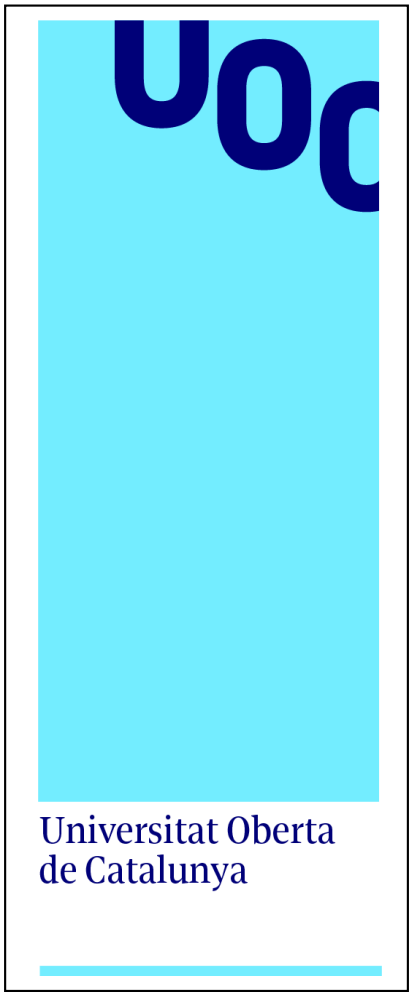
EL GUARDIÁN DE LA NUBE

Cómo proteger los datos y los servicios en la nube pública.



Máster universitario en Seguridad y Privacidad

Seguridad en la nube empresarial

Autora: Soledad Vicente Martín

Tutor de TFM: Amadeu Albós Raya
P. responsable asignatura: Víctor García Font

Junio 2023

DEDICATORIA

A mis padres, por estar siempre.
A Marci, por su apoyo incondicional en todos mis retos.
A Nora, para que siempre luche por sus sueños independiente del esfuerzo, para que sea fuerte, imparable e indestructible, para que sea feliz amando lo que hace.

Índice

Lista de figuras

1. Introducción: Plan de trabajo

1.1. Contexto y justificación del Trabajo

Nuestra forma de trabajar se ha transformado sustancialmente en los dos últimos años. Conceptos como trabajo en remoto, virtualización de puestos de trabajo, reuniones virtuales, escenarios de presencia híbrida o equipos colaborativos son ahora habituales en la mayoría de las empresas. La nube como infraestructura ha ayudado a esta transformación.

La larga lista de ventajas que ofrece la computación en la nube como la alta disponibilidad, flexibilidad, rendimiento, estabilidad, escalabilidad o reducción de costes, son un reclamo para las empresas, que acaban optando por utilizar estos servicios tanto en sus nuevas aplicaciones como en aplicaciones legacy que son migradas al nuevo paradigma.

El gran número de casos de uso y la variación de escenarios, así como la falta de expertise de los empleados o el gran volumen de información acerca de esta tecnología, hace en muchos casos que la configuración de la seguridad en los entornos Cloud de las empresas no sea la más apropiada, dejando brechas de seguridad que pueden ocasionar grandes pérdidas económicas y reputacionales a la compañía. Estamos en continua exposición, al utilizar la nube pública la superficie de ataque disponible para los cibercriminales es mayor, los *riesgos* y las *amenazas* aumentan, teniendo que poner foco en proteger nuestros activos.

Las compañías se muestran preocupadas por la seguridad en la nube lo que deja patente que la transición a la nube se percibe en muchos casos como un *riesgo* en términos de seguridad. Configurar el entorno en uso para que cumpla con las políticas de seguridad y convertirlo en un ambiente seguro aumentará la confianza de las compañías y de sus clientes.

Partiendo de este escenario, utilizando el análisis de los principales *riesgos* como base del estudio, en este TFM se analizarán y desarrollarán las opciones y las herramientas que tienen las empresas para configurar sus entornos Cloud de manera segura.

1.2. Objetivos del trabajo

El principal objetivo de este trabajo es generar una guía de buenas prácticas en el manejo de la información en proveedores de servicio y clientes de la nube, para aumentar la seguridad de sus activos.

Se apoyará en objetivos específicos tales como:

- Conocer en detalle los principales *riesgos* existentes en servicios de computación en la nube.

- Entender los requerimientos y necesidades de seguridad en la nube.

- Conocer las posibles soluciones o mitigaciones para tener un entorno de la nube más seguro.

- Conocer las herramientas y configuraciones de los servicios de la nube para garantizar, en la medida de lo posible, la seguridad.

- Conocer y contraponer los diferentes escenarios disponibles.

1.3. Enfoque y método seguido

Se utilizará una metodología hibrida, waterfall y agile, la primera para en el proyecto y la segunda en las fases de desarrollo de éste, con la idea de coger lo mejor de cada método.

- Metodología Waterfall:
  La metodología waterfall o en cascada es la que será utilizada en el proyecto. Un modelo predictivo donde se ha invertido tiempo al comienzo para entender y realizar el plan completo con sus fases, con unas fechas de entrega que no podrán ser cambiadas.

  En el roadmap del proyecto, se resalta las fechas de entrega establecidas en el programa de TFM.

- Metodología agile.
  La metodología agile se utiliza en las fases de desarrollo del proyecto, principalmente por su gran potencial en la capacidad de adaptación. Se generan auto-entregables que permiten preguntarnos si vamos por buen camino. A continuación, se muestran las pautas a seguir:

  - En cada tarea existe un auto-entregable que incrementa el contenido de la memoria y conforma la documentación para las distintas PEC.
  - Las auto-entregas se realizan en periodos cortos (sprint de 1 o 2 semanas principalmente), como se puede ver en la planificación.
  - En cada iteración se realiza un auto-entregable que incrementa la documentación del proyecto, aportando valor al producto.
  - Los requisitos del proyecto pueden cambiar a medida que se vayan ejecutando las tareas planificadas y se vayan obteniendo los auto-entregables. Esto no es un problema sino una ventaja, porque significa que se está profundizando en los temas.

Existen tres fases de desarrollo diferenciadas:

Fase de Investigación:
Si no conocemos los *riesgos* difícilmente podemos tener esperanza de saber cómo protegernos. En esta fase investigaremos y analizaremos los principales *riesgos* de los servicios en la nube. Esta será la base que se utilizará como columna vertebral para el desarrollo del proyecto y del resto de fases.

Fase de análisis:
En esta fase, partiendo de los *riesgos* identificados anteriormente, se identificarán las necesidades y las especificaciones para aumentar/garantizar la seguridad a los servicios.

Fase de Profundización:
En esta parte se tratar la evaluación de los escenarios, siempre teniendo en cuenta la información obtenida en las dos fases anteriores

Conclusiones y Memoria Final:
Partiendo del análisis de las fases anteriores, se muestran conclusiones y posibles líneas de trabajo futuras.

1.4. Impacto en sostenibilidad, ético-social y de diversidad

Este trabajo se organiza alrededor de tres dimensiones:

- Sostenibilidad

  El proyecto tiene impacto positivo.

  La innovación y el progreso tecnológico son claves para descubrir soluciones duraderas para los desafíos económicos y medioambientales. La computación en la nube se considera una de las TIC más sostenibles y eficientes, al estar basada en un conjunto de recursos informáticos compartidos. Entre otras cosas, permite reducir costes además de reducir el consumo de energía y las emisiones provocadas por los métodos tradicionales de servidores y plataformas locales. Con este proyecto se pone un granito de arena para que este progreso tecnológico en la nube pueda tener éxito, sin la seguridad apropiada la nube no sería una solución duradera en el tiempo, ya que las organizaciones no confiarían en su uso.

- Comportamiento ético y responsable

  El proyecto tiene impacto neutro.

La estructura descentralizada de las empresas proveedoras de la nube complica la legislación ya que desdibuja los límites jurisdiccionales. El proyecto no impacta directamente, pero si es relevante señalar que dependiendo de la ubicación de las instalaciones existe una jurisdicción local que se debe cumplir, incluyendo la privacidad y la seguridad de datos, este proyecto aumenta la seguridad por lo tanto ayuda indirectamente a que se haga un uso ético y responsable de la información.

- Diversidad y derechos humanos

  El proyecto tiene impacto neutro

  El enorme impacto científico producido durante las últimas décadas en los campos de la innovación y la tecnología, combinado con la globalización, fue esencialmente bueno, pero causó daños colaterales como una creciente desigualdad. Este proyecto no impacta directamente, pero si se considera importante hacer mención.

  Por otro lado, la nube se está convirtiendo en un lugar significativo de almacenamiento de información. La privacidad y la seguridad de los datos es esencial para cumplir con los derechos humanos. Este proyecto si impacta indirectamente en aumentar la seguridad de este activo.

1.5. Planificación del Trabajo

Se presenta una sencilla planificación basada en entregables. A medida que avancemos las tareas serán susceptibles de posibles cambios dependiendo de los resultados que vamos obteniendo en fases anteriores, principalmente en las fases de desarrollo.

A continuación, se detallan las tareas:

- Plan de trabajo (01/03/2023 – 14/03/2023):
  - Documentación y formación (01/03/2023 – 07/07/2023): recoger toda la información necesaria para llevar a cabo esta sección. Se utilizarán todas las fuentes disponibles y que se consideren necesarias.
  - Definición de plan (08/03/2023 – 13/07/2023): rellenar la plantilla facilitada, el punto correspondiente al plan de trabajo, detallando: contexto, objetivos, tareas, fechas, …
  - Entrega PEC1 (14/07/2023): entrega del desarrollo del plan de trabajo.

- Fase de investigación (15/03/2023 – 11/04/2023):
  Su desarrollo y ejecución será en agile, consideraremos tres auto-entregables que ayudarán a componer la PEC2, junto con los realizados en la fase anterior.

- Documentación y formación (15/03/2023 – 28/03/2023): recoger toda la información de los principales *riesgos* en la nube. Se utilizarán todas las fuentes disponibles y que se consideren necesarias.
- Principales *riesgos* (29/03/2023 – 04/04/2023): listar los principales *riesgos* en la nube, en los que consideramos profundizar.
- Analizar y desarrollar *riesgos* (05/04/2023 – 10/04/2023): analizar y documentar los *riesgos* especificados en el punto anterior.
- Entrega PEC2 (11/04/2023): entrega de la documentación realizada en la fase de investigación.

- Fase de análisis (29/03/2023 – 25/04/2023):
  Su desarrollo y ejecución será en agile, consideraremos tres auto-entregables que ayudarán a componer la PEC3, junto con los realizados en la fase anterior.

  - Documentación y formación (29/03/2023 – 11/04/2023): basándose en los *riesgos* de la fase anterior, recoger toda la información acerca de los servicios en la nube y de su configuración para asegurar su uso.
  - Especificaciones seguridad (12/04/2023 – 18/04/2023): listar las especificaciones de seguridad necesarias para mitigar los *riesgos* listados en la fase anterior.
  - Analizar y desarrollar especificaciones (19/04/2023 – 25/04/2023): analizar y documentar especificaciones, herramientas y configuraciones de los servicios para garantizar, en la medida de lo posible, la seguridad de los activos en la nube.

- Fase de Profundización (26/04/2023 – 09/05/2023):
  Su desarrollo y ejecución será en agile, se generarán tres auto-entregables que, junto con los entregables de las fases anteriores, ayudarán a componer la PEC3.

  - Documentación y formación (26/04/2023 – 02/05/2023): recoger información sobre los distintos escenarios disponibles de la nube.
  - Evaluación escenarios (03/05/2023 – 08/05/2023): contraponer los distintos escenarios y documentarlo.
  - Entrega PEC3 (09/05/2023): entrega de la documentación de la fase de análisis y la fase de profundización.

- Conclusiones y Memoria Final (10/05/2023 – 13/06/2023):

  - Conclusiones y trabajos futuros (10/05/2023 – 23/05/2023): documentar las conclusiones, el resumen de proyecto y completar aquellos apartados que, al ver el proyecto en global, consideremos ampliar para tener un mejor resultado.
  - Maquetación memoria (24/05/2023 – 12/06/2023): asegurar la calidad de la entrega de la memoria en forma. Apoyarnos en ella para generar las diapositivas que utilizaremos en la realización del video y en la defensa del TFM.

  - Entrega PEC4 (13/06/2023): entregar la memoria finalizada.

- Presentación Video (07/06/2023 – 20/06/2023):

  - Preparación Video (07/06/2023 – 13/06/2023): definir el qué y el cómo queremos presentar el proyecto en el video de presentación. Realizar pruebas de concepto y ajustar la documentación a utilizar.
  - Grabación Video (14/06/2023 – 19/06/2023): Grabar el video final.
  - Entrega grabación (20/06/2023): Entregar el video.

- Defensa TFM (20/06/2023 – 26/06/2023): preparar documentación y realizar la defensa del proyecto.

Se identifican algunos riesgos derivados del plan de trabajo definido:

- Riesgo sobreinformación: sólo es necesario escribir en google las palabras seguridad en la nube para observar toda la información que nos muestra. Diferenciar y discernir qué información es la veraz tiene a veces cierta complejidad.

  Mitigar: elegir aquellas fuentes donde podamos garantizar su fiabilidad (ejem. Gartner o proveedores la nube).

- Riesgo déficit de información: no siempre tener mucha información significa que es la adecuada. Localizar la información que buscamos puede llevarnos más tiempo del esperado, poniendo en riesgo la planificación.

  Mitigar: en el caso de no encontrar la información que consideramos necesaria podríamos ampliar fuentes: libros, videos, especialistas o contactar con proveedor/empresas.

- Riesgo dimensionamiento alcance: tanto si el alcance sobrepasa o no llega a cumplir con las expectativas, es un riesgo que corremos a lo largo de todo el proyecto.

  Mitigar: ir ajustando a medida que vamos desarrollando el proyecto, sin perder el foco en las fechas de entrega.

