuerte. Por ejemplo, aísle redes utilizando almacenamiento en la nube o un servicio de colas que lo comunique con la red del proveedor, no dentro de su

red virtual. Esto forzará a los atacantes a comprometer al proveedor de nube en su totalidad o bien limitarse a ataques a nivel de aplicación, ya que las rutas para ataques de red estarán cerradas.

Un ejemplo de esto sería el utilizar almacenamiento de objetos para transferencia de datos y procesamiento por lotes, en vez de realizar transferencias por SFTP a instancias estáticas. Otro ejemplo es aislar por cola de mensajes, ejecutar componentes de la aplicación en distintas redes virtuales que no están conectadas, transfiriendo datos a través del servicio de cola de mensajes del proveedor de nube. Esto elimina los ataques de red de una parte de la aplicación a la otra.

11.1.6 Monitoreo, auditoría, alerta

Estos deberían enlazarse en un monitoreo global de la nube (Ver Dominios 3, 6 y 7). Se debe identificar (y alertar acerca del mismo) cualquier acceso público o cambio en la asignación de derechos a datos sensibles. Se debe utilizar etiquetado para soportar las alertas si es que está disponible.

Se necesitará monitorear tanto el acceso a la *API* como el acceso al almacenamiento, ya que los datos pueden ser expuestos por cualquiera de las dos -- en otras palabras, el acceso a los datos en el almacenamiento de objetos a través de una llamada a la *API* o a través de compartir en forma pública una *URL*. El monitoreo de actividad, incluyendo el Monitoreo de Actividad de Base de Datos, puede ser una opción. Asegúrese de almacenar sus logs en una ubicación segura, como una cuenta dedicada al registro de logs.

11.1.7 Controles adicionales de seguridad de los datos

11.1.7.1 Controles Específicos de la Plataforma/Proveedor de Nube

Una plataforma o proveedor de nube pueden tener controles de seguridad de los datos que no estén cubiertos en ninguna otra parte en este dominio. Pese a que típicamente ellos corresponderán a alguna forma de control de acceso o cifrado, esta Guía no puede cubrir todas las opciones posibles.

11.1.7.2 Prevención de fuga de datos

La Prevención de Fuga de Datos (*DLP* por su nombre en inglés) es una forma típica de monitorear y proteger los datos a los que sus empleados acceden, por medio de monitoreo de sistemas locales, web, correo electrónico, y otro tipo de tráfico. No se usa típicamente en centros de procesamiento de datos, luego es más aplicable a *SaaS* que a *PaaS* o *IaaS*, donde usualmente no se aplica.

- *CASB:* Algunos *CASB*s incluyen características básicas de *DLP* para los servicios específicos que protegen. Por ejemplo, se podría configurar una política para que los números de tarjeta de crédito jamás sean almacenados en un servicio de nube en particular. La efectividad depende en gran medida de la herramienta específica, el

servicio de nube, y cómo el *CASB* está integrado para monitorear. Algunas herramientas de *CASB* también pueden encaminar tráfico a plataformas dedicadas de *DLP* para un análisis más robusto que el que típicamente está disponible en el *CASB* cuando ofrece características de *DLP*.

- *Característica del Proveedor de Nube:* El propio proveedor de nube puede ofrecer capacidades de *DLP*, tales como una plataforma de almacenamiento de archivos y de colaboración en la nube que revise los archivos que se suben en busca de contenido y les aplique las políticas de seguridad respectivas.

11.1.7.3 Gestión de derechos empresariales

Al igual que con *DLP*, este es típicamente un control de seguridad para los empleados que no siempre es aplicable en la nube. Dado que todos los Gestores de Derechos Digitales (*DRM* por su nombre en inglés) / Gestor de Derechos Empresariales (*ERM* por su nombre en inglés) están basados en cifrado, las herramientas existentes pueden romper las capacidades de nube, especialmente en SaaS.

- *DRM Completo:* Corresponde a la gestión tradicional y completa de derechos digitales, utilizando una herramienta existente. Por ejemplo, aplicar derechos a un archivo antes de almacenarlo en el servicio de nube. Como se mencionó, puede que rompa algunas características del proveedor de nube, tales como previsualización en el navegador o la colaboración, a menos que exista algún tipo de integración (lo cual es raro al momento de escribir este documento).

- *Control basado en el proveedor:* La plataforma de nube puede ser capaz de imponer los controles de manera muy similar al *DRM* completo utilizando capacidades nativas. Por ejemplo, usuario/dispositivo/vista contra edición: una política que solo permite a ciertos usuarios ver un archivo en un navegador web, mientras que otros usuarios pueden descargar y/o editar los contenidos. Algunas plataformas incluso pueden vincular estas políticas a dispositivos específicos, no solo a nivel de usuario.

11.1.7.4 Enmascaramiento de datos y generación de datos de prueba

Estas son técnicas para proteger los datos utilizados en ambientes de desarrollo y de pruebas, o para limitar el acceso en tiempo real a los datos en las aplicaciones.

- *Generación de datos de prueba:* Corresponde a la creación de una base de datos con datos de prueba no sensibles, basados en una base de datos “real”. Puede utilizar desordenamiento y otras técnicas de aleatorización para crear un conjunto de datos que se parece al origen en tamaño y estructura pero que carece de datos sensibles.

- *Enmascaramiento dinámico:* El enmascaramiento dinámico reescribe los datos sobre la marcha, típicamente utilizando un mecanismo de proxy, para enmascarar todos o una

parte de los datos a un usuario. Se utiliza habitualmente para proteger algunos datos sensibles en aplicaciones, por ejemplo, enmascarando todos excepto los últimos dígitos de un número de tarjeta de crédito cuando se le presenta a un usuario.

11.1.8 Imposición de la gestión del ciclo de vida de la seguridad

- *Gestionar la ubicación/residencia de los datos:* En ciertos momentos, se necesitará inhabilitar ubicaciones que ya no son necesarias. Se deberá utilizar el cifrado para imponer el acceso a nivel de contenedor u objeto. Luego, incluso si los datos se mueven a una ubicación que no ha sido aprobada, los datos aún estarán protegidos a menos que la clave se mueva con ellos.

- *Asegurar cumplimiento:* No solo se necesita implementar controles para mantener el cumplimiento, también se necesita documentar y probar dichos controles. Estos son "artefactos de cumplimiento", e incluyen cualquier artefacto de auditoría que se tenga.

- *Respaldos y continuidad de negocio:* Vea el Dominio 6.

11.2 Recomendaciones

- Entienda las capacidades específicas de la plataforma de nube que está utilizando.
- No descarte la seguridad de los datos del proveedor de nube. En muchos casos es más segura que construir la propia, y tiene un costo menor.
- Cree una matriz de asignación de derechos para determinar los controles de acceso. La imposición variará dependiendo de las capacidades del proveedor de nube.
- Considere *CASB* para monitorear los datos que fluyen hacia un *SaaS*. Incluso puede ser útil para algunos *PaaS* e *IaaS*, pero apóyese más en las políticas existentes y en la seguridad del repositorio de datos para esos tipos de grandes migraciones.
- Utilice las opciones de cifrado apropiadas basado en el modelo de amenazas de sus datos, negocio, y requerimientos técnicos.
- Considere utilizar las opciones de cifrado y almacenamiento gestionado que ofrezca el proveedor. Cuando sea posible, utilice claves gestionadas por el cliente.
- Aproveche la arquitectura para mejorar la seguridad de los datos. No dependa completamente en controles de acceso y cifrado.
- Asegúrese que exista monitoreo a nivel de *API* y de datos, y que los logs se ajustan a los requerimientos de cumplimiento y políticas de ciclo de vida.
- Los estándares existen para ayudar a establecer una buena seguridad y el correcto uso de técnicas y procesos de cifrado y gestión de claves. Específicamente, *NIST* SP-800-*57* y *ANSI X9.69 y X9.73.*

Dominio 12 Gestión de Identidades, Derechos y Accesos

12.0 Introducción

La Gestión de Identidades, asignación de derechos y accesos (*IAM* por sus siglas en inglés) están profundamente afectados por la computación en la nube. En las nubes públicas y privadas ambos participantes (proveedor y usuario) son necesarios para la gestión de identidades y el control de acceso sin comprometer la seguridad. Este dominio se centra en qué cambios son necesarios en la gestión de identidades en entornos de nube. Se revisarán conceptos fundamentales manteniendo el foco principal en cómo la nube cambia la gestión de identidades y qué hacer al respecto.

La computación en la nube introduce múltiples cambios en cómo se ha gestionado tradicionalmente la identidad y el acceso en los sistemas internos. No quiere decir que sean problemas nuevos, pero son problemas mayores cuando se trata de entornos de nube.

La diferencia principal es la relación entre el proveedor de servicio de nube y el usuario de la nube, incluso si se trata de nubes privadas. La gestión de identidades y el control de acceso no pueden ser gestionados por uno de los actores de manera individual, sino que se requieren relaciones de confianza y delegación de responsabilidades, que son implementadas por diferentes mecanismos técnicos. Normalmente estos mecanismos técnicos se implementan como una federación de identidades. Esto se complica por el hecho de que muchas organizaciones tienen diferentes (a veces cientos) proveedores de nube para los que es necesario extender dicha gestión.

La nube tiende a cambiar más rápidamente, a ser un entorno más distribuido (incluso en diferentes jurisdicciones legales), a incrementar la complejidad de la gestión y a basarse principalmente (y en la mayoría de las ocasiones de manera exclusiva) en amplias redes de comunicación para toda su actividad, lo que expone la infraestructura principal de administración a ataques en red. Como extra hay muchas diferencias entre los distintos proveedores, y entre los servicios y modos de uso.

Este dominio se centra principalmente en la gestión de identidades y el control de acceso entre una organización y los proveedores de servicio o bien entre los proveedores y los servicios ofrecidos. Está fuera del alcance del presente dominio la gestión de identidades y el control de acceso dentro de una aplicación en la nube, como por ejemplo la gestión dentro de una aplicación empresarial corriendo en *IaaS*. Estos problemas son muy similares a los que se encuentran en diferentes aplicaciones y servicios que usan infraestructuras tradicionales.