1.6. Breve sumario de productos obtenidos

A lo largo del proyecto se generarán dos productos:

- Análisis pormenorizado de los principales *riesgos* en computación en la nube: Descripción, detalle y análisis de las principales *amenazas* y *riesgos* que se pueden encontrar actualmente en la nube.

- Guía de buenas prácticas en Seguridad de la computación en la nube.
  Descripción, detalle y análisis de las opciones y las herramientas a utilizar para crear entornos de computación en la nube seguros.

1.7. Breve descripción de los otros capítulos de la memoria

A continuación, se muestran los capítulos que formarán parte del desarrollo del proyecto:

- *Riesgos* en la nube:
  Descripción de los principales r*iesgos* de computación en la nube.

- Seguridad en la nube:
  Descripción de los requisitos de seguridad y de las posibles herramientas y configuraciones de los servicios de la nube para aumentar la seguridad de los activos.

- Seguridad con tipos de computación en la nube:
  Contraponer los distintos posibles escenarios de la nube.

2. *Riesgos* en la nube

2.1. Contexto

Durante los últimos años hemos asistido a un enorme incremento en las capacidades de procesamiento y de almacenamiento de los sistemas informáticos, así como a un paulatino abaratamiento de los mismos, aspectos que, unidos a la mejora sustancial en la velocidad y en el acceso a las redes de ordenadores, han propiciado la aparición de nuevos paradigmas tecnológicos tales como la computación en la nube.

La computación en la nube permite nuevos modelos de negocio basados en proveer una gran variedad de servicios tecnológicos de forma descentralizada, optimizados y contratados bajo demanda, utilizando para ello la infraestructura de internet. La nube nos permite utilizar recursos de computación que de otra forma no estarían a nuestro alcance. Además de permitirnos almacenar y administrar datos en servidores remotos, nos ofrece ventajas como el pago por uso, el acceso desde cualquier lugar, la unificación de recursos y una implementación rápida, al evitarnos tener que construir o mantener infraestructuras. Actualmente existen muchos proveedores y variedad de servicios en la nube, pero, ¿tomamos las precauciones necesarias para utilizar la nube con seguridad?

Muchas empresas expresan interés en mover la mayoría de sus cargas de trabajo a la nube, creciendo de forma exponencial los servicios en ésta. La rápida implantación y el supuesto abaratamiento de los costes han conseguido que esta tecnología se acerque a las empresas para hacerlas más competitivas. Sin embargo, tener los servicios en la nube entraña una serie de *Riesgos*. Por ello, las empresas deben realizar un análisis y un estudio antes de contratar un proveedor de servicios en la nube, prestando especial atención a la parte destinada a la seguridad. La mitigación y solución de las *amenazas* y los *Riesgos*, para las tecnologías que avanzan, es más importante que nunca.

2.2. Computación en la nube

La computación en la nube es un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet. El hardware, el software y los datos se pueden ofrecer bajo demanda. El cliente puede acceder a los servicios y recursos contratos con flexibilidad de dimensionamiento y acceso. De tal manera que se abstrae de la infraestructura tecnológica necesaria para poder utilizar una aplicación, simplemente con un navegador web con conexión a la red puede tener acceso a los procesos y datos, pudiendo acceder desde cualquier lugar en cualquier momento, adaptándolo a sus necesidades.

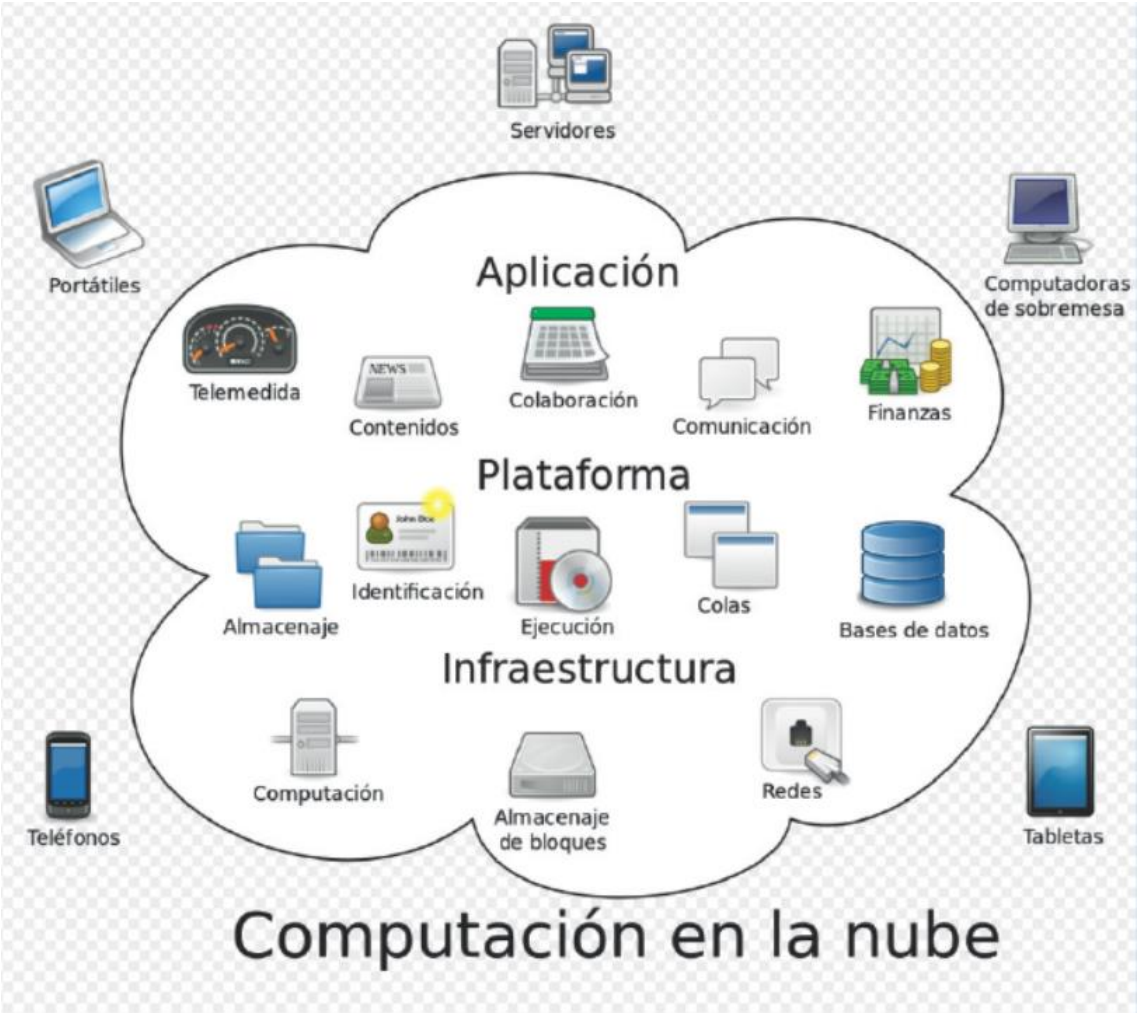


Figura 1. Computación en la nube

La posibilidad de tener sistemas y aplicaciones sin necesidad de adquirirlos, simplemente contratando un servicio, permite una versatilidad a las empresas que con el modelo clásico era impensable.

En este contexto, con el uso creciente de la computación en la nube, la importancia de su seguridad es una de las características más relevantes en el momento de utilizar o decidir migrar los recursos informáticos a este servicio. La seguridad de la información representa una prioridad para la mayoría de compañías, además de la capacidad de almacenar grandes volúmenes de datos de manera integral y confiable. Es por ello que los servicios ofrecidos en la nube, intentan proveer cada vez mejores garantías en cuanto a la confidencialidad y resistencia a posibles problemas de seguridad.

2.3. Modelos de servicio y responsabilidades de la computación en la nube

Los proveedores de la nube ofrecen diferentes modelos de servicio con el objetivo de ajustarse a las necesidades del cliente. A lo largo del proyecto se hará referencia a algunos de estos modelos. A continuación, se muestran los más populares:

- *IaaS* (Infraestructure as a Service):

Este modelo ofrece a los usuarios la virtualización, el almacenamiento, la red y los servidores a petición, siendo pago por uso. En este caso, los usuarios se encargan de las aplicaciones, los datos, el sistema operativo, el middleware y los tiempos de ejecución. El usuario no necesita tener un centro de datos local ni debe preocuparse por actualizar o mantener físicamente estos elementos.

- *PaaS* (Platform as a Service):

Plataforma como servicio (*PaaS*) es un entorno de desarrollo e implementación completo en la nube. En este caso, el proveedor aloja el hardware y el software en su propia infraestructura y ofrece la plataforma al usuario como una solución integrada, una pila de soluciones o un servicio a través de Internet.

- *SaaS* (Software as a Service):

El software como servicio (*SaaS*) es la más completa de las opciones de la computación en la nube, permite a los usuarios conectarse a aplicaciones basadas en la nube a través de Internet y usarlas. Ofrece una aplicación integral que gestiona el proveedor, a través de un explorador web. El usuario se conecta a la aplicación a través de un panel o una API.

Figura 2. Tipos servicios en la nube (Microsoft)

IaaS, *PaaS* y *SaaS* se pueden combinar para formar un entorno de computación en la nube con la infraestructura, la plataforma y las aplicaciones que necesita el cliente, sin las respectivas complicaciones y distracciones. Dependiendo del modelo elegido, el cliente estará más o menos involucrado y tendrá mayor o menor responsabilidad.

En el centro de datos local, la organización tiene toda la responsabilidad. A medida que se traslada a la nube, algunas responsabilidades se transfieren al proveedor de la nube, generando una matriz de responsabilidades compartidas que mucho tiene que ver con los distintos servicios que hemos comentado. A continuación, se muestra como ejemplo la matriz de responsabilidad compartida de uno de los proveedores de computación en la nube más popular [9].

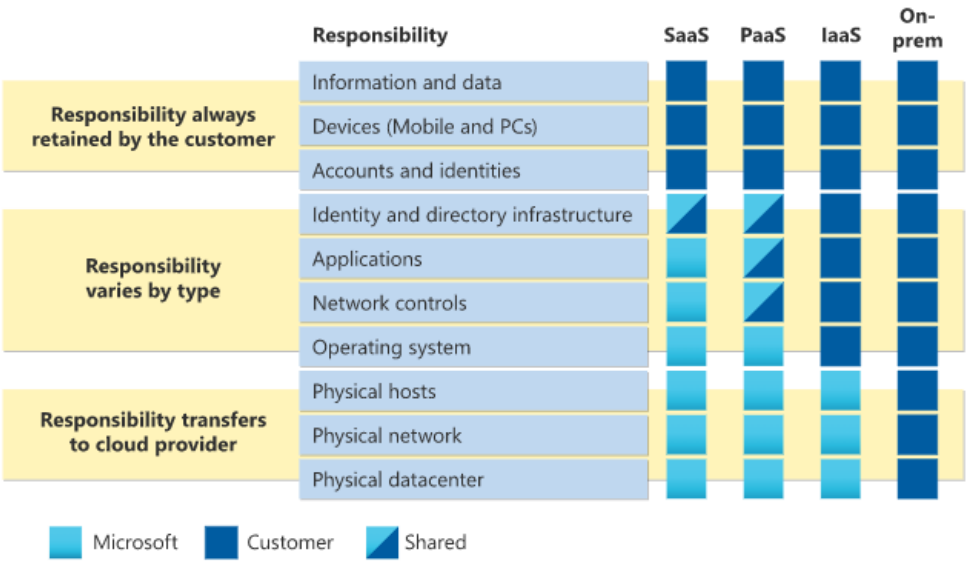


Figura 3. Matriz responsabilidad compartida Azure

Una de las diferencias más importantes está en la seguridad utilizada en estos modelos, dependiendo del modelo la seguridad la responsabilidad cambia. Un caso muy claro son los servicios *IaaS*, la seguridad de la infraestructura recae en el proveedor de la nube con el que se haya contratado el servicio, sin embargo, el proveedor no es el responsable de los problemas de seguridad que puedan tener las aplicaciones instaladas por el usuario. En contraposición están los servicios *SaaS*, que tanto la infraestructura como la seguridad de las aplicaciones instaladas recae sobre el proveedor de la nube.

Dado que el uso de los servicios de computación en la nube abarca al cliente y al proveedor, la responsabilidad por los aspectos de seguridad puede distribuirse entre ambas organizaciones, con la posibilidad de que partes vitales de la defensa queden desprotegidas si no se asigna claramente dicha responsabilidad siendo fuente de posibles *riesgos* y *amenazas*. Por ello, es necesario que el acuerdo de servicio (los *SLA*) y la descripción del servicio en la nube sean claros en los aspectos de seguridad y privacidad asociadas con el servicio en la nube, para mitigar el riesgo de imprecisión en las responsabilidades y sus posibles consecuencias.

2.4. Principales *riesgos* y *amenazas* en computación en la nube

La computación en la nube ha introducido una nueva serie de *amenazas* y desafíos de seguridad que están transformando en las organizaciones el uso, almacenamiento y compartición de datos, aplicaciones y cargas de trabajo. Con tanta información en la nube, y en particular en los servicios de nube pública, estos recursos se convierten en objetivos naturales para ciberdelincuentes.

Para proporcionar a las organizaciones una visión de los posibles problemas de seguridad en la nube, y que los tengan en cuenta a la hora de tomar decisiones y realizar estrategias de adopción a esta tecnología, *CSA* ha ido generando un informe con las principales *amenazas* existentes. En el último, *Top Threats to Cloud Computing* realizado en 2022 [2], se recogen 11 *amenazas* donde se identifican las mayores preocupaciones de los expertos de la industria.

2.4.1. Principales *Amenazas*

2.4.1.1. Gestión insuficiente de identidades, credenciales y acceso

Los delincuentes que se hacen pasar por usuarios legítimos, operadores o desarrolladores pueden leer, modificar y eliminar datos. También pueden detectar los datos en tránsito e incluso pueden liberar software malicioso que parece provenir de una fuente legítima. Como resultado, una identidad, credencial o administración de claves insuficientes puede permitir el acceso no autorizado a datos y daños potencialmente catastróficos a organizaciones o usuarios finales.

Impacto

Tener una gestión o un control insuficiente puede ocasionar un impacto y unas consecuentes graves:

- Bloqueos y accesos excesivamente restrictivos que perjudican al desempeño de los equipos.
- Corrupción o modificación de datos versus filtración por parte de usuarios no autorizados.
- Pérdida de confianza e ingresos en el mercado.
- Costes incurridos por incidentes y análisis forenses.
- Interrupción del servicio por ransomware o posibles ciberataques.

2.4.1.2. Interfaces y API inseguras

Los proveedores de la nube exponen un conjunto de interfaces de usuario de software o API que los clientes utilizan para administrar e interactuar con los servicios de la nube. El aprovisionamiento, la administración y la monitorización de la nube se realizan con estas interfaces, por lo tanto, la seguridad de éstas es relevante.

Impacto

El principal impacto en este caso es la exposición no intencionada de datos confidenciales o privados.

2.4.1.3. Configuraciones incorrectas y control de cambios inadecuado

La falta de conocimiento del entorno o las malas intenciones pueden dar lugar a errores de configuración que dejan vulnerables los sistemas a daños no deseados o actividades maliciosas. La configuración incorrecta de los recursos en la nube es una de las principales causas de violación de datos. Una mala configuración puede permitir la eliminación o modificación de los recursos y con esto la interrupción del servicio.

Por otro lado, un control de cambios inadecuado en la nube pude ayudar a que se den configuraciones incorrectas. Los cambios en la nube son más difíciles de controlar, requiere un entorno dinámico con un enfoque ágil y proactivo, basándose en la automatización, la expansión de roles y el acceso para admitir cambios rápidos.

Impacto

Las consecuencias de una mala configuración pueden llegar a ser importantes. Podríamos estar hablando de un impacto en confidencialidad, disponibilidad, integridad, operacional, financiero, reputacional:

- Exposición, divulgación, modificación, perdida y destrucción de datos.
- Desempeño e interrupción de los sistemas.
- Demanda de rescates.
- Incumplimientos y multas.
- Impacto reputacional, pérdida de confianza e ingresos en el mercado.

2.4.1.4. Falta de arquitectura y estrategia de seguridad en la nube

La estrategia y la arquitectura de seguridad en la nube abarcan la consideración y selección de puntos clave como: modelos de implementación, proveedores, zonas de disponibilidad o principios generales. El rápido ritmo de cambio y el enfoque predominante, descentralizado y de autoservicio, para la administración de la infraestructura en la nube, dificultan la capacidad de tener en cuenta las consideraciones técnicas, comerciales y el diseño necesario.

Impacto

La ausencia de una estrategia y una arquitectura de seguridad impacta principalmente en el incumplimiento de normativas que puede llevar infracciones con importantes multas. Además de implantaciones alternativas que incrementan el coste.

2.4.1.5. Desarrollo de software inseguro

Las vulnerabilidades en software son errores explotables en los programas que los atacantes pueden usar para infiltrarse en un sistema y robar datos, tomar el control del sistema o interrumpir las operaciones de servicio. Todos los meses los principales proveedores de software lanzan parches que corrigen errores podrían usarse para afectar la confidencialidad, la integridad y/o la disponibilidad de un sistema. El software es complejo y las tecnologías en la nube tienden aumentar esta complejidad.

Impacto

Algunos de los impactos del desarrollo inseguro son la pérdida de confianza del cliente en el producto o el daño reputacional debido a la violación de datos.

2.4.1.6. Recursos de terceros no seguros

El uso de recursos de terceros está aumentando, estos recursos se convierten y forman parte del proceso de entrega de un producto o un servicio. Hay una amplia variación, puede tratarse desde código abierto, pasando por productos *SaaS* o API. Los riegos derivados de terceros también son vulnerabilidades en la cadena y deben entrar en consideración y análisis.

Impacto

A continuación, se muestran algunos de los impactos que se puede generar:

- Pérdida o paralización de procesos clave de negocio.
- Datos comerciales a los que acceden terceros.
- Parchear o solucionar un problema de seguridad depende del proveedor y de la rapidez con la que responde. Dependiendo de la importancia del componente vulnerable puede tener un impacto importante en el negocio.

2.4.1.7. Vulnerabilidades del sistema

Las vulnerabilidades del sistema son fallos en las plataformas de servicios en la nube. Todos los componentes pueden contener vulnerabilidades que pueden dejar los servicios en la nube abiertos a ataques. En la nube los sistemas de varias organizaciones se colocan uno cerca de otro y se les da acceso a la memoria y a recursos compartidos, creando una nueva y mayor superficie de ataque. La implementación de prácticas de fortalecimiento de la seguridad es esencial.

Impacto

Los principales impactos en este punto son:

- Violación de datos.
- Pérdida de confianza y clientes.
- Aumento de costes por incidentes.

2.4.1.8. Divulgación accidental de datos en la nube

El cambio de paradigma y la complejidad de la nube hace que los equipos involucrados tengan más posibilidades de realizar configuraciones incorrectas. Esta sea una de las mayores *amenazas* actualmente.

Impacto

El mayor impacto es comercial, los datos divulgados pueden ser confidenciales, datos de empleados, del producto, siendo un coste añadido la recuperación, además de la pérdida de clientes y la pérdida de confianza en el mercado.

2.4.1.9. Configuración incorrecta y explotación de cargas de trabajo de contenedor sin servidor

El entorno de la nube cambia completamente la forma de hacer las cosas, permite administrar y escalar la infraestructura de una manera mucho más ágil. En este modelo sin servidor es el *CSP (Content Security Policy)* quien asume la responsabilidad de la seguridad por lo que la configuración del mismo es de suma importancia.

Impacto

Las aplicaciones implementadas con tecnología sin servidor sin la experiencia necesaria y la diligencia debida pueden provocar infracciones graves, pérdida de datos y costes importantes, teniendo gran impacto en el negocio.

2.4.1.10. Crimen Organizado/Hackers/*APT*

Esta *amenaza* existe siempre: intrusos o equipo de intrusos que pueden establecer una presencia ilícita a largo plazo en una red y extraer datos.

Impacto

El principal impacto es comercial, los grupos ATP difieren unos de otros, desde motivaciones políticas hasta un grupo de crimen organizado. Dependiendo del objetivo el impacto puede tener mayor o menor gravedad.

2.4.1.11. Filtración de datos de almacenamiento en la nube

La filtración de datos de almacenamiento en la nube es un incidente que involucra información sensible, protegida o confidencial. Estos datos pueden ser divulgados, vistos, robados o utilizados por un individuo fuera del entorno operativo de la organización. En la mayoría de los casos se conoce la extracción de la información pasado mucho tiempo lo que hace que la mitigación no sea relevante.

Impacto

El mayor impacto es comercial:

- Pérdida de propiedad intelectual.
- La pérdida de confianza de los clientes, las partes interesadas, los socios y los empleados.
- Multas financieras o demanda de cambio de proceso y negocio.
- Las implicaciones geopolíticas pueden afectar la conducta empresarial.
- Pérdida de confianza de los empleados en la capacidad de la organización para proteger los datos de los empleados.

Observando las *amenazas* descritas, podemos intuir que los *riesgos* no son introducidos principalmente por la infraestructura en la nube en sí, sino por los usuarios inexpertos que implementan malas prácticas. Las formas más comúnmente reportadas de incidentes de seguridad en la nube involucran recursos compartidos abiertos, en los que alguien deliberadamente pone datos confidenciales a disposición de personas externas. El uso seguro de todas las formas de nube pública requiere nuevas políticas, habilidades y actividades organizacionales. Ninguna tecnología, en las instalaciones o en la nube pública, puede considerarse cien por cien segura o confiable, especialmente cuando a los usuarios y al personal de la organización se les proporciona una nueva capacidad sin orientación sobre su uso o administración.

A continuación, enumeramos los principales riegos de computación en la nube recogidos prioritariamente de la guía de cloud computing realizada por el Instituto Nacional de Ciberseguridad (INCIBE) [3] [13].

2.4.2. Principales *Riesgos*

2.4.2.1. Acceso a usuarios privilegiados

Este tipo de *riesgo* aparece cuando un empleado deshonesto con acceso a cuentas privilegiadas puede robar información y datos confidenciales o sabotear sistemas críticos, en realidad puede moverse por la organización sin ser detectado.

Destacan dos escenarios:

- Acceso de empleado que actúan de forma maliciosa.
- Privilegios dados por error a empleados que por desconocimiento provoquen daños.

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

Impacto

Podría darse una pérdida de confidencialidad, integridad e incluso disponibilidad de la información.

2.4.2.2. Incumplimiento normativo

El incumplimiento normativo es un tipo de *riesgo* que aparece cuando el proveedor no cumple o no nos permite cumplir con nuestras obligaciones legales:

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

Por cumplimiento normativo se entiende la materia y el proceso consistente en garantizar que una empresa cumple la legislación establecida por las administraciones públicas en su ubicación geográfica, o las normas del sector adoptadas voluntariamente. En el caso de las organizaciones multinacionales (especialmente las de los sectores con mucha regulación, como los servicios financieros y la atención sanitaria), el cumplimiento puede ser muy complicado. Hay un gran número de normas y regulaciones que, en ciertos casos, cambian con frecuencia. El resultado es que para las empresas cada vez es más difícil mantenerse al tanto de la evolución de las leyes internacionales de gestión de datos electrónicos.

Impacto

Por este tipo de infracciones pueden darse sanciones administrativas e incluso penales, ocasionando una importante pérdida reputacional.

2.4.2.3. Desconocimiento de la localización de los datos

El proveedor aloja los datos del cliente en un Centro de Datos del cual podemos desconocer la ubicación. Este *riesgo* aparece principalmente por la falta de conocimiento de la legislación que le corresponde aplicar.

El desconocimiento de la ubicación de la nube no exime de las responsabilidades en materia de protección de datos. Esto es especialmente sensible en aquellos casos en los que el usuario contrata un servicio en la nube que puede tener físicamente los servidores en otro país, en este caso se genera una transferencia internacional de datos que requiere de una serie de acciones adicionales cuando se trata de otro país de la UE o de Estados Unidos.

Impacto

Por el desconocimiento en la localización de los datos se pueden cometer infracciones graves que conlleven importantes sanciones, ocasionando una irreversible pérdida reputacional.

2.4.2.4. Falta de aislamiento de los datos

El *riesgo* por falta de aislamiento en los datos aparece en los servicios en los que nuestra empresa comparte la infraestructura en la nube con otras compañías, en estos casos es necesario que el proveedor gestione que los

datos de las distintas empresas no se mezclen y que cada empresa tenga acceso a los suyos.

La multiprestación y los recursos compartidos son características que definen la computación en nube. Esta categoría de *riesgo* abarca el fallo de los mecanismos que separan el almacenamiento, la memoria o el enrutamiento.

Impacto

La materialización de este *riesgo* puede conllevar perdida de confidencialidad con impacto reputacional importante.

2.4.2.5. Indisponibilidad del servicio en caso de desastre o incidente

Si nuestro proveedor sufre un incidente grave o un desastre y no tiene un plan de continuidad adecuado no nos podrá seguir dando servicio, este *riesgo* está relacionado con el plan de continuidad de los proveedores de la nube.

Las empresas deben protegerse y estar preparadas para reaccionar ante posibles incidentes de seguridad que puedan afectar a la capacidad operativa, hacer peligrar la continuidad del negocio o dañar la imagen de la empresa.

En la actualidad, la planificación de la recuperación ante desastres es fundamental para cualquier empresa, en particular, aquellos que operan de forma parcial o total en la nube. Los desastres que interrumpen el servicio y causan la pérdida de datos pueden ocurrir en cualquier momento sin advertencias.

Impacto

Dependiendo de la criticidad del servicio que sufre indisponibilidad el impacto puede ser mayor o menor, pudiendo llegar a causar grandes pérdidas económicas para la empresa.

2.4.2.6. Carencia de soporte investigativo

En caso de que ocurra un incidente, necesitamos revisar los accesos a los datos para saber que ha ocurrido. En este caso, existe un *riesgo* ya que no podremos actuar si el proveedor no nos garantiza el acceso a los logs o registros de actividad y en muchas ocasiones se muestran reacios a ayudar.

Por otro lado, el análisis forense tiene mayor complejidad: como los servidores en la nube a menudo se encuentran en diferentes países, los datos requeridos por los investigadores forenses también pueden estarlo. Esto presenta inmediatamente a los investigadores un obstáculo de la jurisdicción legal.

Impacto

La materialización de este *riesgo* podría ocasionar pérdida reputacional a la empresa.

2.4.2.7. Concentración de proveedor único

Existe el *riesgo* de que las condiciones del contrato sufran alguna modificación debido al cambio de estructura del proveedor, de la alta dirección, a la entrada en situación de quiebra del mismo o a que decida externalizar parte de sus servicios. Por ello es recomendable asegurarse el acceso a los datos y su recuperación.

La oferta actual en cuanto a herramientas, procedimientos o formatos de datos estandarizados o interfaces de servicio que puedan garantizar la portabilidad del servicio, de las aplicaciones y de los datos, resulta escasa. Por este motivo, la migración del cliente de un proveedor a otro o la migración de datos y servicios de vuelta a un entorno de *TI* interno puede ser compleja. Esto conlleva a las empresas a tener una dependencia con el proveedor de servicios en nube elegido, especialmente si no está activada la portabilidad de los datos como aspecto más fundamental.