12.0.1 Cómo la gestión de identidades y el control de acceso es diferente en la nube

La gestión de identidades y el control de acceso siempre son difíciles. En último término se están asociando diferentes entidades (una persona, sistema, partes de código, etc.) a una identidad verificable que posee varios atributos (que pueden cambiar bajo determinadas circunstancias) y entonces se toma una decisión sobre qué puede hacer y qué no basado en sus asignaciones de derechos. Incluso cuando controlas toda la cadena de ese proceso, gestionarlo a través de sistemas y tecnologías dispares de una forma segura y verificable, especialmente a gran escala, es un desafío.

En la computación en la nube el problema fundamental es que diferentes organizaciones están gestionando la identidad y el control de acceso a diferentes recursos, lo que puede complicar el proceso. Por ejemplo, imagine tener que provisionar el mismo usuario a decenas o cientos de servicios diferentes en la nube. La federación de identidades es la principal herramienta para gestionar este problema, creando relaciones de confianza e imponiéndolas a través de diferentes estándares.

La federación de identidades y otras técnicas de gestión y control de acceso han existido desde antes de las primeras computadoras (simplemente pregúntele a un banco o a un gobierno). A lo largo del tiempo las organizaciones han creado retazos y silos de gestión de identidades a medida que sus tecnologías de la información han ido evolucionando. La computación en la nube se puede ver como una función que obliga a evolucionar, ya que la adopción de la nube de manera muy rápida obliga a las organizaciones a revisar sus políticas de gestión de identidades y control de acceso y actualizarlas de tal manera que sean capaces de lidiar con las diferencias que introducen los entornos de nube. Esto es una fuente de oportunidades y de cambios.

A alto nivel, la migración a la nube es una oportunidad para implementar nuevas infraestructuras y procesos usando arquitecturas y estándares modernos. Ha habido grandes avances en la gestión de identidades y control de acceso a lo largo de los años, aunque todavía muchas organizaciones solo han podido implementarlos en unos casos de uso limitados debido al presupuesto limitado o restricciones de arquitecturas obsoletas. La adopción de la computación en la nube ya sea un proyecto pequeño o la migración entera de un centro de proceso de datos, significa crear nuevos sistemas sobre nuevas infraestructuras que, normalmente, han sido diseñadas usando las últimas técnicas en gestión de identidades y control de acceso.

Estos cambios vienen con nuevos retos. Migrar a una federación con múltiples partes internas y externas involucradas puede ser complejo y difícil de gestionar debido a todas las variables involucradas. Determinar e imponer atributos y asignación de derechos entre sistemas y tecnologías muy dispares trae problemas técnicos y de procesos. Incluso las decisiones fundamentales a nivel de arquitectura pueden verse dificultadas por la disparidad en el soporte entre proveedores de nube y plataformas.

La gestión de identidades y control de acceso abarca todos los dominios de este documento. Esta sección comienza con una revisión rápida de la terminología fundamental con la que no todos los lectores pueden estar familiarizados para, a continuación, profundizar en los impactos de la nube en la identidad y luego en el control de acceso y su asignación.

12.1 Visión general

La gestión de identidades y el control de acceso es un área extensa con su propia terminología que puede ser difícil para aquellos que no son especialistas en este dominio, ya que hay algunos términos que tienen distintos significados en diferentes contextos (y que son usados fuera de la gestión de identidades y el control de acceso). Incluso el término “gestión de identidades y control de acceso” no es universal y frecuentemente se utiliza el término gestión de identidades (*IdM* por sus siglas en inglés).

Gartner define la Gestión de Identidades y Control de Accesos como “la disciplina en seguridad que habilita a las diferentes identidades acceder a los recursos adecuados en el momento oportuno y por la razón necesaria”. Antes de que entremos en detalles, presentamos el glosario de términos más relevantes para la discusión que nos ocupa en la computación en la nube.

- *Entidad*: la persona o “cosa” que tendrá una identidad, puede ser una persona, un sistema, un dispositivo o una aplicación.
- *Identidad*: la única representación de una entidad en un espacio de nombres. Una entidad puede tener múltiples identidades digitales, como una persona puede tener una identidad para el trabajo (o incluso múltiples identidades dependiendo del sistema) una identidad en las redes sociales y una identidad personal. Por ejemplo, si usted tiene una única entrada en un único servicio de directorio entonces esa es su identidad.
- *Identificador*: el elemento por el cual una identidad puede ser acreditada. Para identidades digitales suele ser un *token* criptográfico, en el mundo real puede ser su pasaporte.
- *Atributos*: propiedades de una identidad. Los atributos pueden ser relativamente estáticos (como una unidad organizativa) o especialmente dinámicos: dirección IP, dispositivos que están siendo usados, si el usuario se autentica con doble factor de autenticación (*MFA* por sus siglas en inglés), localización etc.
- *Personalidad*: la representación de una identidad con atributos que definen el contexto. Por ejemplo, un desarrollador que comienza a trabajar y se conecta a un entorno de nube como desarrollador de un proyecto particular. La identidad es todavía el individuo, y la personalidad es el individuo en contexto de ese proyecto.
- *Rol*: las identidades pueden tener múltiples roles que indican el contexto. ‘Rol’ es un término confuso y usado abusivamente que se usa en diferentes maneras. Para nuestros propósitos pensaremos en él como personalidad o como un subconjunto de personalidades. Por ejemplo, un desarrollador concreto para un proyecto específico puede tener diferentes roles, como “administrador” o “desarrollador”, los cuales pueden ser usados para la toma de decisiones.
- *Autenticación*: el proceso de acreditar una identidad. Cuando accede a un sistema utiliza un usuario (el identificador) y una contraseña (un atributo que se utiliza como factor de autenticación). También se conoce como ‘*Authn*’.
- *Multi-factor de autenticación (MFA por sus siglas en inglés)*: uso de múltiples factores durante la autenticación. Las opciones más frecuentes incluyen contraseñas de un solo uso generados por un dispositivo físico o virtual (OTP), validación fuera de banda a través de un OTP enviado vía mensaje de texto, o confirmación de un dispositivo móvil, biométrico o *token* que requiera conexión.

- *Control de acceso*: restringir el acceso a un recurso. La gestión de acceso es el proceso de gestionar los accesos a los recursos.
- *Autorización*: permitir el acceso a algo (por ejemplo una función o datos). También se conoce como '*Authz*'.
- *Asignación de derechos*: asociar una identidad (incluyendo roles, personalidad y atributos) a una regla de autorización. La asignación de derechos define lo que se está autorizado a hacer, y se documenta en una matriz de acceso.
- *Gestión de identidades federada*: el proceso de mantener una misma identidad en diferentes sistemas u organizaciones. Es la herramienta principal para habilitar acceso único (*Single Sign On*, *SSO*) y es el núcleo de la gestión de identidades y control de acceso en la computación en la nube.
- *Fuente autorizada*: el origen de una identidad, como el servicio de directorio que gestiona las identidades de los empleados.
- *Proveedor de identidades*: el origen de una identidad en la federación. El proveedor de identidades no es siempre una fuente autorizada, pero puede apoyarse en ellas, especialmente si es un intermediario en el proceso.
- *Entidad que confía*: el sistema que confía en una acreditación de identidad por parte de un proveedor de identidades

Hay algunos términos adicionales que serán tratados en las próximas secciones, incluyendo el estándar principal de gestión de identidades y control de acceso. También, aunque este dominio puede parecer centrado en nube pública, los mismos principios se extienden a nubes privadas. El alcance de los mismos se reduce ya que la organización puede tener más control sobre todo el proceso.

12.1.1 Estándares de gestión de identidades y control de acceso para computación en la nube

Hay varios estándares para la gestión de identidades y el control de acceso que pueden ser utilizados en computación en la nube. Independientemente de su diversidad la industria se basa en un conjunto clave de ellos, muy frecuentes en los despliegues y que están soportados por la gran mayoría de los proveedores. También existen estándares muy prometedores pero que no están lo suficientemente extendidos. Esta lista no refleja ninguna preferencia particular y no incluye todas las opciones, pero es bastante representativa de las tecnologías más aceptadas por los diferentes proveedores:

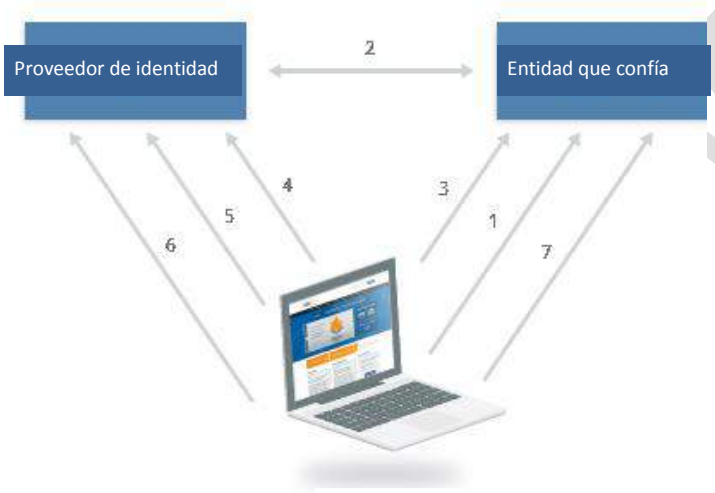
- *Security Assertion Markup Language (SAML)* 2.0 es un estándar de OASIS para sistemas federados de gestión de identidades que proporciona autenticación y autorización. Utiliza XML para hacer aseveraciones entre un proveedor de servicio de identidad y un usuario del mismo. Dichas aseveraciones pueden ser sobre la autenticación, los atributos o la autorización. *SAML* está muy extendido y usado en herramientas empresariales y proveedores de nube, pero puede ser complejo configurarlo desde cero.
- *Oauth* es un estándar IETF para autorización que está muy extendido en servicios web (incluyendo servicios de usuario). *Oauth* está diseñado para funcionar sobre HTTP, su

versión actual es 2.0 y no es compatible con la versión 1.0. Para añadir un poco más de confusión, *Oauth* 2.0 es más un marco de referencia y es menos rígido que *Oauth* 1.0 lo que significa que las implementaciones pueden no ser compatibles entre sí. Normalmente se utiliza para delegar el control de acceso/autorización entre servicios.