A continuación, añadimos una imagen donde se muestra los cuatro aspectos más importantes en el *riesgo* de concentración de proveedor único:

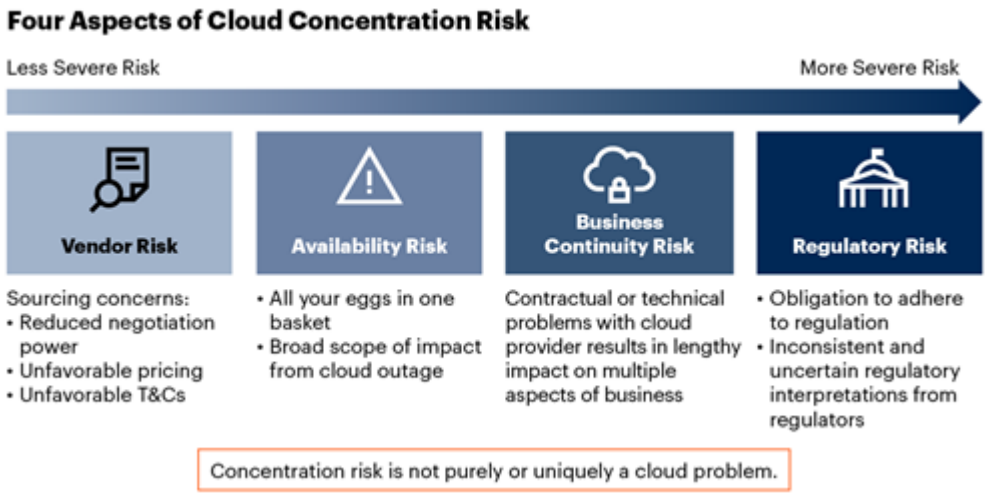


Figura 4. *Riesgos* concentración Cloud

Impacto

En este caso la empresa podría sufrir un impacto económico grave.

2.4.2.8. Falta de protección de datos

La computación en nube plantea varios *riesgos* relativos a la protección de datos tanto para clientes en nube como para proveedores del servicio. Puede resultar difícil para el cliente de la nube comprobar de manera eficaz las prácticas de gestión de datos del proveedor en nube, y, en consecuencia, tener la certeza de que los datos son gestionados de conformidad con la ley. Este problema aumenta cuando existen transferencias múltiples de datos entre nubes.

Impacto

Podría darse una pérdida de confidencialidad, integridad e incluso disponibilidad de la información.

2.4.2.9. Eliminación de datos insegura o incompleta

Al igual que sucede en la mayoría de los sistemas operativos, cuando se realiza una solicitud para eliminar un recurso en nube en ocasiones el proceso no elimina definitivamente los datos, este es el *riesgo* al que se hace referencia. La eliminación adecuada o puntual de los datos a veces también puede ser imposible, ya sea porque se almacenan copias adicionales de los datos, pero no están disponibles, o porque el disco que se va a eliminar también almacena datos de otros clientes. En el caso de multiprestación y la reutilización de recursos de hardware, esto representa un mayor *riesgo* para el cliente que en el caso del hardware dedicado.

Impacto

Se podría cometer infracciones con sanciones administrativas e incluso penales, ocasionando una importante pérdida reputacional.

La rápida adopción de los servicios en la nube y las diversas formas en que los servicios se implementan y se consumen en toda la organización han provocado un cambio en el panorama de *amenazas* y la aparición de nuevos *riesgos*. A menudo es posible, y en algunos casos recomendable, que el cliente en nube transfiera el *riesgo* al proveedor de ésta, pero no todos los *riesgos* pueden ser transferidos: si un *riesgo* provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños. En última instancia, puede subcontratar la responsabilidad, pero no puede subcontratar la obligación de rendir cuentas.

3. Seguridad en la nube

El crecimiento constante de las tecnologías, estrategias y nuevos proveedores plantea un desafío adicional para la seguridad en la nube, convirtiéndose, como hemos comentado a lo largo del proyecto, en una de las mayores preocupaciones de las compañías. Si la seguridad no está implementada desde el principio, se tiene una alta probabilidad de que se produzcan infracciones o ataques maliciosos con éxito.

Una vez vistas las principales *amenazas* y *riesgos* en computación en la nube podríamos pensar que es sencillo buscar una solución de seguridad para cada caso, pero nada más lejos de la realidad. Ejecutar controles de seguridad sólo es una parte de su implementación.

Apoyándonos en la siguiente imagen de Gartner, se presenta un plan de implantación de seguridad en la nube que está formado por cuatro bloques principales, para ayudar a las empresas en su migración.

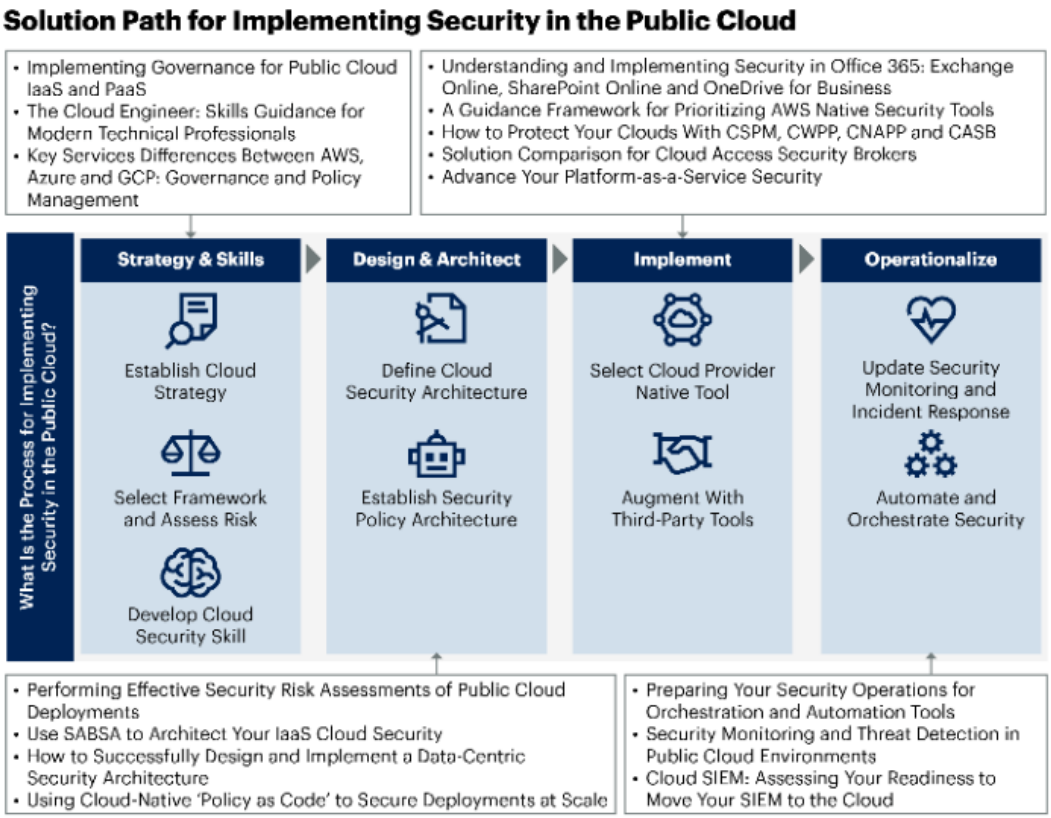


Figura 5. Implantación de la seguridad en la nube pública

Vamos a dedicar un espacio a cada uno de los bloques, detallándolo en mayor o menor medida, pero ir introduciéndonos en los conceptos:

3.1. Estrategia y habilidades

A medida que las organizaciones adoptan rápidamente nuevos servicios en la nube, la seguridad debe poder adaptarse a estos cambios con la misma fluidez que el resto de la organización. La creación de un plan estratégico ayudará a progresar y mejorar su implementación en la nube aprovechando los nuevos servicios y capacidades de seguridad.

Migrar a la nube sin una estrategia clara da como resultado patrones de adopción ad hoc, lo que da lugar a costes más altos, a una administración desarticulada, a vulnerabilidades de seguridad y a una insatisfacción general con los resultados obtenidos.

Mostramos a continuación algunos de los elementos clave para formular una buena estrategia:

- Estrategia de la nube alineada con la estrategia empresarial: las estrategias de negocio varían significativamente según las organizaciones, es imprescindible un alineamiento entre estrategia de la nube y estrategia de negocio.

- Evaluar riesgos: al establecer una estrategia en la nube es esencial evaluar los riesgos relacionados con ésta como el riesgo de agilidad, de disponibilidad, de seguridad, de proveedor o de cumplimiento. Los posibles riesgos deben sopesarse con los beneficios potenciales de manera equilibrada y conforme.

- Planificar posibles rutas a la nube: la adopción de la nube puede realizarse de diferentes formas, es importante planificar las posibles rutas y evaluar cuál es la mejor para la organización, incluyendo siempre la seguridad.

- Modelo de responsabilidad compartida de la nube: ya introdujimos este concepto con anterioridad. Las responsabilidades del proveedor se definen por las características y capacidades del servicio en la nube que se ofrece. El cliente debe aprovechar las capacidades del servicio en la nube dentro de los propios procesos de la organización para obtener el resultado deseable. Los *SLA* y una clara descripción del servicio en la nube son especialmente relevantes en este punto.

- Papel cambiante del departamento de *TI*: independientemente de la estrategia implementada, ésta implicará un papel cambiante para la organización interna de *TI*. Se deben generar nuevos roles que deberán ser cubiertos por personal cualificado para el desarrollo de sus funciones. Identificar los roles y responsabilidades en detalle es fundamental para utilizar la nube de forma segura.

La seguridad debe estar muy presente dentro de la estrategia que se defina. Para conseguir una buena seguridad se debe comprender los requerimientos de negocio y alinearlos con el personal correctamente capacitado que pueda cumplir con ellos. La

implementación de un proceso de migración a la nube sin una estrategia y sin el personal con las habilidades necesarias podría complicar mucho su ejecución. Implementar la seguridad en la nube requiere un cambio de mentalidad y exige nuevas habilidades que abarquen las áreas de estrategia, liderazgo, seguridad operativa y técnica. La seguridad en la nube abarca múltiples disciplinas, las cuales son necesarias para abordar los riesgos, prevenir intrusiones y disuadir amenazas.

Seguridad y mitigación de *riesgos* y *amenazas*

Algunas de las principales *amenazas* y *riesgos* de la computación en la nube vienen derivadas del desconocimiento del personal implicado. Tener empleados cualificados permite reducir el *riesgo* de configuraciones incorrectas en los entornos de la nube y posibles incidentes. En el caso de incidente grave el análisis forense se vería reforzado por este conocimiento.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.3. Configuraciones incorrectas y control de cambios inadecuado.
- 2.3.1.4. Falta de arquitectura y estrategia de seguridad en la nube.
- 2.3.1.8. Divulgación accidental de datos en la nube.
- 2.3.1.9. Configuración incorrecta y explotación de cargas de trabajo de contenedor sin servidor.
- 2.3.2.6. Carencia de soporte investigativo.

3.2. Diseño y Arquitectura

Para el diseño de la arquitectura de seguridad en la nube se necesitan nuevos conceptos, procesos y herramientas a fin de tener en cuenta los nuevos modelos de implantación como *SaaS*, *PaaS* e *IaaS*. Estos nuevos componentes deberán descomponerse y enfocarse para definir las necesidades de seguridad particulares de cada área de implementación de la nube.

Existen múltiples enfoques de la arquitectura de seguridad, incluido el uso de marcos y metodologías para respaldar los pasos de diseño e implementación. El uso de una arquitectura de seguridad ayuda a crear implantaciones manejables en la nube, ayuda a centrarse en las necesidades de seguridad particulares de cada área y facilita el enfoque en las integraciones entre las nubes, sus zonas y sus interfaces, lo que garantiza que se aborden todos los aspectos de la implementación.

Para proteger los datos y las aplicaciones en la nube, las organizaciones comienzan eligiendo un conjunto apropiado de controles de seguridad nativos para posteriormente complementarlo con otras herramientas de terceros y de este modo dar mayor garantía de seguridad a sus activos. También elegir una plataforma de terceros a veces es una forma de eficientar y simplificar, principalmente cuando se utiliza estrategia multinube.

Teniendo como objetivo proteger y mitigar las *amenazas* y *riesgos* que se han visto en apartados anteriores, a continuación, se muestran varios enfoques posibles para implantar la seguridad en un entorno de nube pública:

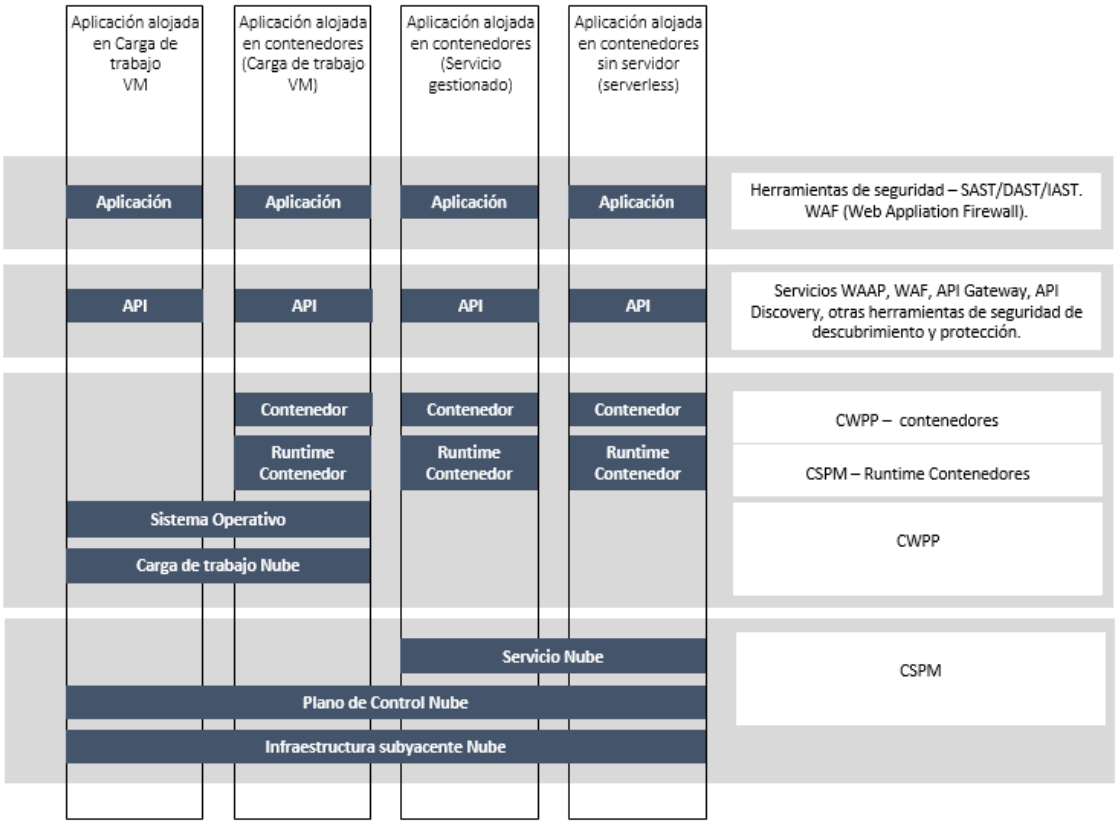


Figura 6. Enfoques seguridad de aplicaciones en nube

Para realizar el diseño de los distintos enfoques de seguridad, que podemos ver en la imagen, se han tratado todas las variedades de cargas de trabajo existentes en la nube. A continuación, se muestra detalle sobre ellas para darlas a conocer:

Tipo	Modelo de servicio	Abstraído en	Ubicación del alojamiento	Entorno
Servidor	Autoalojado	Hardware físico	Local	Su propio hardware
Máquina virtual	*IaaS*, *PaaS*, *SaaS*	Hipervisor	En la nube o en local	Su propio hardware virtual
Contenedor	*IaaS*, *PaaS*	Núcleo del sistema operativo	Nube	Su propio sistema operativo
Función sin servidor	*FaaS*	En función del proveedor	Nube	En función del proveedor

En el siguiente apartado se revisará cada una de las capas indicadas en el diseño (figura 6).

Seguridad y mitigación de *riesgos* y *amenazas*

Una de las principales *amenazas* de la nube es la falta de arquitectura y estrategia de seguridad. Diseñar una arquitectura y una estrategia de seguridad precisa permitirá reducir *riesgos* al estar enfocada en proteger los datos y las aplicaciones. La mitigación de *riesgos* y *amenazas* que puede cubrir dependerá de la profundidad y el detalle con que se realice.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.4. Falta de arquitectura y estrategia de seguridad en la nube.
- 2.3.2.3. Desconocimiento de la localización de los datos.
- 2.3.2.5. Indisponibilidad del servicio en caso de desastre o incidente.
- 2.3.2.7. Concentración de proveedor único, 2.3.2.8. Falta de protección de datos.

3.3. Implementación

Aprovechar el conjunto de controles de seguridad existentes y adecuados para una organización es un gran reto. Continuamente aparecen nuevas capacidades nativas de seguridad que mejoran las funciones existentes. Aun así, puede ocurrir que no cubran todos los casos de uso de las organizaciones, por ello las empresas tienen siempre la posibilidad de buscar aumentar la seguridad utilizando herramientas de terceros.

El primer paso para implementar los controles es utilizar y aprovechar los controles nativos del proveedor o proveedores de la nube que la organización haya seleccionado. La elección de controles es uno de los principales desafíos de seguridad al que nos enfrentaremos para migrar aplicaciones, servicios y datos.

A continuación, entraremos a analizar cada capa de seguridad que mostrábamos en el apartado anterior.

3.3.1. Seguridad Aplicación

En la seguridad alrededor de las aplicaciones utilizaremos:

3.3.1.1. Herramientas de seguridad DevOps

Dentro de la seguridad de las aplicaciones añadimos la seguridad en el ciclo de vida del software (*SSDLC*), incluyendo herramientas de análisis de código que nos permiten tener software libre de vulnerabilidades que podrían ser explotadas por algún usuario malicioso.

- SAST (Static Application Security Testing): tecnología diseñada para analizar el código fuente de las aplicaciones e identificar vulnerabilidades de seguridad.

- DAST (Dynamic Application Security Testing): pruebas de seguridad de caja negra en la que una aplicación se prueba desde el exterior.

- IAST (Iinterative Application Security Testing): detección inmediata de los problemas de seguridad en el software gracias al análisis de flujo de ejecución de las aplicaciones.

La automatización en los despliegues, incluido la infraestructura como código (*IAC*) o políticas como código (*PaC*), ayuda a evitar errores de configuración y a tener una mejor gestión y un mayor control en los cambios.

Alrededor de la integración de DevOps, los proveedores de nube ofrecen servicios y partners que pueden ser complementados con herramientas de terceros para introducir la seguridad en el ciclo de vida del software, siempre con el objetivo de llevarla lo más a la izquierda posible para eficientar y agilizar todo el proceso.

Seguridad y mitigación de *riesgos* y *amenazas*
Con estas herramientas ayudamos a mitigar configuraciones incorrectas, control de cambios inadecuados, desarrollo de software inseguro o vulnerabilidades del sistema, haciendo más segura la infraestructura, el software y todo lo relacionado con los despliegues.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.3. Configuraciones incorrectas y control de cambios inadecuado.
- 2.3.1.5. Desarrollo de software inseguro.
- 2.3.1.6. Recursos de terceros no seguros.
- 2.3.1.7. Vulnerabilidades del sistema.
- 2.3.1.9. Configuración incorrecta y explotación de cargas de trabajo de contenedor sin servidor.

3.3.1.2. WAF (Web Application Firewall)

Los firewalls de aplicaciones web, nos permite proteger de múltiples ataques a los servidores de aplicación garantizando la seguridad del servidor web. Normalmente, protege las aplicaciones web de ataques tales como falsificaciones entre sitios, scripts entre sitios (XSS) o inclusiones de archivos en inyecciones de código SQL, entre otros.

En las diferentes nubes públicas encontramos servicios WAF, aquí nombramos algunos de ellos: Azure Web Application Server [21], AWS WAF [22] o Google Cloud Armor [23] son algunos de los ejemplos.

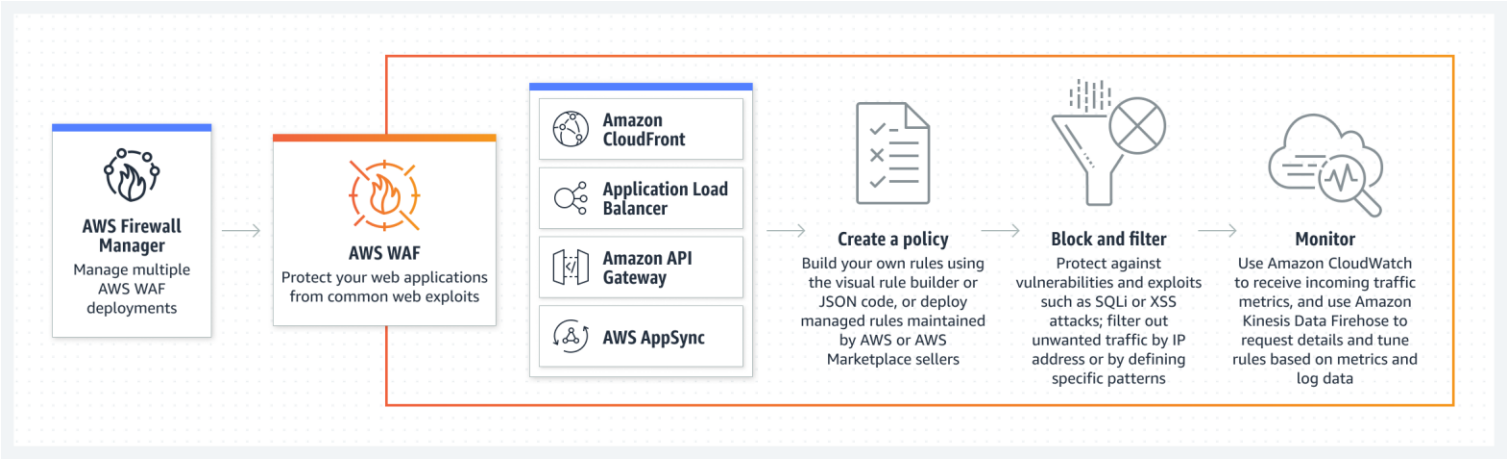


Figura 7. Diagrama AWS WAF [22]

Seguridad y mitigación de riesgos y amenazas

Con un WAF ayudamos principalmente a la protección de datos, analizando todo el tráfico HTTP/S entrante, bloqueando el que sea malicioso, y asegurando que no sale ningún dato no autorizado.

Principales amenazas y riesgos mitigados:

- 2.3.2.8. Falta de protección de datos.
- 2.3.2.4. Falta de aislamiento de los datos.

3.3.2. Seguridad API

El uso de las API está en continuo crecimiento. Las empresas utilizan las API para conectar los servicios y transferir datos. Las API dañadas, expuestas o pirateadas son la causa de las principales vulneraciones de la seguridad de los datos.

3.3.2.1. Servicios WAAP (Web Application and API Protection)

Los servicios completos de protección de API y aplicaciones web protegen sus aplicaciones web y API contra un amplio espectro de ataques. Un servicio WAAP debe inspeccionar eficazmente las solicitudes antes de que lleguen a la aplicación o al punto final de la API.

Principales Funcionalidades:

- Firewall de aplicaciones web de próxima generación (WAF de próxima generación con análisis de comportamiento e inteligencia artificial (IA))
- Autoprotección de aplicaciones en tiempo de ejecución (*RASP*)
- Protección contra bots maliciosos.

- Protección de denegación de servicio distribuida (*DDoS*).
- Limitación de velocidad avanzada.
- Protección para microservicios y API.
- Protección de apropiación de cuentas.

Un proveedor que ofrece servicio WAAP es Google Cloud, donde ofrece el paquete conformado por tres soluciones [24]: Cloud Armor, reCAPTCHA Enterpres y Apigee.

En aquellos proveedores de nube que no ofrecen este servicio podría ser sustituido por un WAF, aunque la solución es menos completa.

Seguridad y mitigación de *riesgos* y *amenazas*
Con un servicio WAAP ayudamos principalmente a la protección de datos, analizando todo el tráfico entrante y asegurando el tráfico de salida. En este caso se apoya en análisis de comportamiento.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.2. Interfaces y API inseguras.
- 2.3.1.6. Recursos de terceros no seguros.
- 2.3.2.8. Falta de protección de datos.
- 2.3.2.4. Falta de aislamiento de los datos.

3.3.2.2. Api Gateway

Es un gestor del tráfico que interactúa con los datos o el servicio backend real y aplica políticas, autenticación y control de acceso general para las llamadas de una API, de este modo se protege los datos valiosos.

Figura 8. API Gateway

Permite optimizar la comunicación entre los clientes y sus servicios de back-end, es la forma de controlar el acceso a los sistemas y dichos servicios. Un

API Gateway garantiza la escalabilidad y la alta disponibilidad de sus servicios, mantiene una conexión segura entre sus datos y las API, y gestiona el tráfico y las solicitudes de una API, incluido el equilibrio de carga, tanto dentro como fuera de su empresa.

Los proveedores de cloud ofrecen este servicio. Algunos ejemplos son: Amazon API Gateway en AWS [26] o Azure API Management + Azure Application Gateway [27].

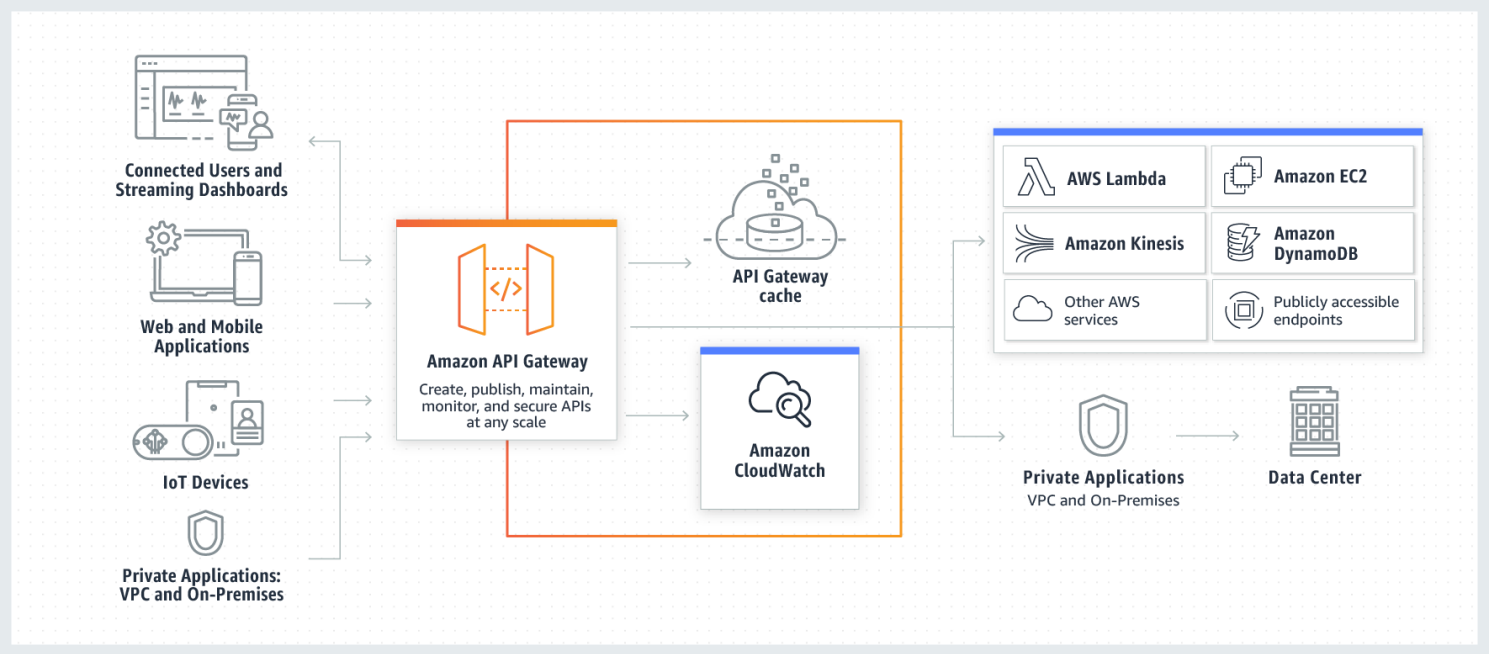


Figura 9. Diagrama Amazon API Gateway [26]

Seguridad y mitigación de *riesgos* y *amenazas*

Con API Gateway administramos el tráfico ayudando a la disponibilidad del servicio, controlando la autorización y el acceso para evitar accesos no deseados. También se monitoriza y administra las versiones de API lo que permite mayor seguridad en las configuraciones y en el software.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.1. Gestión insuficiente de identidades, credenciales y acceso.
- 2.3.1.2. Interfaces y API inseguras.
- 2.3.1.6. Recursos de terceros no seguros.
- 2.3.2.8. Falta de protección de datos.
- 2.3.2.4. Falta de aislamiento de los datos.