- *OpenID* es un estándar para autenticación federada que está ampliamente soportado por servicios web. Está basado en HTTP con *URL*s usadas para identificar el proveedor de servicio de identidad y el usuario o la identidad (por ejemplo identity.identityprovider.com). La versión actual es *OpenID Connect* 1.0 y es muy común su uso en servicios de usuario.

Hay otros dos estándares que no son tan frecuentes, pero pueden ser útiles en computación en la nube:

- *eXtensible Access Control Markup Language* (*XACML*) es un estándar para definir reglas de control de acceso/autorizaciones basadas en atributos. Es un lenguaje para definir políticas de acceso en un punto de decisión de políticas y pasar los resultados a un punto de imposición de políticas. Puede ser usado con *SAML* y con *Oauth* ya que resuelve diferentes partes del problema, i.e. decidir qué está autorizada a hacer una entidad con un conjunto de atributos, en contraposición a gestionar accesos o delegaciones de autoridad.
- Sistemas para gestión de identidades entre dominios (SCIM por sus siglas en inglés) es un estándar para intercambiar información sobre identidades entre diferentes dominios. Puede ser usado para provisionar y borrar cuentas en sistemas externos, también puede ser usado para intercambio de información para los atributos.



1. El usuario envía su *URL* de *OpenID*
2. El proveedor de identidad y la identidad que confía fijan un secreto compartido.
3. El navegador es redirigido para obtener el *token* del proveedor de identidad.
4. Se pide al proveedor de identidad un *token* para el sitio que quiere ser accedido
5. Se autentica si es necesario
6. El *token* se envía al navegador
7. El *token* se presenta a la entidad que lo solicitó

Cómo funciona la gestión de identidades federada: la federación necesita un proveedor de identidades que toma decisiones para un tercero después de haber establecido una relación de confianza entre ambos. Se fundamenta en una serie de operaciones criptográficas para establecer la relación de confianza y el intercambio de credenciales. Por ejemplo, un usuario accediendo a su red de trabajo, que alberga un servicio de directorio para diferentes cuentas. Ese usuario abre, en un navegador, una conexión a una aplicación *SaaS*. En lugar de hacer *login*, hay una serie de operaciones entre bambalinas, donde el proveedor de identidades (el servicio de directorio interno) garantiza la identidad del usuario, incluyendo que está

autenticado, y cualquier atributo necesario. La aplicación *SaaS* confía en dichas aseveraciones y permite acceder al usuario sin necesidad de introducir nuevas credenciales. De hecho, la aplicación *SaaS* no tiene ni usuario ni credenciales para ese usuario concreto, sino que redirige la decisión de autenticación al proveedor de identidades para garantizar la autenticación. Desde el punto de vista del usuario, él simplemente va a la dirección web de la aplicación *SaaS* y accede, asumiendo siempre que está autenticado contra el servicio de directorio interno.

Esto no implica que no existan otras técnicas o estándares usados en computación en la nube para la identificación, la autenticación y la autorización. La gran mayoría de los proveedores de nube, especialmente los *SaaS*, tienen sus propios sistemas de gestión de identidades y control de acceso que pueden no usar ninguno de estos estándares o pueden estar conectados a una organización usando estos estándares. Por ejemplo, la firma de peticiones HTTP es usada muy frecuentemente para autenticar *REST APIs* y las decisiones de autorización son gestionadas por políticas internas del proveedor de nube. La firma de peticiones puede aceptar *SSO* a través de *SAML*, el *API* puede estar basado en OAuth o incluso usar su propio mecanismo de *tokens*. Muchos proveedores empresariales de nube ofrecen, de alguna manera, soporte para entornos federados.

Los protocolos de identidad y los estándares no representan una solución completa en sí mismos, pero son un medio para llegar al fin perseguido.

Los conceptos esenciales a la hora de elegir un protocolo de identidad son:

- Ningún protocolo es la piedra filosofal para resolver todos los problemas de la identidad y el control de acceso.
- Los protocolos de identidad deben ser analizados en el contexto de sus casos de uso. Por ejemplo, navegadores basados *SSO*, claves *API* o autenticación móvil-a-la-nube pueden cada una llevar a las compañías a usar diferentes soluciones.
- La principal suposición en operaciones debería ser que la identidad es un perímetro en sí misma, como por ejemplo una DMZ. Debido a esto, cada protocolo de identidad debe ser seleccionado y diseñado desde el punto de vista de qué puede transitar por territorio peligroso y resistir ataques maliciosos.

12.1.2 Gestión de usuarios e identidades en computación en la nube

La parte de “identidad” en la gestión de identidades está centrada en los procesos y tecnologías para registrar, aprovisionar, propagar, gestionar y borrar identidades. Gestionar estas identidades y provisionarlas en los diferentes sistemas son problemas que la seguridad de la información lleva afrontando décadas. No hace mucho tiempo los administradores IT necesitaban crear las diferentes identidades de manera individual en cada uno de los sistemas internos. Incluso hoy, con los servicios de directorio centralizados y una gran variedad de estándares, tener una configuración *SSO* real para todo es relativamente raro, los usuarios todavía gestionan una serie de credenciales, aunque este número es menor que en el pasado.

Nota sobre el alcance: las descripciones en esta sección son genéricas pero presentan sesgo hacia la gestión de usuarios. Los mismos principios aplican a identidades para servicios, dispositivos, servidores, código y otras entidades, pero los procesos y detalles en torno a ellos

pueden ser más complejos y están relacionados de manera más estrecha con la seguridad de aplicaciones y arquitecturas. Este dominio sólo incluye una pequeña discusión de todos los problemas internos de gestión de identidades para proveedores de nube, por la misma razón anterior. Esto no implica que éstas últimas áreas sean menos importantes, en muchos casos lo son más, pero introducen un grado de complejidad que no puede ser tratado de manera completa en esta guía, debido a las restricciones de alcance de la misma.

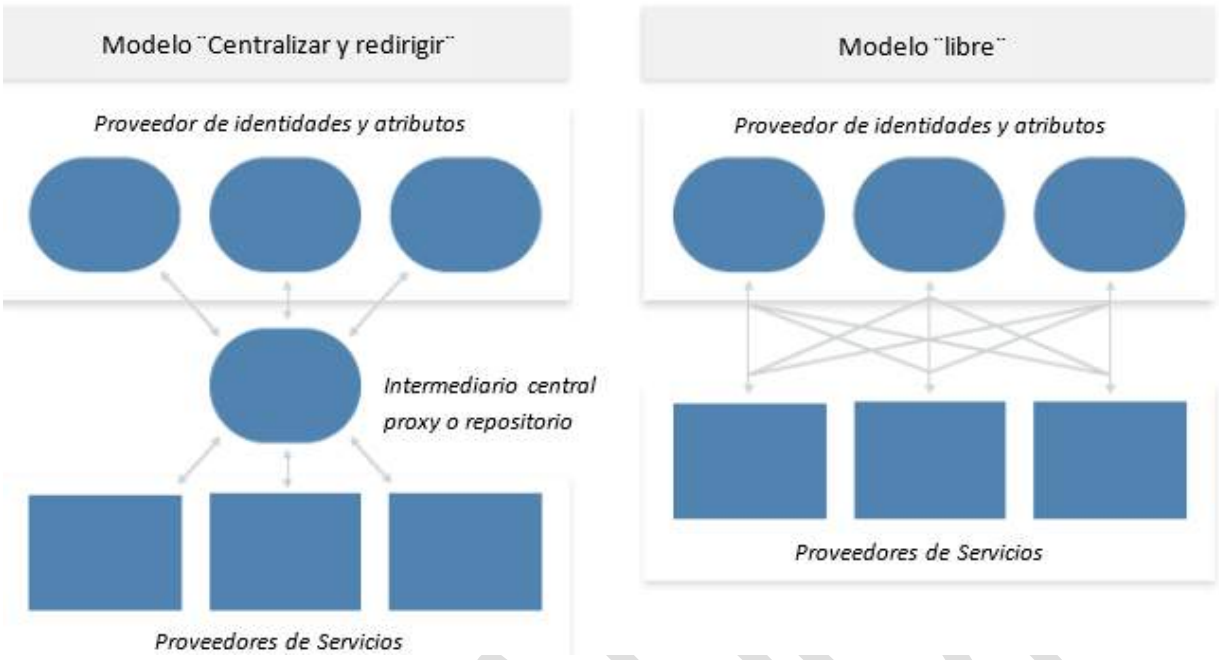
Los proveedores de nube y los usuarios de nube necesitan comenzar con la decisión fundamental de cómo gestionar las identidades:

- Los proveedores de nube casi siempre necesitan soportar identidades internas, identificadores y atributos para usuarios que acceden directamente al servicio, al mismo tiempo que dan soporte a federaciones para que las diferentes organizaciones no tengan que aprovisionar y administrar manualmente cada usuario en los sistemas del proveedor de nube y emitir a cada uno credenciales diferentes.
- Los usuarios de nube necesitan decidir si quieren gestionar sus identidades y que modelos de arquitectura y tecnologías quieren soportar para integrarse con los proveedores de nube.

Como usuario de nube, puede acceder a un proveedor de nube y crear todas sus identidades en los sistemas del proveedor. Esto no es escalable para la mayoría de las organizaciones, por lo que muchas de ellas eligen el modelo de federación. Nótese que puede haber excepciones donde tenga sentido mantener todas o solo algunas identidades aisladas del proveedor de nube, como por ejemplo las cuentas de administrador de *backup* para ayudar a depurar problemas con la conexión en la federación.

Cuando se usa una federación, el usuario de la nube necesita determinar la fuente de confianza que mantiene las identidades que serán parte de la federación. Normalmente es un servicio de directorio interno. La siguiente decisión es si usar directamente la fuente de confianza como proveedor de identidades, usar otra fuente que se aprovisione de los usuarios de la fuente de confianza (como por ejemplo un directorio aprovisionado por un sistema de recursos humanos) o integrar un *intermediario de identidades (identity broker)*.