3.3.2.3. API Discovery

Es un servicio que permite encontrar y probar API ocultas/públicas/abiertas, comparar API privadas/internas con estándares líderes en la industria y monitorizar API para dar mayor seguridad. Incluso se podrían realizar pruebas de seguridad automatizadas utilizando los marcos OWASP top-10 y CIS top-20 para mitigar las vulnerabilidades específicas de la API.

Algunos proveedores ofrecen directamente este servicio como Google API Discovery Services [28] y en otros como AWS tiene en su Marketplace la posible integración con un tercero (TeejLab) [29].

Seguridad y mitigación de *riesgos* y *amenazas*
Con API Discovery podemos descubrir nuevas API que no están autorizadas. Existe también la posibilidad de realizar comparaciones entre las API de la industria. Esto nos permite evitar API inseguras y darles una mayor protección.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.2. Interfaces y API inseguras.
- 2.3.1.6. Recursos de terceros no seguros.

3.3.3. Seguridad en Contenedores y/o Sistema Operativo

3.3.3.1. CWPP (Cloud Workload Protection Platforms)

Es una plataforma de protección de la carga de trabajo. Es una herramienta de seguridad que detecta y elimina las *amenazas* dentro del software que se ejecuta en la nube, ya sea una aplicación, un servicio o una funcionalidad. Los *CWPP* ofrecen capacidades de seguridad y protección en máquinas virtuales, contenedores, *PaaS* y cargas de trabajo sin servidor. Sus principales funciones son:

- Gestión del endurecimiento, la configuración y la vulnerabilidad: ayuda a garantizar que no haya vulnerabilidades en el software, incluso antes que se pase a producción.

- Firewall, visibilidad y microsegmentación de la red: protege y microsegmenta una red, divide una red en porciones más pequeñas para que un atacante no pueda poner en *riesgo* toda la red a la vez.

- Garantía de la integridad del sistema: se asegura de que los sistemas en la nube funcionen según lo previsto.

- Control de aplicaciones y listas de permitidos: permite y bloquea aplicaciones en base a una lista de aplicaciones permitidas.

- Prevención de vulnerabilidades y protección de la memoria: evita que se puedan aprovechar de las vulnerabilidades en el software que se ejecuta activamente.

- Detección y respuesta de puntos de conexión de la carga de trabajo del servidor (*EDR*), supervisión del comportamiento, y respuesta y detección de las *amenazas*: responden a los cambios sospechosos en el comportamiento del servidor y de las aplicaciones, así como a las *amenazas* activas.

- Prevención de intrusiones basada en el servidor con protección ante vulnerabilidades: impiden las incursiones externas en los servidores.

- Escaneado antimalware: detectan el malware incrustado en las cargas de trabajo en la nube.

Aunque en proveedores de nube podemos encontrar servicios nativos que cubren algunas funcionalidades de esta plataforma, son plataformas de terceros las que nos ayudan a dar una mayor cobertura.

Servicios nativos podemos encontrar, por ejemplo, en AWS con Symantec Cloud Workload Protection Suite (CWP) [30] [31] que incluyen escaneo antimalware, sistema de prevención de intrusos basado en host y seguridad en contenedores

En el caso de Azure encontramos una plataforma ofrecida por Microsoft, Microsoft Defender for Cloud [32], que permite una amplia cobertura para proteger las cargas de trabajo, detecta y responde a *amenazas* de malware, realiza análisis de vulnerabilidades. Posibilidad de integración también con AWS y Google.

Son variados los proveedores que ofrecen esta plataforma y con diferente orientación y funcionalidades. A continuación, listamos algunos de ellos:

- Amplio espectro: Alibaba Cloud Server Guard, Microsoft, Atomicorp, McAfee.
- Centrados en servidores: Sysdig, Palo Alto Networks-PureSec, Trend Micro, Aqua Security
- Centrados en contenedores: Aqua Security, Qualys, Palo Alto Neworks, Sysdig
- Centrados en *EDR*: Ava Security, Qualys, SentinelOne

Seguridad y mitigación de *riesgos* y *amenazas*

CWP ayuda a proteger el acceso a datos y aplicaciones dando el aislamiento correspondiente (microsegmentación) o bloqueando aplicaciones no permitidas. Protege de vulnerabilidades que pueden estar ejecutándose activamente, protegiendo la memoria y los entornos de Producción. Por otro lado, verificando comportamiento de la carga ayuda a garantizar la disponibilidad de los sistemas y protección ante intrusos.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.7. Vulnerabilidades del sistema.
- 2.3.1.10. Crimen Organizado/Hackers/APT.
- 2.3.2.1. Acceso a usuarios privilegiados.
- 2.3.2.4. Falta de aislamiento de los datos.
- 2.3.2.8. Falta de protección de datos.

3.3.4. Seguridad Runtime contenedores y/o Servicios de la nube.

3.3.4.1. CSPM (Cloud Security Posture Management)

Las herramientas CSPM permite a las empresas visualizar el estado de la seguridad en sus entornos y activos en la nube. Sin embargo, va mucho más allá de esta simple evaluación de la postura para proporcionar capacidades generales de gestión del plano de seguridad. Desempeña un papel importante en la seguridad de la nube al identificar, remediar o alertar a los equipos de *TI* sobre configuraciones incorrectas de seguridad, *riesgos*, incumplimiento y otras vulnerabilidades. Algunas herramientas incluso proporcionan detección y reparación automática de fallos. Además, ofrecen monitorización y visibilidad continua de la postura de seguridad en la nube de la organización. Sus principales funciones son:

- Supervisión continua del entorno y los servicios de la nube: proporciona una visibilidad completa de los componentes y las configuraciones.

- Comparación de configuraciones y políticas de la nube: verificación de un conjunto de pautas aceptables. Proporcionan visibilidad de las políticas y garantizan una aplicación coherente en todos los proveedores en entornos multinube.

- Detección de errores de configuración y cambios de política: analiza sus instancias de computación y su almacenamiento en busca de errores de configuración y ajustes inadecuados que puedan dejarlas vulnerables a la explotación.

- Identificación de *amenazas* existentes, nuevas y potenciales.

- Realización de evaluaciones de *riesgo* con respecto a marcos y normas externas, como las propuestas por la Organización Internacional de Normalización (ISO) y el Instituto Nacional de Normas y Tecnología (NIST).

- Corrección de las configuraciones incorrectas en función de las reglas preconstruidas y los estándares de la industria: ayuda a reducir los *riesgos* debido a errores humanos que podrían resultar en configuraciones incorrectas.

Microsoft Defender for Cloud [32] también ofrece CSPM pudiéndose integrar con AWS, Azure y Gooble pero la mayor oferta es de terceros. Algunos de estos proveedores son: Aqua Security, Accurics, Alert Logic, BMC, Bridgecrew, C3M Cloud Control, Cloudnosys,…

Seguridad y mitigación de *riesgos* y *amenazas*

CSPM nos permite un mayor control de los componentes y las configuraciones, detectando errores o cambios de configuración y de políticas, con la posibilidad además de corregirlos automáticamente, esto da agilidad y reduce *riesgo*. Ayuda a evitar incumplimientos de normativa. Para el runtime de contenedores permite visualizar su superficie de ataque para localizar *riesgos* y *amenazas*, así como detectar si existe exposición a internet u otras configuraciones por defecto. El escaneo de imágenes permite la detección de vulnerabilidades.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.7. Vulnerabilidades del sistema.
- 2.3.1.8. Divulgación accidental de datos en la nube.
- 2.3.1.9. Configuración incorrecta y explotación de cargas de trabajo de contenedor sin servidor.
- 2.3.1.11. Filtración de datos de almacenamiento en la nube.
- 2.3.2.2. Incumplimiento normativo.
- 2.3.2.9. Eliminación de datos insegura o incompleta.

3.3.5. CASB (Cloud Access Security Broker)

CASB es un tipo de software que protege las aplicaciones SaaS de las empresas para que los datos de la organización estén seguros. Se encarga de la seguridad del acceso y los datos. Sus principales funciones son:

- Evaluación y administración de Shadow IT: aportan visibilidad en todas las aplicaciones de la nube.

- Análisis del comportamiento de los usuarios y control de accesos: ofrece una administración detalla del uso de la nube.

- Cumplimiento: ayuda a la aplicación de las políticas de seguridad y asistencia de conformidad con *GDPR*

- Alerta de *amenaza* para la seguridad: detección de comportamientos inusuales.

- Detección de malware.

Encontramos soluciones de terceros como: Bitglass, Broadcom-Symantec, CipherCloud, McAfee MVISION Cloud, Microsoft Cloud App Security (MCAS) [35], Force Point.

Seguridad y mitigación de *riesgos* y *amenazas*

CASB permite evitar incumplimientos de normativa. La detección de comportamientos inusuales o malware ayuda a detectar posibles intrusos, protegiendo las aplicaciones y los datos tanto de indisponibilidad como de robo de información.

Tener la visibilidad que te ofrecen estos servicios también ayuda a recoger información para hacer análisis en caso de incidente, mitigando el *riesgo* de carencia de soporte investigativo que comentábamos en apartados anteriores.

Cuando los entornos son poco complejos es posible que muchos de los *riesgos* puedan mitigarse con controles de seguridad nativos. Sin embargo, a medida que los entornos de la organización se complican o los datos que se manejan tienen una alta sensibilidad lo más aconsejable es apoyarse en otras herramientas de terceros que puedan cubrir ciertos gaps. Como vemos hay multitud de proveedores que ofertan herramientas, plataformas y servicios que pueden ayudar a las compañías a cubrir todos sus requerimientos adaptándose al negocio correspondiente.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.1.6. Recursos de terceros no seguros.
- 2.3.1.10. Crimen Organizado/Hackers/APT.
- 2.3.1.11. Filtración de datos de almacenamiento en la nube.
- 2.3.2.1. Acceso a usuarios privilegiados.
- 2.3.2.2. Incumplimiento normativo.
- 2.3.2.8. Falta de protección de datos.

3.4. Operación

Con la creciente complejidad de las arquitecturas de la nube, con las *amenazas* en constante evolución y con la necesidad de coordinar múltiples productos de seguridad, de monitorización y de respuesta a incidentes, poner en funcionamiento la seguridad y su operación en un entorno de nube se convierte en todo un desafío.

Los casos de uso de la tecnología de monitorización de seguridad en la nube son:

- Detección de *amenazas*: supervisar ataques, accesos no autorizados y otros problemas de seguridad. Detectar eventos de seguridad procesables y alertar cuando sea necesario. El proceso de clasificación de alertas se encuentra entre los procesos de detección y respuesta a incidentes de seguridad.

- Respuesta e investigación de incidentes de seguridad: recopilar los datos y permitir que los investigadores clasifiquen los detalles después de descubrir un incidente de seguridad.

- Cumplimiento normativo: ofrecer otras capacidades de monitoreo prescritas por los marcos de cumplimiento normativo (que pueden impulsar la detección y la investigación, así como la retención y la revisión de la actividad).

No existe una única "mejor práctica" para hacer operativa la seguridad en la nube. Una posibilidad es utilizar una herramienta específica de monitorización de seguridad como *SIEM* integrada con *SOAR* para automatizar, orquestar y dar respuesta de seguridad.

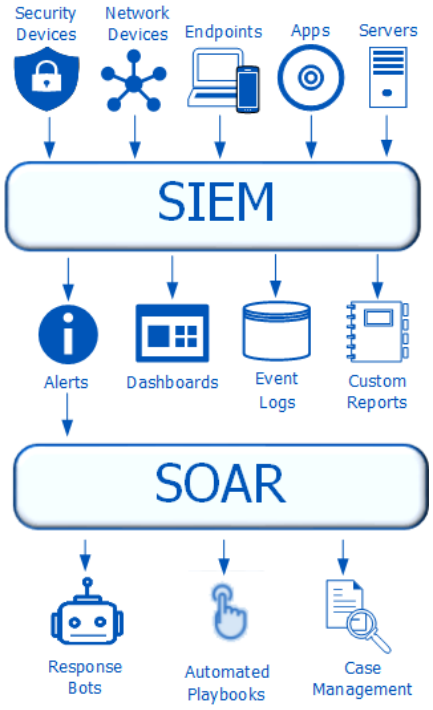


Figura 10. Flujo *SIEM* y *SOAR*

Las herramientas SOAR son probablemente la capacidad más versátil para la automatización y orquestación, permiten realizar el análisis de incidentes y su clasificación. Esto ayuda a definir, priorizar e impulsar actividades estandarizadas de respuesta a incidentes de acuerdo con un flujo de trabajo estándar.

Un despliegue eficaz de SOAR requiere no solo herramientas, procesos y procedimientos de respuesta a incidentes bien documentados, sino también la capacidad de ejecutarlos con consistencia y precisión. Además de la capacidad de refinar y actualizar las respuestas a medida que surgen las mejores prácticas.

SOAR se convierte en el eje central para que la organización logre varios objetivos:

- Monitoreo de eventos desde SIEM.
- Orquestación de diferentes productos de seguridad para construir el contexto.
- Priorización de múltiples elementos e incidentes simultáneos.
- Enriquecimiento de la información del evento automáticamente.
- Respuesta correspondiente.

La automatización y orquestación de la seguridad es un área en evolución y, actualmente, no existe un solo producto o proveedor que pueda automatizar y orquestar todo. Las organizaciones necesitarán combinar entre un número limitado de soluciones que mejor se alineen con sus necesidades y sus principales prioridades de seguridad, incluidas herramientas ya utilizadas para la monitorización de seguridad en local.

Seguridad y mitigación de *riesgos* y *amenazas*

La monitorización de seguridad centralizada ayudará a la detección de *amenazas*, la respuesta e investigación de incidentes y al cumplimiento normativo, como comentábamos. Esto permite reducir el *riesgo* existente en estos puntos.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.2.2. Incumplimiento normativo.
- 2.3.2.6. Carencia de soporte investigativo.

4. Seguridad con tipos de computación en la nube

Durante todo el recorrido de este proyecto hemos hablado de la seguridad en la nube pública, haciendo hincapié en el interés de todas las organizaciones por migrar e introducir en su estrategia esta emergente tecnología. Sin embargo, no siempre la nube pública es la única solución dentro del plan de transformación de las empresas.

En este escenario vamos a poner en contexto dos conceptos:

Los servicios de **nube pública** de terceros hacen que recursos como el almacenamiento y las aplicaciones de software como servicio (*SaaS*) estén disponibles de forma remota. Eliminando los matices, los proveedores de nube pública son responsables de proteger la infraestructura, mientras que los clientes son responsables de la seguridad de los datos.

Las **nubes privadas** se alojan en una infraestructura a la que solo pueden acceder los usuarios de una determinada organización. Puede tratarse de una infraestructura de terceros o de una infraestructura propia de la organización, el responsable último es la propia compañía.

La combinación de ambas y el uso de varios proveedores nos da una serie de posibilidades que nos ayudan en muchos casos a mitigar ciertos *riesgos* y *amenazas* de seguridad que de otro modo sería difícil de conseguir. A continuación, nos adentraremos en el mundo de nubes hibridas y multinube, pero antes es importante saber cuál es la diferencia entre ellas:

Multinube hace referencia al uso de los servicios de varios proveedores de servicios en la nube del mismo tipo, pública o privada. Con la multinube, la empresa puede supervisar diferentes proyectos en distintos entornos de nube de varios proveedores.

Nube híbrida puede utilizar entornos de varias nubes. No obstante, en una configuración de nube híbrida, el trabajo se distribuye en un sistema de carga de trabajo compartida entre nube pública, recursos locales y nube privada. Hace referencia al despliegue de cargas de trabajo comunes en varios entornos de computación.

4.1. Seguridad nube hibrida

En muchos casos las organizaciones se decantan por una estrategia de nube híbrida debido a que no pueden permitirse poner todos los elementos en la nube pública. Estas son las principales razones por las que se decide la combinación de ambas nubes:

- Incumplimiento regulatorio: casos en lo que los servicios de nube pública carezcan del cumplimiento de seguridad necesaria.

- Aplicaciones y sistemas heredados: no es viable la transformación a la nueva tecnología.

- Restricciones contables o modelo de financiación.

- Limitaciones con subcontratación: imposibilidad en cambio de gobernanza.

En esta solución hibrida parte de las aplicaciones y datos están en la nube privada, normalmente las aplicaciones críticas. La nube hibrida permite a las empresas tener un mayor control y seguridad sobre sus datos y aplicaciones. Las aplicaciones críticas pueden alojarse en servidores privados para mayor seguridad, mientras que las aplicaciones no críticas pueden alojarse en la nube pública para mayor escalabilidad. Los datos menos confidenciales suelen almacenarse en una nube pública, mientras que los datos altamente confidenciales se almacenan en una nube privada.

La seguridad en nube híbrida es un proceso para proteger la infraestructura, los datos y las aplicaciones a través de varios y diferentes entornos: nubes privadas, nubes pública y *CPDs* locales. El objeto es el de siempre: protegerse frente a ciberataques e intrusos.

Una arquitectura de nube híbrida puede mejorar la postura de seguridad de su organización ayudándole a:

- Gestionar su *riesgo* de seguridad: disponer de opciones de almacenamiento público y privado le permite aislar sus datos más confidenciales y/o altamente regulados en una infraestructura bajo su control, a la vez que ahorra en gastos generales almacenando los datos menos confidenciales con un tercero.

- Evitar tener un único punto de fallo: igual que con cualquier inversión, la diversificación ofrece seguridad. Almacenar sus datos en varias nubes hace mucho menos probable que los pierda todos a la vez por culpa de ransomware o de otro ataque de malware.

- Gobernanza internacional de los datos: al aprovechar una nube híbrida, especialmente un entorno multinube alojado en diferentes proveedores de servicios en la nube, la organización puede cumplir más fácilmente con las regulaciones de privacidad.

- Reducir su superficie de ataque: con una buena configuración, como microsegmentación, puede conseguir que la superficie de ataque sea menor.

- Ofrecer un acceso seguro a los datos y a las aplicaciones: no siempre es necesario ni es la mejor opción es exponer a internet los recursos.

Los entornos de nube híbrida difieren de una organización a otra. Sus necesidades y procedimientos cambiarán según el sector, la geografía y su arquitectura híbrida. Pero

como acabamos de ver, puede ser una forma de mitigar algunos de los *riesgos* y *amenazas* que comentábamos anteriormente.

Haciendo referencia al apartado anterior, ésta sería una posible integración a alto nivel de nube hibrida:

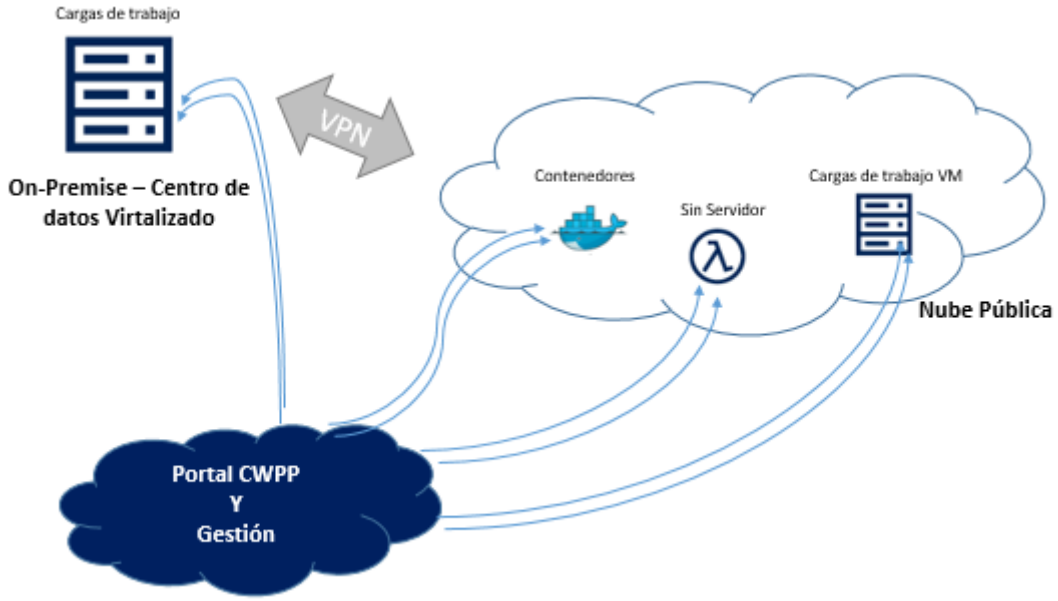


Figura 11. Uso de CWPP en nube híbrida

Algunas de las ventajas de la nube hibrida vienen dadas por el propio hecho de estar distribuida en distintos tipos de entornos o nubes. Vamos a introducirnos un poco más en el concepto de multinube, que también hemos comentado durante el proyecto.

4.2. Seguridad en multinube

La transición a la infraestructura multinube parece inevitable en todos los sectores. Asociarse con varios proveedores de nubes permite a las empresas personalizar en función de sus necesidades y evitar la dependencia de un servicio que tiene puntos fuertes, pero también puntos débiles.

Con el uso de multinube podemos mejorar la seguridad en:

- Evitar *riesgo* de proveedor único: ya con antelación hemos dedicado unas líneas a este *riesgo*. El uso de entornos multinube reduce la dependencia y mitiga los *Riesgos* asociados a trabajar con un único proveedor de servicios en la nube.

- Asegurar una alta disponibilidad para evitar interrupciones en el sitio web: por diseño, muchos de los servicios centrales con la nube pública y su infraestructura subyacente se replican en diferentes zonas geográficas. Esto ayuda a garantizar la

durabilidad y disponibilidad de sus datos y servicios y protege contra el tiempo de inactividad. Sin embargo, ocurren interrupciones. Para protegerse contra el costoso tiempo de inactividad, muchas empresas distribuyen sus servicios entre varios proveedores para reducir las posibilidades de fallas.

- Desarrollar un plan más sólido de protección de datos y mitigación de *riesgos*: en caso de pérdida de datos causada por un error humano de su parte, un ataque malintencionado u otros incidentes, sus opciones de recuperación dependen de la estrategia de backup y ésta puede aprovechar las ventajas de multinube, aumentando la seguridad de tener los datos a recuperar.

- Seguir las reglas de cumplimiento específicas de cada región: en las soluciones multinube tienes más posibilidades a la hora de elegir región y por lo tanto seguir las reglas de cumplimiento correspondientes.

Como nos ocurría con la nube hibrida, al utilizar entornos multinube mitigamos algunas de las *amenazas* y *riesgos* vistas con anterioridad.

Haciendo referencia al apartado anterior, ésta sería una posible integración a alto nivel de multinube:

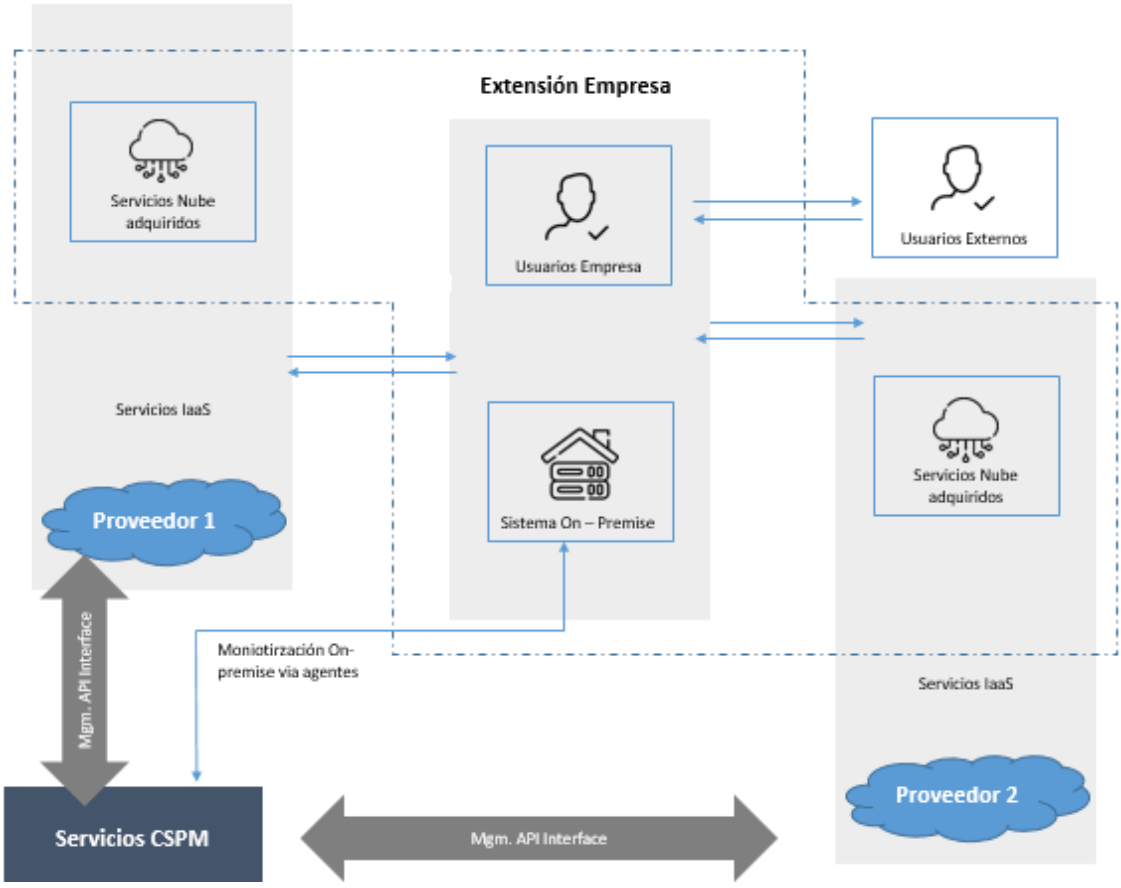


Figura 12. Uso de CSPM en Multinube

En ambos casos, nube hibrida y multinube, podemos ver el uso de plataformas que permiten administrar las diferentes nubes o entornos de una manera centralizada, reduciendo la complejidad de gestión.

Claramente en el contexto actual, los *CPDs* corporativos han quedado atrás frente a las posibilidades que ofrecen las plataformas globales de última generación, aunque, como comentábamos, no siempre la solución puede ser la nube. Ya sea por motivos de negocio, privacidad u otras razones, el mercado apunta hacia soluciones concretas que cubran a la perfección cada una de sus necesidades específicas en cuanto a gestión de TI, y esta flexibilidad solo se encuentra en las soluciones híbridas y multinube. La seguridad debe evolucionar para poder dar respuesta a todo este abanico de opciones que permita la versatilidad que necesitan las compañías para hacer crecer sus negocios.