Estas son dos posibles arquitecturas:



Centralizar y dirigir vs modelo libre

- *Modelo libre*: los proveedores de identidad internos (normalmente servicios de directorio) conectan directamente con los proveedores de nube.
- *Centralizar y redirigir*: los proveedores de identidad internos se comunican con un intermediario de identidades o repositorio que sirve como el proveedor de identidades para la federación con proveedores de nube.

Federar directamente los proveedores de identidad internos en el modelo libre presenta los siguientes problemas:

- El directorio necesita acceso a internet. Esto puede ser un problema, dependiendo de la topología existente, o puede violar políticas de seguridad.
- Puede requerir que los usuarios se conecten vía *VPN* a la red corporativa antes de acceder al servicio de nube.
- Dependiendo del servicio de directorio existente, y especialmente si existen múltiples servicios de directorio en diferentes silos organizativos, federar con un proveedor de servicio externo puede ser complejo y presentar dificultades técnicas.

Intermediario de identidades: gestionan la federación entre los proveedores de identidad y las entidades que confían en dichos proveedores (quienes no tienen por qué ser siempre un servicio de nube). Pueden estar en el perímetro de red o incluso en la nube para habilitar web-*SSO*.

Los proveedores de identidad no tienen por qué ser internos, muchos proveedores de nube proporcionan servicios de directorios basados en la nube que soportan federación interna y con otros proveedores de servicios. Por ejemplo, arquitecturas más complejas pueden sincronizar o federar una parte de las identidades de una organización en un servicio de directorio interno a

través de un intermediario de identidades y después a un directorio almacenado en la nube que sirva como proveedor de identidades para la conectividad con otras federaciones.

Después de determinar el modelo a gran escala, todavía hay procesos y decisiones de arquitectura que son necesarias en cualquier implementación:

- Cómo gestionar identidades para aplicaciones, sistemas, dispositivos y otros servicios. Se pueden mantener los mismos modelos y estándares o decidir tomar una aproximación diferente dentro de los casos de usos de nube y aplicaciones. Por ejemplo, las descripciones realizadas más arriba se refieren a usuarios accediendo a servicios, pero puede ser que no apliquen por igual a servicios que se comunican con otros servicios, o para diferentes componentes dentro de un caso de uso *IaaS*.
- Definir el proceso de aprovisionamiento de identidades y cómo integrarlo en los casos de uso de nube. Puede haber también múltiples procesos de aprovisionamiento para diferentes casos de uso, aunque el objetivo debería ser tener un proceso lo más uniforme posible.
    - Si la organización tiene ya un proceso de aprovisionamiento que resulta efectivo para sus infraestructuras tradicionales debería ser extendido idealmente a los casos de usos de nube. Sin embargo, si los procesos internos existentes son problemáticos entonces la organización debería aprovechar la migración a la nube como una oportunidad para redefinir el proceso de manera más efectiva.
- Aprovisionar y soportar proveedores de nube y casos de uso de manera individual. Debería existir un procedimiento formal para añadir nuevos proveedores dentro de la infraestructura de gestión de identidades y control de acceso. Esto incluye el procedimiento de establecer cualquier conexión para una federación, así como:
    - Relacionar los atributos (incluido los roles) entre el proveedor de servicio y la entidad que confía en sus decisiones.
    - Habilitar la monitorización/acceso necesario, incluida la monitorización de la seguridad relativa a la identidad, como análisis de comportamiento.
    - Construir una matriz de asignación de derechos (explicada en más detalle en la próxima sección).
    - Documentar los escenarios de pérdida de servicio y recuperación en los casos en los que hay un fallo técnico de cualquier federación u otras técnicas usadas para establecer la relación entre las partes.
    - Asegurar que los diferentes planes de recuperación ante potenciales suplantaciones de identidades, incluso de cuentas privilegiadas están implementados.
- Implementar procedimientos de borrado o de cambios de asignación de derechos para las identidades y los proveedores de nube. En un entorno de federación se requieren acciones en ambos extremos de la federación.

Por último, los proveedores de nube necesitan determinar qué estándares de gestión de identidades quieren proporcionar. Algunos proveedores proporcionan sólo federación mientras que otros proporcionan múltiples estándares de gestión de identidades y control de acceso junto con su propia gestión de usuarios/cuentas internas. Los proveedores que ofrecen

servicios a entornos empresariales necesitarán proporcionar federación de identidades y muy probablemente *SAML*.

12.1.3 Autenticación y credenciales

La autenticación es el proceso de verificar o confirmar una identidad. En seguridad de la información la autenticación se refiere normalmente al acto de acceder por parte de un usuario, pero también se refiere al hecho de que, en cualquier momento, una entidad verifique quién es y que asuma una identidad. La autenticación es responsabilidad del proveedor de identidades.

El mayor impacto de la computación en la nube para la autenticación es una mayor necesidad de *autenticación robusta* usando *múltiples factores*. Esto es así por dos razones:

- El amplio acceso en red implica que los servicios de nube están siempre accesibles a través de la red y normalmente desde internet. La pérdida de credenciales puede derivar fácilmente en una suplantación de una cuenta por un atacante, ya que los ataques no están restringidos a la red interna.
- El mayor uso de la federación de *SSO* implica que un conjunto de credenciales puede, potencialmente, comprometer un mayor número de servicios de nube.

El factor de autenticación múltiple ofrece una de las mejores opciones para reducir la suplantación de cuentas. No es la panacea, pero confiar sólo en un factor de autenticación (contraseña) para los servicios de nube conlleva un riesgo muy alto. Cuando se usa múltiples factores con federación, el proveedor de identidades puede y debería enviar el estado de dichos factores como un atributo a la entidad que confía en sus decisiones.

Hay múltiples opciones para implementar factor de autenticación múltiple incluyendo

- *Token hardware*: son dispositivos físicos que generan una contraseña de un solo uso para ser usados de manera manual o utilizados en un lector. Estos son la mejor opción cuando se necesita el máximo nivel de seguridad.
- *Token software*: funcionan de manera similar a los *tokens hardware,* pero son aplicaciones que se ejecutan en un móvil o en un ordenador. Los *tokens* software son también una excelente opción, pero pueden ser comprometidos si el dispositivo del usuario es comprometido también. Esto debe ser considerado en cualquier análisis de riesgos.
- *Contraseñas fuera de banda*: son texto u otros mensajes enviados al teléfono del usuario (normalmente) y son usados como cualquier otra contraseña de un solo uso generado por un *token*. Aunque también es una buena opción cualquier análisis de amenazas debe considerar la intercepción del mensaje, especialmente con SMS.
- La *biometría* está creciendo como una opción, gracias a que los lectores biométricos están disponibles en teléfonos móviles, normalmente. Para los servicios de nube, la biometría es una protección local que no envía información biométrica al proveedor de nube, sino que es un atributo que puede ser enviado al proveedor. Por todo esto la seguridad y la propiedad del dispositivo local tiene que ser considerada.

Para clientes, *FIDO* es un estándar que puede agilizar la autenticación fuerte para los usuarios mientras que reduce los desacuerdos.

12.1.4 Asignación de derechos y control de acceso

Los términos *asignación de derechos*, *autorización* y *control de acceso* se solapan hasta cierto punto y también se pueden definir de manera distinta según el contexto. Aunque fueron definidas con anterioridad en esta sección, presentamos una revisión rápida.

Autorización es otorgar permisos para hacer algo - acceso a un archivo en red o realizar alguna función como llamar a una *API* de un recurso.

Control de acceso es permitir o denegar la expresión de esa autorización, por lo que incluye aspectos como asegurar que el usuario está autenticado antes de permitir el acceso.

La *asignación de derechos* relaciona identidades a autorizaciones y cualquier atributo requerido (por ejemplo, el usuario x está autorizado a acceder al recurso y cuando el atributo z tiene un valor determinado). Normalmente nos referimos a una relación de esas asignaciones de derechos como una matriz de asignación de derechos. La asignación de derechos es, frecuentemente, codificada como políticas para la distribución y la imposición.

Esto es solo una definición de estos términos y puede verlos usados en otros documentos de manera diferente. Nosotros usamos también el término gestión de acceso como la “A” en el acrónimo *IAM* y se refiere a todo el proceso de definir, propagar e imponer las autorizaciones.

Ejemplo de matriz de asignación de derechos

Asignación de derechos	Super-admin	Admin del servicio 1	Admin del servicio 2	Dev	Auditor de seguridad	Administrador de seguridad
Lista de servicio 1	X	X		X	X	X
Lista de servicio 2	X		X	X	X	X
Servicio 1 Modificar la red	X	X		X		X
Servicio 2 Modificar reglas seguridad	X	X				X
Leer logs de auditoria	X				X	X

Aquí tenemos un ejemplo de nube real. El proveedor de nube dispone de una *API* para lanzar nuevas máquinas. Esa *API* tiene su correspondiente autorización para permitir lanzar nuevas máquinas, con opciones adicionales de autorización para determinar en qué red dicho usuario puede lanzar la máquina virtual. El administrador de la nube crea una asignación de derechos que dice que los usuarios en el grupo de desarrolladores pueden lanzar máquinas virtuales sólo

en sus proyectos y sólo si están autenticados usando factor de autenticación múltiple. El grupo y el uso del factor de autenticación múltiple son atributos de la identidad del usuario. Esa asignación de derechos está escrita como una política que está cargada en el sistema del proveedor de nube para su imposición.