Seguridad y mitigación de *riesgos* y *amenazas*

Con el uso de nube hibrida y multinube se ayuda a mitigar *riesgos* como concentración en proveedor único, indisponibilidad del servicio en caso de desastre o incidente, pudiendo tener los datos y aplicaciones en varias localizaciones y varios proveedores, o protección de datos, pudiendo tener los datos y aplicaciones críticas en local.

Principales *amenazas* y *riesgos* mitigados:

- 2.3.2.2. Incumplimiento normativo.
- 2.3.2.3. Desconocimiento de la localización de los datos.
- 2.3.2.7. Concentración de proveedor único.
- 2.3.2.5. Indisponibilidad del servicio en caso de desastre o incidente.
- 2.3.2.8. Falta de protección de datos.

Hemos visto como nos ayuda la nube hibrida para mitigar algunos *riesgos* y *amenazas* comentados en apartados anteriores. Pero no podemos finalizar sin también exponer algunos retos de seguridad que presentan estos tipos de entorno:

- Protección de datos: los datos pueden estar en tránsito o en reposo, lo que implica que se deben implementar mecanismos de seguridad en ambos estados. Encontrar formas de limitar la exposición de los datos a través del cifrado también es un asunto importante principalmente en modelos de nube híbridos.

- Cumplimiento: Verificar que los entornos distribuidos están acordes a las normas vigentes, y cumplir las reglas que indican que determinados tipos de datos deben mantenerse en la infraestructura de nube privada o contar con accesos restringidos a determinados perfiles tiene su complejidad.

- Gestión de incidentes: las organizaciones deben trabajar con el proveedor de nube para resolver el problema, a menudo con complicaciones añadidas como,

por ejemplo, inconvenientes de privacidad de datos, análisis insuficiente de registros o falta de definición precisa o conjunta de lo que es entendido como incidente. Si añadimos a la ecuación a varios proveedores la complejidad aumenta.

- Aplicación de la seguridad: cuando las aplicaciones están distribuidas en un entorno híbrido, las empresas tienen dificultades para tener visibilidad de toda la infraestructura. Por lo tanto, es un reto es hallar el servicio o plataforma que les permita una supervisión integral, combinando diferentes funciones.

5. Conclusiones y trabajos futuros

5.1. Conclusiones

Con la migración de las aplicaciones empresariales a la nube pública y con organizaciones cuyas implementaciones son cada vez más nativas, el uso de la nube se está disparando. La computación en la nube está todavía en una fase de crecimiento acelerado y cada vez son más las empresas que lo utilizan por sus diversas ventajas como flexibilidad, escalabilidad y agilidad, entre otras. A medida que evoluciona su uso, el número *amenazas* y *riesgos* en torno a la nube pública va incrementándose.

La seguridad de la información representa una prioridad para la mayoría de compañías, además de la capacidad de almacenar grandes volúmenes de datos de manera integral y confiable. La seguridad se ha convertido en un factor limitante que determina la decisión de uso de la nube. Por este motivo, los proveedores de computación en la nube están en continua evolución para facilitar cada vez mejores garantías de protección para las amenazas y los riesgos que se presentan.

Como podíamos esperar, son muchas las *amenazas* y los *riesgos* que se deben mitigar. Las compañías difícilmente encuentran perfiles con experiencia y conocimientos profundos en el área de la nube y menos aún en el área de seguridad. Son pocos y muy demandados lo que complica aún más el escenario. Para mi sorpresa muchas de las *amenazas* y *riesgos* vienen originados por la mala configuración de los servicios y las herramientas, consecuencia directa de lo que acabamos de comentar. Se estima que un porcentaje muy alto de organizaciones tienen configuraciones incorrectas en la nube que podrían ser aprovechadas por atacantes maliciosos.

No existe una arquitectura única, cada compañía debe diseñar aquella que más se adapte a su negocio. Los proveedores de la nube ponen a disposición distintos modelos para que las organizaciones puedan realizar sus diseños apoyándose en nubes hibridas y/o multinube si es necesario, con el objetivo de cumplir todos los requerimientos. En estos diseños cobra gran importancia la seguridad.

La implantación de los servicios y herramientas de seguridad debe mitigar y solucionar las *amenazas* y los *riesgos* ligados a la nube, desde una mala configuración, a un acceso no permitido o un incumplimiento legal.

En este TFM se ha presentado un diseño de seguridad para los distintos modelos de computación en nube que ayudará a las empresas a protegerse de las principales *amenazas* y *riesgos*. Se han mostrado diferentes herramientas y proveedores para su implantación y cumpliendo, logrando el objetivo propuesto de generar una guía para aumentar la seguridad de las empresas y sus activos.

Se ha realizado siguiendo la metodología y la planificación estimada, sin grandes cambios a lo considerado en el comienzo del proyecto. En algunos momentos hemos podido

perder el foco sobre la base, amenazas y riesgos, pero finalmente hemos conseguido reconducirlo para obtener el resultado esperado.

5.2. Trabajos futuros

Este TFM deja varias líneas abiertas para trabajos futuros como la profundización en la operación de la seguridad o en el detalle de nubes hibridas y multinubes, donde se podrán hacer diferentes diseños para adaptarlos a las compañías y sus negocios.

La nube tiene todo un futuro por delante y es un hecho que está marcando la pauta sobre cómo las empresas y los usuarios operarán en las siguientes décadas. La seguridad en la nube seguirá evolucionando y cambiando, generando nuevas líneas de trabajos alrededor de las *amenazas* y los *riesgos* que vayan apareciendo.

6. Glosario

Amenaza: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas.

CSA (Cloud Security Alliance): Organización sin ánimo de lucro que tiene por objetivo "promover el uso de las mejores prácticas para ofrecer garantías de seguridad en la computación en la nube, y proporcionar educación sobre sus usos para ayudar a asegurar todas las otras formas de informática".

Top threats to Cloud Computing: Informe emitido por CSA donde se presentan las principales amenazas en computación en la nube según los expertos en seguridad de la munidad CSA. El último informe fue publicado en 2022.

CSP (Content Security Policy): es una capa de seguridad adicional que ayuda a prevenir y mitigar algunos tipos de ataque, incluyendo Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques son usados con diversos propósitos, desde robar información hasta la desfiguración de sitios o distribución de malware.

APT (Advanced Persistent Threa): una amenaza persistente avanzada o APT, es un tipo de ciberataque a gran escala, que tiene como objetivo el robo de datos a empresas u organismos públicos o llevar a cabo el espionaje de sus sistemas. Es un ataque a largo plazo y un ataque complejo, que emplea diferentes tipos de recursos y frentes para llevarse a cabo.

Riesgo: Posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños. Para medir el riesgo de un sistema informático se debe asumir que existe una vulnerabilidad ante una amenaza. El riesgo es, por lo tanto, la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad existente.

SLA (Service Level Agreement): Acuerdo de nivel de servicio o Garantía de nivel de servicio. Se trata de un contrato firmado entre las partes involucradas en una negociación que determina cuáles son las responsabilidades de cada uno en relación a los servicios contratados.

TI (tecnología de la información): Conjunto de recursos tecnológicos como hardware, software y servicios, que proporcionan una plataforma para almacenar, recolectar, procesar y distribuir información.

PaC (Policy as Code): Política como código es la representación de políticas y regulaciones como código para mejorar y automatizar la aplicación y gestión de políticas.

GDPR (General Data Protection Regulation): Reglamento general de Protección de datos. Es una ley creada por la Unión Europa para garantizar la protección y la privacidad de los datos de los usuarios.

CPD (Centro Procesamiento Datos): instalación que centraliza las operaciones y la infraestructura de TI de una organización, en la que se almacenan, procesan, tratan y difunden datos y aplicaciones.

EDR (Endpoint Detection and Response): solución de seguridad diseñada para detectar y bloquear amenazas a nivel de dispositivo.

IaaS (Infraestructure as a Service): modelo de servicio en nube que ofrece a los usuarios la virtualización, el almacenamiento, la red y los servidores a petición, siendo pago por uso.

PaaS (Platform as a Service): modelo de servicio en nube que ofrece como servicio un entorno de desarrollo e implementación completa en la nube. el proveedor aloja el hardware y el software en su propia infraestructura y ofrece la plataforma al usuario como una solución integrada.

SaaS (Software as a Service): modelo de servicio en nube que ofrece ofrece una aplicación integral que gestiona el proveedor, a través de un explorador web.

FaaS (Function as a Service): modelo de servicio en la nube que permite que los desarrolladores diseñen, ejecuten y gestionen paquetes de aplicaciones como funciones sin tener que ocuparse del mantenimiento de su propia infraestructura.

IAC (Infrastructure as Code): permite gestionar y preparar la infraestructura a través del código, en lugar de hacerlo mediante procesos manuales.

RASP (Runtime Application Self Protection): es una de las tecnologías más modernas para la protección de aplicaciones web. Protege las aplicaciones en tiempo de ejecución y desde el interior. Tiene una visibilidad mucho mejor del flujo de datos y las consecuencias de cada entrada que recibe la aplicación.

DDOS (Distributed Denial of Service): es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

SIEM (Security Information and Event Management): sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos.

SOAR (Security Orchestration Automation and Response): plataforma de operaciones y generación de informes de seguridad que utiliza datos extraídos de distintas fuentes para proporcionar capacidades de gestión, análisis y generación de informes en apoyo a los equipos analistas en un SOC.

7. Bibliografía

[1] Plain Concepts; Cloud Computing y la tecnología sostenible; < Cloud Computing y la tecnología sostenible - Plain Concepts>

[2] CSA; Cloud Security Alliance's Top Threats to Cloud Computing; <Cloud Security Alliance's Top Threats to Cloud | CSA>

[3] INCIBE; Cloud Computing: una guía de aproximación para el empresario; <Cloud Computing: una guía de aproximación para el empresario | INCIBE>

[4] INCIBE; TemáTICas Cloud; <TemáTICas Cloud | INCIBE>

[5] INCIBE; TemáTICas: Seguridad en la nube; <TemáTICas: Seguridad en la nube | INCIBE>

[6] NIST; The NIST Deinition of Cloud Computing; <NIST SP 800-145, The NIST Definition of Cloud Computing>

[7] HashiCorp; HashiCorp State of Cloud Strategy Survey 2022: Multi-Cloud Is Working; <HashiCorp State of Cloud Strategy Survey 2022: Multi-Cloud Is Working>

[8] Gartner; How to Manage Concentration Risk in Public Cloud Services; <https://www.gartner.com/document/4073099?ref=solrAll&refval=362566386>

[9] Microsoft; Responsabilidad Compartida en la nube; <Responsabilidad compartida en la nube - Microsoft Azure | Microsoft Learn>

[10] Microsoft; Introducción al cumplimiento normativo; <Introducción al cumplimiento normativo - Cloud Adoption Framework | Microsoft Learn>

[11] Enisa; Cloud Computing risk assement; <Cloud-Computing-risk-assessment-spanish (europa.eu)>

[12] Google Cloud; ¿Qué es un plan de recuperación ante desastres?; <¿Qué es la recuperación ante desastres y por qué es importante? | Google Cloud | Google Cloud>

[13] INCIBE; Plan de contingencia y continuidad de negocio, ¿qué herramientas necesito?; <Plan de contingencia y continuidad de negocio, ¿qué herramientas necesito? | INCIBE>

[14] INTECO; *Riesgos* y amenazas en Cloud Computing; <*Riesgos* y amenazas en Cloud Computing (aeiciberseguridad.es)>

[15] Microsoft; Infraestructura como servicio; Infraestructura como servicio | Microsoft Azure

[16] AWS; Arquitectura de Seguridad de referencia; AWSArquitectura de referencia de seguridad (AWSSRA) - AWSGuía prescriptiva

[17] Azure; Servicios de Seguridad Azure; Documentación de los aspectos básicos de la seguridad en Azure | Microsoft Learn

[18] AWS; Servicios nube; Productos de seguridad, identidad y conformidad en la nube – Amazon Web Services (AWS)

[19] Azure; Servicios nube; Directorio de Azure Cloud Services | Microsoft Azure

[20] Google Cloud; Servicios nube; Productos de seguridad e identidad | Google Cloud

[21] Azure; WAF, Azure Web Application Firewall (WAF) | Microsoft Azure

[22] AWS; WAF; Firewall de aplicaciones web - Protección de API web - AWS WAF - AWS

[23] Google cloud; WAF; Descripción general de Google Cloud Armor | Google Cloud Armor

[24] Google cloud; WAAP; Protección de APIs y aplicaciones web (WAAP) | Google Cloud | Google Cloud

[25] Imperva; WAAP; What is Web Application and API Protection (WAAP)

[26] AWS; API Gateway; Amazon API Gateway | API Management | Amazon Web Services

[27] Azure; API Gateway; API gateway overview | Microsoft Learn

[28] Google cloud; API Discovery; Google API Discovery Service | Google Developers

[29] AWS; API Discovery; AWS Marketplace: TeejLab Inc. (amazon.com)

[30] AWS; CWP; Security Orchestration with Symantec Cloud Workload Protection and AWS Systems Manager | AWS Partner Network (APN) Blog (amazon.com)

[31] AWS; CWP; Cloud workload security (amazon.com)

[32] Microsoft; CWPP & CSPM; Microsoft Defender for Cloud - CSPM & CWPP | Microsoft Azure

[33] Gartner; CWPP; Cloud Workload Protection Platforms Reviews 2023 | Gartner Peer Insights

[34] Gartner; CSPM; Cloud Security Posture Management Tools Reviews 2023 | Gartner Peer Insights

[35] Microsoft; CASB; Microsoft Defender for Cloud Apps | Seguridad de Microsoft

[36] Oracle; CASB; ¿Qué es CASB? | Oracle España

[37] AWS; SIEM/SOAR; Integración con SIEM/SOAR :: Modelo de Madurez en Seguridad en AWS

[38] Google; Multinube; ¿Qué es la multinube? Definición y ventajas | Google Cloud

[39] Gartner; Nube hibrida; La guía del CIO para la nube distribuida