La nube impacta la asignación de derechos, autorizaciones y la gestión de accesos de múltiples maneras:

- Los proveedores de nube y plataforma, como cualquier otra tecnología, tendrán su propio conjunto de posibles autorizaciones específicas para ellos. Salvo que el proveedor proporcione *XACML* (poco frecuente hoy en día) el usuario de la nube necesitará configurar la asignación de derechos dentro del entorno de la nube directamente.
- El proveedor de la nube es responsable de la imposición de las autorizaciones y el control de acceso.
- El usuario de la nube es responsable de definir la asignación de derechos y configurarlos de manera adecuada en la plataforma en la nube.
- Las plataformas de nube suelen tener un mayor soporte para el modelo de *control de acceso basado en atributos* (*ABAC* por sus siglas en inglés) para la gestión de identidades y el control de acceso, que ofrece mayor flexibilidad y seguridad que el modelo de *control de acceso basado en roles* (*RBAC* por sus siglas en inglés). *RBAC* es el modelo tradicional para imponer las autorizaciones y descansa en lo que es frecuentemente un único atributo (un rol definido). ABAC permite mayor granularidad y decisiones dependientes de contexto incorporando múltiples atributos como roles, localizaciones, métodos de autenticación y otros.
    - *ABAC* es el modelo preferido para la gestión de acceso basada en la nube.
- Cuando usamos federación, el usuario de la nube es responsable de relacionar los atributos, incluyendo los roles y grupos, en el proveedor de nube y asegurar que se envían de manera adecuada durante la autenticación.
- Los proveedores de nube son responsables de permitir definiciones granulares de atributos y autorizaciones para habilitar *ABAC* y una seguridad efectiva para los usuarios de la nube.

12.1.5 Gestión de usuarios privilegiados

En términos de control de riesgos, pocas cosas son más fundamentales que la gestión de usuarios privilegiados. Los requisitos mencionados anteriormente de autenticación robusta deben ser considerados en mayor medida para todos los usuarios privilegiados. De manera adicional, el registro de cuentas y de las sesiones deberían ser implementados para garantizar la responsabilidad y la visibilidad de los usuarios privilegiados.

En algunos casos, será beneficioso para un usuario privilegiado iniciar sesión a través de un sistema distinto estrechamente controlado utilizando mayores niveles de garantías para el control de credenciales, certificados digitales, puntos de acceso físicamente y lógicamente separados, y/o servidores de salto.

12.2 Recomendaciones

- Las organizaciones deberían desarrollar un plan formal y entendible junto a procesos para gestionar identidades y autorizaciones en los servicios de nube.
- Cuando se acceda a proveedores de nube externos, se debe usar la técnica de federación, si es posible, para extender la gestión de identidades ya existente. Hay que intentar minimizar los silos de identidades en los proveedores de nube que no estén asociados a identidades internas.
- Considerar el uso de intermediarios de identidades cuando aplique.
- Los usuarios de la nube son responsables de mantener el proveedor de identidad y definir las identidades y los atributos.
    - Deben estar basados en una fuente autorizada de datos.
    - Las organizaciones distribuidas deberían considerar el uso de servicios de directorio alojados en la nube cuando las opciones en la propia infraestructura no sean viables o no cumplan con los requerimientos.
- Los usuarios de la nube deberían preferir factor de autenticación múltiple para todas las cuentas de nube externas y enviar su estado como un atributo cuando se use la autenticación de tipo federación.
- Las identidades privilegiadas deberían usar siempre un factor de autenticación múltiple.
- Desarrollar una matriz de asignación de derechos para cada proveedor de nube y proyecto, con énfasis en el acceso a la meta-estructura y/o la capa de gestión.
- Traducir la matriz de asignación de derechos en políticas técnicas cuando esté soportado por el proveedor de servicio o plataforma.
- Preferir control de acceso basado en atributos al control de acceso basado en roles en la computación en la nube.
- Los proveedores de nube deberían ofrecer identidades internas o federadas usando estándares abiertos.
- No hay protocolos mágicos: seleccione los casos de uso y las restricciones primero y luego busque el protocolo adecuado.

Dominio 13 Seguridad como Servicio

13.0 Introducción

Aunque la mayor parte de esta guía se centra en proteger las plataformas y despliegues de nube, este dominio cambia la orientación para cubrir los servicios de seguridad desde la nube. Estos servicios, que normalmente son *SaaS* o *PaaS*, no son necesariamente utilizados de modo exclusivo para proteger despliegues de nube; es más probable que se utilicen para proteger instalaciones tradicionales en las propias instalaciones.

En la seguridad como servicio (*SecaaS*), los proveedores ofrecen capacidades de seguridad como un servicio en la nube. Esto incluye tanto proveedores *SecaaS* dedicados, como características empaquetadas de seguridad de proveedores generales de servicios en la nube. La seguridad como servicio abarca una gama muy amplia de tecnologías, pero debe cumplir los siguientes criterios:

- *SecaaS* incluye seguridad de productos o servicios que se entregan como un servicio en la nube.
- Para ser considerado *SecaaS*, los servicios deben cumplir con las características esenciales de *NIST* para la computación en la nube, tal como se definen en el Dominio 1.

Esta sección destaca algunas de las categorías más comunes en el mercado, pero *SecaaS* evoluciona constantemente y las descripciones y la siguiente lista no deben considerarse como canónicas. Hay ejemplos y servicios no cubiertos en este documento, y entran más al mercado de manera constante.

13.1 Visión general

13.1.1 Beneficios potenciales y preocupaciones de *SecaaS*

Antes de profundizar en los detalles de las diferentes categorías significativas de *SecaaS* es importante entender cómo *SecaaS* es diferente tanto de la seguridad local como de la seguridad auto administrada. Para ello, tenga en cuenta los posibles beneficios y consecuencias.

13.1.1.1 Beneficios potenciales

- *Ventajas de la computación en la nube.* Las ventajas del potencial normal de la computación en la nube -tales como reducción de gastos de capital, agilidad, redundancia, alta disponibilidad y flexibilidad- son todas aplicables a *SecaaS*. Como con cualquier otro proveedor de la nube, la magnitud de estos beneficios depende de los precios, la ejecución y la capacidad del proveedor de seguridad.

- *Personal y experiencia.* Muchas organizaciones tienen dificultades para contratar, capacitar y retener a profesionales de seguridad en todos los ámbitos relevantes de experiencia. Esto se agrava debido a las limitaciones de los mercados locales, los altos costos de los especialistas, y el equilibrar las necesidades del día a día con la alta tasa de innovación de los atacantes. Como tal, los proveedores *SecaaS* traen como beneficio un amplio dominio de conocimientos e investigación que puede ser inalcanzable para muchas organizaciones que no están exclusivamente centradas en la seguridad o en un dominio específico de la seguridad.
- *Intercambio de inteligencia.* Los proveedores *SecaaS* protegen a varios clientes al mismo tiempo y tienen la posibilidad de compartir datos de inteligencia y datos a través de ellos. Por ejemplo, encontrar una muestra de malware en un cliente permite al proveedor inmediatamente añadirla a su plataforma defensiva, protegiendo así a todos los demás clientes. Hablando en términos prácticos esto no es una varita mágica, la eficacia variará entre categorías, pero ya que intercambio de inteligencia está integrada en el servicio, el potencial de crecimiento está allí.
- *Flexibilidad de implementación. SecaaS* puede estar mejor posicionado para la evolución de los lugares de trabajo y migraciones de nube, ya que es en sí mismo un modelo de nube nativo entregado mediante un amplio acceso a la red y elasticidad. Los servicios normalmente pueden manejar más modelos de implementación flexibles, tales como el apoyo de ubicaciones distribuidas sin la complejidad de instalaciones de hardware en múltiples sitios.
- *Aislamiento de clientes.* En algunos casos, *SecaaS* puede interceptar los ataques antes de que lleguen a la organización directamente. Por ejemplo, el filtrado de spam y cortafuegos de Aplicaciones Web basados en nube están colocados *entre* los atacantes y la organización. Pueden absorber ciertos ataques antes de que lleguen a los activos del cliente.
- *Escalamiento y costo.* El modelo en la nube provee al consumidor con un modelo "Pague a medida que crece", que también ayuda a las organizaciones a centrarse en su negocio y les permite dejar las preocupaciones en materia de seguridad a los expertos.

13.1.1.2 Problemas potenciales

- *Falta de visibilidad.* Dado que los servicios operan de forma separada del cliente, a menudo proporcionan menos visibilidad o datos en comparación con la operación propia. Es posible que el proveedor de *SecaaS* no revele detalles sobre cómo implementa su propia seguridad y gestiona su propio entorno. Dependiendo del servicio y el proveedor, eso puede generar una diferencia en las fuentes de datos y el nivel de detalle disponible para tareas como monitoreo e incidentes. Parte de la información que el cliente puede estar acostumbrado a tener puede ser diferente, tener lagunas o no estar disponible en absoluto. La evidencia real y las evidencias de cumplimiento, así como otros datos de investigación, pueden no cumplir los objetivos del cliente. Todo esto puede y debe determinarse antes de celebrar cualquier acuerdo.

- *Diferencias de regulación*. Teniendo en cuenta los requisitos normativos globales, los proveedores de *SecaaS* pueden no ser capaces de garantizar el cumplimiento en todas las jurisdicciones en las que opera una organización.
- *Manejo de datos regulados*. Los clientes también necesitarán la garantía de que cualquier información regulada que se pueda extraer como parte del escaneo de seguridad de rutina o un incidente de seguridad se maneja de acuerdo con los requisitos de cumplimiento; esto también debe cumplir con las diferencias jurisdiccionales internacionales antes mencionadas. Por ejemplo, el monitoreo de los empleados en Europa es más restrictivo que en los Estados Unidos, e incluso las prácticas básicas de monitoreo de seguridad pueden violar los derechos de los trabajadores en esa región. Del mismo modo, si un proveedor de *SecaaS* reubica sus operaciones, debido a la migración del centro de datos o al balanceo de carga, puede violar las reglamentaciones que incluyan restricciones geográficas en la residencia de datos.
- *Fuga de datos*. Al igual que con cualquier servicio o producto de computación en la nube, siempre existe la preocupación de que los datos de un usuario se filtren a otro. Este riesgo no es exclusivo de *SecaaS*, pero la naturaleza altamente confidencial de los datos de seguridad (y otros datos reglamentados potencialmente expuestos en escaneos de seguridad o incidentes) significa que los proveedores de *SecaaS* deben cumplir con los más altos estándares de aislamiento y segregación de múltiples propietarios. Los datos relacionados con la seguridad también pueden estar involucrados en litigios, investigaciones policiales y otras situaciones de descubrimiento. Los clientes quieren asegurarse de que sus datos no se expongan cuando estas situaciones involucran a otro cliente en el servicio.
- *Cambiando proveedores*. Aunque, en apariencia, cambiar de proveedor de *SecaaS* puede parecer más fácil que cambiar el hardware y el software local, las organizaciones pueden estar preocupado por estar atrapados debido a la posibilidad de perder el acceso a los datos, incluidos los datos históricos necesarios para el cumplimiento o el apoyo de la investigación.
- *Migración a SecaaS*. Para las organizaciones que tienen operaciones de seguridad existentes y soluciones de control de seguridad heredadas en sus instalaciones, la migración a *SecaaS* y el límite y la interfaz entre cualquier departamento de TI interno y los proveedores de *SecaaS* deben estar bien planificados, ejercitados y mantenidos.

13.1.2 Principales categorías de ofertas de seguridad como servicio

Hay una gran cantidad de productos y servicios que se incluyen bajo el título de Seguridad como servicio. Si bien la siguiente no es una lista canónica, describe muchas de las categorías más comunes vistas al momento de escribir este artículo.

13.1.2.1 Gestión de identidades, derechos y accesos

La identidad como servicio es un término genérico que abarca uno o varios de los servicios que pueden comprender un ecosistema de identidad, como Políticas de Puntos de Cumplimiento (*PEP-as-a-service*), Políticas de Puntos de Decisión (*PDP-as-a-service*), Políticas de Puntos de Acceso (*PAP-as-a-service*), servicios que proporcionan identidad a las entidades, servicios que proporcionan atributos (por ejemplo, autenticación de factores múltiples) y servicios que proporcionan reputación.

Una de las categorías más conocidas que se usa mucho en la seguridad de la nube es la de Agentes de Identidad Federada. Estos servicios ayudan a intermediar *IAM* entre los proveedores de identidad existentes de una organización (directorios internos u hospedados en la nube) y los diferentes servicios en la nube utilizados por la organización. Pueden proporcionar inicio de sesión único (*SSO*) basado en la web, lo que ayuda a aliviar la complejidad de conectarse a una amplia gama de servicios externos que usan diferentes configuraciones de federación.

Hay otras dos categorías comúnmente vistas en las implementaciones en la nube. Los servicios de autenticación robustos usan aplicaciones e infraestructura para simplificar la integración de varias opciones de autenticación robusta, incluidas aplicaciones de dispositivos móviles y *tokens* para *MFA*. La otra categoría aloja servidores de directorio en la nube para servir como proveedor de identidad de una organización.

13.1.2.2 Agentes de acceso a la nube y Seguridad (*CASB*, también conocido como *Cloud Security Gateways*)

Estos productos interceptan las comunicaciones que se dirigen a un servicio en la nube o se conectan directamente al servicio a través de una *API* con el fin de monitorear la actividad, aplicar políticas y detectar y/o prevenir problemas de seguridad. Se usan comúnmente para administrar los servicios *SaaS* sancionados y no autorizados de una organización. Si bien hay opciones de *CASB* en las instalaciones, a menudo también se ofrece como un servicio alojado en la nube.

Los *CASB* también pueden conectarse a herramientas locales para ayudar a una organización a detectar, evaluar y potencialmente bloquear el uso de la nube y de servicios no aprobados. Muchas de estas herramientas incluyen capacidades de calificación de riesgo para ayudar a los clientes a comprender y categorizar cientos o miles de servicios en la nube. Las calificaciones se basan en una combinación de las evaluaciones del proveedor, que pueden ponderarse y combinarse con las prioridades de la organización.

La mayoría de los proveedores también ofrecen prevención básica de pérdida de datos para los servicios en la nube cubiertos, de forma inherente o mediante la asociación e integración con otros servicios.

Dependiendo de la organización que defina "*CASB*", el término también se usa a veces para incluir Agentes de Identidad Federados. Esto puede ser confuso: aunque la combinación de las capacidades de "Gateway de Seguridad" e "Intermediario de Identidad" es posible y existe, el mercado todavía está dominado por servicios independientes para ambas capacidades.

13.1.2.3 Seguridad web (puertas de enlace en seguridad web)

La seguridad web implica protección en tiempo real, que se ofrece localmente mediante la instalación de software y/o dispositivos, o a través de la nube mediante el proxy o la redirección del tráfico web al proveedor de nube (o un híbrido de ambos). Esto proporciona una capa adicional de protección sobre la otra protección, como software antimalware para evitar que el malware ingrese a la empresa a través de actividades como la navegación web. Además, también puede aplicar reglas de política sobre tipos de acceso a la red y ventanas de tiempo cuando estén permitidas. La gestión de autorización de aplicaciones puede proporcionar un nivel extra de aplicación de seguridad granular y contextual para aplicaciones web.

13.1.2.4 Seguridad del correo electrónico

Se debe proporcionar control sobre el correo electrónico entrante y saliente, proteger a la organización de riesgos como el phishing y archivos adjuntos maliciosos, así como aplicar políticas corporativas como el uso aceptable y la prevención del spam, y proporcionar opciones de continuidad del negocio.

Además, la solución puede admitir el cifrado de correos electrónicos basado en políticas, así como la integración con varias soluciones de servidor de correo electrónico. Muchas soluciones de seguridad de correo electrónico también ofrecen características como firmas digitales que permiten la identificación y no repudio. Esta categoría incluye la gama completa de servicios, desde funciones tan sencillas como antispam hasta *gateways* de seguridad de correo electrónico completamente integrados con protección avanzada contra malware y phishing.

13.1.2.5 Evaluación de seguridad

Las evaluaciones de seguridad son auditorías de terceros o dirigidas por el cliente de los servicios en la nube o evaluaciones de los sistemas en las instalaciones a través de soluciones proporcionadas por la nube. Las evaluaciones de seguridad tradicionales para infraestructura, aplicaciones y auditorías de cumplimiento están bien definidas y respaldadas por múltiples estándares como *NIST*, *ISO y CIS*. Existe un conjunto de herramientas relativamente maduro, y se han implementado varias herramientas utilizando el modelo de despliegue de *SecaaS*. Utilizando ese modelo, los suscriptores obtienen los beneficios típicos de la computación en la nube: elasticidad variable, tiempo de configuración insignificante, baja sobrecarga de administración y pago por uso con bajas inversiones iniciales.

Hay tres categorías principales de evaluaciones de seguridad:

- Evaluaciones tradicionales de seguridad/vulnerabilidad de los activos que se implementan en la nube (por ejemplo, máquinas/instancias virtuales para parches y vulnerabilidades) o en las propias instalaciones.
- Evaluaciones de seguridad de aplicaciones, incluidas *SAST, DAST* y la gestión de *RASP*.

- Herramientas de evaluación de la plataforma en la nube que se conectan directamente con el servicio en la nube a través de una *API* para evaluar no solo los activos desplegados en la nube, sino también la configuración de la nube.

13.1.2.6 Cortafuegos de aplicaciones web

En un *WAF* basado en la nube, los clientes redirigen el tráfico (con *DNS*) a un servicio que analiza y filtra el tráfico antes de que pasen a través de la aplicación web de destino. Muchos de *WAFs* en la nube también incluyen capacidades anti-*DDoS*.

13.1.2.7 Detección y prevención de intrusiones (*IDS/IPS*)

Los sistemas de Detección/Prevención de Intrusos monitorean los patrones de comportamiento usando modelos basados en reglas, heurísticos o de comportamiento para detectar anomalías en la actividad que pueden presentar riesgos para la empresa. Con *IDS/IPS* como servicio, la información se alimenta en la plataforma administrada de un proveedor de servicios, en lugar de que el cliente sea responsable de analizar los eventos por sí mismos. Un *IDS/IPS* en la nube puede usar el hardware existente para la seguridad local, dispositivos virtuales para la nube (vea el Dominio 7 para conocer las limitaciones) o también la configuración de agentes basados en el host.

13.1.2.8 Gestión de información y eventos de seguridad (*SIEM*)

Los sistemas de Gestión de Información y Eventos de Seguridad agregan (mediante mecanismos de inserción o extracción) datos de eventos y registros de redes, aplicaciones y sistemas virtuales y reales. Esta información luego se correlaciona y analiza para proporcionar informes en tiempo real y alertas de información o eventos que pueden requerir intervención u otro tipo de respuestas. Los *SIEM* en la nube recopilan estos datos en un servicio en la nube, a diferencia de un sistema en las instalaciones administradas por el cliente.

13.1.2.9 Cifrado y gestión de claves

Estos servicios cifran datos y/o administran claves de cifrado. Pueden ser ofrecidos por servicios en la nube para respaldar el cifrado y la seguridad de los datos administrados por el cliente. Pueden estar limitados a solo proteger los activos dentro de ese proveedor específico de la nube, o pueden ser accesibles a través de múltiples proveedores (e incluso locales, a través de *API*) para una administración del cifrado más amplia. La categoría también incluye *proxies* de cifrado para *SaaS*, que interceptan el tráfico *SaaS* para cifrar datos discretos.

Sin embargo, el cifrado de datos fuera de una plataforma *SaaS* puede afectar la capacidad de la plataforma para utilizar los datos en cuestión.

13.1.2.10 Continuidad del negocio y recuperación ante desastres.

Los proveedores de servicios *BC/DR* en la nube respaldan datos de sistemas individuales, centros de datos o servicios en la nube a una plataforma en la nube en lugar de confiar en el almacenamiento local o traslado de cintas. Pueden usar una puerta de enlace local para acelerar las transferencias de datos y recuperaciones locales, y el servicio en la nube sirve como el repositorio final para los escenarios del peor caso o con fines de archivo.

13.1.2.11 Administración de seguridad

Estos servicios complementan las capacidades tradicionales de gestión de seguridad, como la protección EPP (punto final), gestión de agentes, seguridad de red, gestión de dispositivos móviles, etc. en un solo servicio en la nube. Esto reduce o elimina la necesidad de servidores de administración locales y puede ser particularmente adecuado para las organizaciones distribuidas.

13.1.2.12 Protección de denegación de servicio distribuida

Por naturaleza, la mayoría de las protecciones DDoS están basadas en la nube. Operan redireccionando el tráfico a través del servicio *DDoS* para absorber los ataques antes de que puedan afectar la propia infraestructura del cliente.

13.2 Recomendaciones

- Antes de contratar a un proveedor de *SecaaS*, asegúrese de comprender todos los requisitos específicos de seguridad para el soporte de manejo de datos (y disponibilidad), investigación y cumplimiento.
- Preste especial atención al manejo de datos regulados, como PII.
- Comprenda sus necesidades de retención de datos y seleccione un proveedor que pueda admitir fuentes de datos que no creen una situación de bloqueo.
- Asegúrese de que el servicio *SecaaS* sea compatible con sus planes actuales y futuros, tales como sus plataformas en la nube (y locales), las estaciones de trabajo y los sistemas operativos móviles que utiliza, y así sucesivamente.

Dominio 14 Tecnologías Relacionadas

14.0 Introducción

A lo largo de esta guía, nos hemos centrado en proporcionar antecedentes y las mejores prácticas para proteger directamente la computación en la nube. Como una tecnología fundacional, también hay una variedad de tecnologías relacionadas que traen sus propias preocupaciones de seguridad.

Aunque cubrir todos los usos potenciales de la nube van mucho más allá del alcance de este documento, CSA considera que es importante incluir antecedentes y recomendaciones sobre las tecnologías clave que están interrelacionadas con la nube. Algunas, como contenedores y redes definidas por software, están tan estrechamente entrelazadas que las cubrimos en otros dominios de la guía. Este dominio proporciona más detalles en tecnologías adicionales, que no encajan claramente en los dominios existentes.

Al separarlos en su propia sección, se obtiene más flexibilidad para actualizar la cobertura, agregando y eliminando tecnologías a medida que su uso cambia y surgen nuevas capacidades.

14.1 Visión general

Las tecnologías relacionadas se dividen en dos amplias categorías:

- Tecnologías que dependen casi exclusivamente de la computación en la nube para operar.

- Tecnologías que no dependen necesariamente de la nube, pero que se ven comúnmente en la nube

Esto no quiere decir que estas tecnologías *no puedan trabajar* sin la nube, solo que a menudo se las ve superpuestas o confiando en implementaciones en la nube, viéndose comúnmente que tienen implicaciones para la mayoría de los profesionales de seguridad en la nube.

La lista actual incluye:

- *Big Data*
- Internet de las Cosas (*IoT*)
- Dispositivos móviles
- Computación sin servidor

Cada una de estas tecnologías está actualmente cubierta por grupos de trabajo de investigación adicionales del Cloud Security Alliance, en múltiples proyectos y publicaciones en curso:

- Grupo de trabajo *Big Data*
- Grupo de trabajo *Internet of Things*
- Grupo de trabajo sobre Móviles

14.1.1 Big Data

Big data incluye una colección de tecnologías para trabajar con conjuntos de datos extremadamente grandes y que las herramientas tradicionales de procesamiento de datos no pueden administrar. No se trata de una tecnología única, sino que se refiere a los marcos distribuidos de recopilación, almacenamiento y procesamiento de datos.

Gartner lo define así: "*Big Data* es un gran volumen, alta velocidad y/o una gran variedad de activos de información que requieren nuevas formas de procesamiento para permitir una mejor toma de decisiones, descubrimiento de conocimiento (*insight*) y optimización de procesos".

Las "3 V" son comúnmente aceptadas como la definición central de *big data*, aunque hay muchas otras interpretaciones.

- *Gran volumen*: un gran tamaño de datos, en términos de cantidad de registros o atributos.
- *Gran velocidad*: generación rápida y procesamiento de datos, es decir, datos en tiempo real o de transmisión.
- *Gran variedad*: datos estructurados, semiestructurados o no estructurados.

La computación en la nube, debido a su elasticidad y capacidades de almacenamiento masivo, es muy a menudo donde se implementan proyectos de *big data*. *Big Data* no es exclusivo de la nube de ninguna manera, pero las tecnologías de *big data* se integran con mucha frecuencia en las aplicaciones de computación en la nube y son ofrecidas por los proveedores de la nube como *IaaS* o *PaaS*.

Hay tres componentes comunes de *Big Data*, independientemente del conjunto de herramientas específicas utilizadas:

- *Recopilación de datos distribuidos:* Mecanismos para ingerir grandes volúmenes de datos, a menudo de naturaleza de transmisión. Esto podría ser tan "liviano" como el análisis de transmisión por clic en la web y tan complejo como la imagen científica altamente distribuida o los datos del sensor. No todos los *Big Data* se basan en la recopilación de datos distribuidos o en tiempo real, pero es una tecnología central de *big data*.
- *Almacenamiento distribuido:* la capacidad de almacenar grandes conjuntos de datos en sistemas de archivos distribuidos (como *Google File System, Hadoop Distributed File System*, etc.) o bases de datos (a menudo NoSQL), que a menudo se requiere debido a las limitaciones de las tecnologías de almacenamiento no distribuidas.
- *Procesamiento distribuido:* Herramientas capaces de distribuir trabajos de procesamiento (como *map reduce, spark*, etc.) para el análisis eficaz de conjuntos de datos tan masivos y cambiantes que el procesamiento de un solo origen no puede manejarlos de forma efectiva.

14.1.1.1 Consideraciones de seguridad y privacidad

Debido a la combinación de la naturaleza altamente distribuida de las aplicaciones de big data (con recopilación, almacenamiento y procesamiento de datos distribuidos entre diversos nodos) y el gran volumen y la sensibilidad potencial de la información, la seguridad y la privacidad suelen ser de alta prioridad, pero son desafiadas por un mosaico de diferentes herramientas y plataformas.

14.1.1.2 Recolección de datos

Es probable que los mecanismos de recopilación de datos usen un almacenamiento intermedio que debe asegurarse adecuadamente. Este almacenamiento se utiliza como parte de la transferencia de datos desde la recopilación hasta el almacenamiento. Incluso si el almacenamiento primario está bien protegido, también es importante verificar el almacenamiento intermedio, que podría ser tan simple como un espacio de intercambio en un nodo de procesamiento. Por ejemplo, si la recolección se ejecuta en contenedores o máquinas virtuales, asegúrese de que el almacenamiento subyacente esté adecuadamente protegido. Los nodos de análisis/procesamiento distribuido probablemente también utilizarán alguna forma de almacenamiento intermedio que necesitará seguridad adicional. Esto podría ser, por ejemplo, el almacenamiento de volumen para instancias que ejecutan trabajos de procesamiento.

14.1.1.3 Gestión de claves

La gestión de claves para el almacenamiento puede ser complicada dependiendo de los mecanismos exactos utilizados debido a la naturaleza distribuida de los nodos. Existen técnicas para cifrar correctamente la mayoría de las capas de almacenamiento de *big data* de hoy, y estas se alinean con nuestra guía en el *Dominio 11: Seguridad y cifrado de datos*. El factor de complicación es que la administración de claves necesita manejar la distribución de claves a múltiples nodos de almacenamiento y análisis.

14.1.1.4 Capacidades de seguridad

No todas las tecnologías de *big data* tienen sólidas capacidades de seguridad. En algunos casos, las capacidades de seguridad del proveedor de nube pueden ayudar a compensar las limitaciones de la tecnología de *big data*. Ambos deben incluirse en cualquier arquitectura de seguridad y los detalles serán específicos de la combinación de tecnologías seleccionada.

14.1.1.5 Gestión de identidades y accesos

La administración de identidades y accesos probablemente ocurrirá en los niveles de herramientas de nube y de *big data* a la vez, lo que puede complicar las matrices de derechos.

14.1.1.6 *PaaS*

Muchos proveedores de la nube están expandiendo el soporte de *big data* con el *aprendizaje automático* y otras plataformas como opciones de servicio que dependen del acceso a datos empresariales. No se deben usar sin una comprensión completa de las posibles implicancias de la exposición, el cumplimiento y la privacidad de los datos. Por ejemplo, si el aprendizaje automático se ejecuta como *PaaS* dentro de la infraestructura del proveedor, donde los empleados del proveedor podrían acceder técnicamente, ¿Crea eso una exposición de cumplimiento?

Esto no significa que no deba usar los servicios, solo significa que necesita comprender las implicancias y tomar las decisiones de riesgo apropiadas. El aprendizaje automático y otros servicios de análisis no son necesariamente inseguros y no necesariamente violan los compromisos de privacidad y cumplimiento.

14.1.2 Internet de las cosas (*IoT*)

Internet de las cosas es un término general para los dispositivos informáticos no tradicionales utilizados en el mundo físico que utilizan la conectividad a Internet. Incluye todo, desde tecnología operacional habilitada para Internet (utilizada por servicios públicos como energía y agua) hasta rastreadores de fitness, bombillas conectadas, dispositivos médicos y más. Estas tecnologías se implementan cada vez más en entornos empresariales para aplicaciones tales como:

- Seguimiento digital de la cadena de suministro.
- Seguimiento digital de la logística física.
- Gestión de marketing, venta minorista y relaciones con los clientes.
- Aplicaciones conectadas de salud y estilo de vida para empleados, o entregados a los consumidores.

Un gran porcentaje de estos dispositivos se conectan a la infraestructura de computación en la nube para su procesamiento de *back-end* y almacenamiento de datos. Los principales problemas de seguridad de la nube relacionados con *IoT* incluyen:

- Asegurar la recopilación de datos y la desinfección.
- Registro, autenticación y autorización del dispositivo. Un problema común encontrado hoy es el uso de credenciales almacenadas para realizar llamadas directas de *API* al proveedor de la nube de *back-end*. Se conocen casos de atacantes que descompilan aplicaciones o software de dispositivos y luego usan esas credenciales con fines maliciosos.
- Seguridad *API* para conexiones de dispositivos a la infraestructura de la nube. Además del problema de credenciales almacenadas que acabamos de mencionar, las *API* mismas podrían decodificarse y utilizarse para ataques en la infraestructura de la nube.
- Comunicaciones cifradas. Muchos dispositivos actuales usan cifrado débil, obsoleto o inexistente, lo que pone en riesgo los datos y los dispositivos.
- Posibilidad de parchear y actualizar dispositivos para que no se conviertan en un punto de compromiso. Actualmente, es común que los dispositivos se envíen tal como están y nunca reciban actualizaciones de seguridad para sistemas operativos o aplicaciones. Esto ya ha causado incidentes de seguridad múltiples y muy publicitados, como ataques masivos de *botnets* basados en dispositivos *IoT* comprometidos.

14.1.3 Móvil

La informática móvil no es nueva ni exclusiva para la nube, pero un gran porcentaje de las aplicaciones móviles se conectan a la computación en la nube para su procesamiento de *back-end*. La nube puede ser una plataforma ideal para admitir dispositivos móviles, ya que los proveedores de la nube están geográficamente distribuidos y diseñados para los tipos de cargas de trabajo altamente dinámicas que comúnmente se experimentan con las aplicaciones móviles. Esta sección no analizará la seguridad móvil general, solo las partes que afectan a la seguridad de la nube.

Los principales problemas de seguridad para la informática móvil (en el contexto de la nube) son muy similares a *IoT*, excepto que un teléfono móvil o una tableta también es una computadora de propósito general:

- El registro, la autenticación y la autorización del dispositivo son fuentes comunes de problemas. Especialmente (nuevamente), el uso de credenciales almacenadas, y más

aún cuando el dispositivo móvil se conecta directamente a la infraestructura/*API* del proveedor de la nube. Se sabe que los atacantes descompilan aplicaciones móviles para revelar credenciales almacenadas que luego se usan para manipular o atacar directamente la infraestructura de la nube. Los datos almacenados en el dispositivo también deben protegerse con la suposición de que el usuario del dispositivo puede ser un atacante hostil.

- Las aplicaciones *APIs* también son una fuente potencial de compromiso. Los atacantes son conocidos por "*sniffear*" las conexiones *API*, en algunos casos utilizan *proxies* locales a los que redireccionan sus propios dispositivos, y luego descompilan las llamadas *API* (probablemente no cifradas) y las exploran en busca de debilidades de seguridad. La fijación/validación de certificados dentro de la aplicación del dispositivo puede ayudar a reducir este riesgo.

Para obtener recomendaciones adicionales sobre la seguridad de la computación móvil y en la nube, consulte las últimas investigaciones del Grupo de trabajo móvil de CSA.

14.1.4 Informática sin servidor

La informática sin servidor es el uso extensivo de ciertas capacidades de *PaaS* en tal grado que la totalidad o parte de una pila de aplicaciones se ejecuta en un entorno de proveedor de nube sin ningún sistema operativo administrado por el cliente, ni siquiera contenedores.

La "informática sin servidor" es un nombre poco apropiado ya que siempre hay un servidor ejecutando la carga de trabajo en algún lugar, pero esos servidores y su configuración y seguridad están completamente ocultos para el usuario de la nube. El usuario solo administra la configuración del servicio y no las pilas de hardware y software subyacentes.

La informática sin servidor incluye servicios tales como:

- Almacenamiento de objetos
- Balanceadores de carga en la nube
- Bases de datos en la nube
- Aprendizaje automático
- Colas de mensajes
- Servicios de notificación
- Entornos de ejecución de código (Estos son generalmente contenedores restringidos donde un consumidor ejecuta el código de la aplicación cargada).
- Puertas de enlace *API*
- Servidores web

Las capacidades sin servidor pueden estar profundamente integradas por el proveedor de la nube y unidas con sistemas basados en eventos e *IAM* y mensajería integrados para soportar la construcción de aplicaciones complejas sin ninguna administración de servidores, contenedores u otra infraestructura por parte de los clientes.

Desde el punto de vista de la seguridad, los problemas clave incluyen:

- Sin servidor supone una carga de seguridad mucho mayor para el proveedor de la nube. Elegir a su proveedor y comprender los SLA y capacidades de seguridad es absolutamente crítico.
- Al usar "sin servidor", el usuario de la nube no tendrá acceso a los niveles de monitoreo y registro comúnmente utilizados, como los registros del servidor o de la red. Las aplicaciones deberán integrar más registros, y los proveedores de la nube deberían

proporcionar el registro necesario para cumplir con los requisitos de seguridad y cumplimiento.

- Aunque los servicios del proveedor pueden certificarse o validarse para varios requisitos de cumplimiento, no necesariamente todos los servicios coincidirán con todas las regulaciones potenciales. Los proveedores deben mantener las asignaciones de cumplimiento actualizadas, y los clientes deben asegurarse de que solo utilicen los servicios dentro de su alcance de cumplimiento.
- Habrá altos niveles de acceso a la capa de administración del proveedor de la nube, ya que es la única forma de integrar y usar las capacidades “sin servidor”.
- “Sin servidor” puede reducir drásticamente la superficie y las rutas de ataque, y la integración de componentes “sin servidor” puede ser una excelente manera de romper los enlaces en una cadena de ataque, incluso si toda la pila de aplicaciones no es “sin servidor”.
- Cualquier evaluación de vulnerabilidad u otra prueba de seguridad debe cumplir con los términos de servicio del proveedor. Los usuarios de la nube ya no pueden probar directamente las aplicaciones, o deben probar con un alcance reducido, ya que la infraestructura del proveedor ahora está alojando todo y no puede distinguir entre las pruebas legítimas y los ataques.
- La respuesta a incidentes también puede ser complicada y requerirá necesariamente cambios en el proceso y las herramientas para administrar un incidente basado en servidores.

14.2 Recomendaciones

- Big data
  - Aproveche las capacidades del proveedor de la nube siempre que sea posible, incluso si se superponen con las capacidades de seguridad de la herramienta de datos. Esto asegura que tiene una protección adecuada dentro de la meta estructura de la nube y la pila de aplicaciones específicas.
  - Use el cifrado para el almacenamiento primario, intermedio y de respaldo para las capas de recopilación de datos y de almacenamiento de datos.
  - Incluir tanto la herramienta *Big Data* como la Administración de acceso e identidad de la plataforma en la nube en la matriz de derechos del proyecto.
  - Entender completamente los posibles beneficios y riesgos del uso de una máquina de aprendizaje en la nube o servicio analítico. Preste especial atención a las implicaciones de privacidad y cumplimiento.
    - Los proveedores de la nube deben asegurarse de que los datos del cliente no estén expuestos a empleados u otros administradores que usen controles técnicos y de proceso.
    - Los proveedores de la nube deben publicar claramente qué estándares de cumplimiento satisfacen sus servicios de análisis y de aprendizaje automático (para sus clientes).
    - Los usuarios de la nube deben considerar el uso de enmascaramiento u ofuscación de datos al considerar un servicio que no cumple con los requisitos de seguridad, privacidad o cumplimiento.
  - Seguir las mejores prácticas de seguridad de *Big Data*, incluidas las que proporciona la herramienta proveedor (o proyecto de código abierto) y Cloud Security Alliance.

- Internet de las Cosas

- Asegúrese de que los dispositivos se puedan parchear y actualizar.
- No almacene credenciales estáticas en dispositivos que podrían comprometer la aplicación en la nube o la infraestructura.
- Siga las mejores prácticas para el registro seguro del dispositivo y la autenticación en la aplicación del lado de la nube, generalmente utilizando un estándar de identidad federada.
- Cifrar las comunicaciones.
- Use una tubería de recopilación de datos segura y desinfecte los datos para evitar la explotación de aplicación en la nube o infraestructura a través de ataques a la tubería de recopilación de datos.
- Suponga que todas las solicitudes *API* son hostiles.
- Seguir la guía adicional y más detallada emitida por el Grupo de Trabajo Internet de las Cosas de CSA.

- Móvil
  - Siga las instrucciones de su proveedor de servicios de nube para autenticar y autorizar adecuadamente los dispositivos móviles al diseñar una aplicación que se conecte directamente a la infraestructura de la nube.
  - Utilice estándares de la industria, típicamente identidad federada, para conectar aplicaciones de dispositivos móviles a aplicaciones alojadas en la nube.
  - Nunca transfiera claves o credenciales sin cifrar a través de Internet.
  - Probar todas las *API* bajo la suposición de que un atacante hostil tendrá acceso autenticado y no encriptado.
    - Considere la fijación y validación de certificados dentro de las aplicaciones móviles.
    - Valide todos los datos *API* y desinfecte por seguridad.
    - Implementar la supervisión de seguridad del servidor/lado de la nube para la actividad *API* hostil.
  - Asegúrese de que todos los datos almacenados en el dispositivo estén seguros y cifrados.
    - Los datos confidenciales que podrían permitir el compromiso de la pila de aplicaciones no deberían ser almacenados localmente en el dispositivo donde un usuario hostil puede acceder potencialmente a ellos.
  - Siga las recomendaciones e investigaciones más detalladas emitidas por Grupo de Trabajo de Movilidad de CSA.

- Informática “sin servidor”
  - Los proveedores de la nube deben indicar claramente qué servicios de *PaaS* se han evaluado según los requisitos o estándares de cumplimiento.
  - Los usuarios de la nube solo deben usar servicios “sin servidor” que coincidan con sus obligaciones de cumplimiento y gobierno.
  - Considere la posibilidad de inyectar componentes “sin servidor” en pilas de aplicaciones utilizando arquitecturas que reduzcan o eliminen la superficie de ataque y/o vías de red.
  - Comprender los impactos de informática “sin servidor” en evaluaciones de seguridad y monitoreo.
    - Los usuarios de la nube necesitarán confiar más en el escaneo y registro de códigos de aplicaciones y menos en los registros de servidor y red.
  - Los usuarios de la nube deben actualizar los procesos de respuesta a incidentes para las implementaciones “sin servidor”.

- Aunque el proveedor de la nube es responsable de la seguridad por debajo del nivel de la plataforma “sin servidor”, el usuario de la nube sigue siendo responsable de la configuración y el uso correctos de los productos.