Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

ANÁLISIS DE LOS FACTORES CRÍTICOS Y BUENAS PRACTICAS DE SEGURIDAD PARA EL CONSUMO DE LOS SERVICIOS DE LA COMPUTACIÓN EN LA NUBE

Autor:

David Chacón Prieto

Director de la Tesis:

Mg. Marcia Maggiore

2020

Cohorte 2017

Declaración jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual".

_____

FIRMADO

David Chacón Prieto

DNI: 95.688.447

Resumen

En este documento de propósito investigativo se encuentran compiladas la descripción y análisis de los conceptos, riesgos y principales estándares de buenas prácticas de seguridad de la información en un entorno cloud. Asimismo, se propone una arquitectura de implementación en la nube y se crea un modelo de arquitectura de seguridad basado en patrones de diseño enfocados a garantizar la seguridad en cada componente y relación de la arquitectura propuesta, haciendo uso de los conceptos del marco metodológico brindado por el Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 [2] del Cloud Security Alliance (CSA) y el Guidelines on Security and Privacy in Public Cloud Computing - SP 800-144 [18] del National Institute of Standards and Technology (NIST).

Los documentos mencionados fueron usados como referencia y guía para analizar las similitudes y diferencias del análisis de seguridad en un entorno cloud. Posteriormente se definieron los puntos a considerar y los elementos a usar en el modelo de arquitectura de seguridad propuesto para el manejo de los posibles retos de seguridad de la información que se generan al consumir servicios en la nube.

Palabras Clave: Computación en la Nube, Amenaza, Vulnerabilidad, Incertidumbre, Riesgo, Patrones de Diseño, Arquitectura Computacional, Estándares de Buenas Practicas, Tecnología Informática, Información, Continuidad, Seguridad de la Información.

Índice General

Agradecimientos

Primero que nada, deseo expresar mi más grande agradecimiento a la docente, directora de esta tesis de maestría y hoy en día amiga, la Mg. Marcia Maggiore, por su colaboración y apoyo brindado en este proyecto, por su disposición a la resolución de dudas en este proceso y al respeto a mis propuestas e ideas. Por su rigor y detalle en pro de buscar siempre la mejora en todo sentido de esta labor realizada.

Todo trabajo con propósito investigativo es fruto de la colaboración y apoyo esencial que nos brindan las personas que nos aprecian, sin el cual no tendríamos la fuerza y energía que nos anima a crecer como personas y como profesionales. Gracias a mi familia, a mis padres y hermanos, ya que ellos son parte del motivo de estar siempre en busca del crecimiento personal y profesional.

Pero, sobre todo, gracias a mi novia, compañera de viaje en esta aventura de estudiar en el exterior, por su paciencia, comprensión y solidaridad con este proyecto. Sin su respaldo este trabajo nunca se habría escrito y, por eso, este trabajo es también el suyo.

A todos, muchas gracias.

1 - Introducción

Con el incesante auge de la computación en la nube, empresas de diferente índole ya consumen los servicios ofrecidos por esta tecnología, o bien planean consumirlos, para generar ventajas competitivas, simplificación de la gestión y reducción de los costos operativos relacionados con las tecnologías de la información. Con ello, se han generado nuevas amenazas y vulnerabilidades asociadas a este entorno, lo cual implica un cambio sustancial a la hora de afrontar los nuevos desafíos de la seguridad de la información.

Actualmente existen varias iniciativas sobre la seguridad de la información, las que brindan los lineamientos necesarios para el consumo de servicios en la nube de forma segura.

Una de ellas está a cargo del NIST [18], cuyos conceptos son ampliamente aceptados y conforman la base de un gran número de guías y estándares de buenas prácticas.

Mientras que otra de ellas es promovida por la CSA [2], organización europea líder a nivel mundial en la difusión y gestión de la seguridad de la información. Está conformada por especialistas en varias temáticas vinculadas a la seguridad. Esta entidad es conocida por su interacción en materia de seguridad con los grandes proveedores cloud y grandes clientes de diferentes industrias, así como con organismos gubernamentales. Mediante documentación, eventos, entrenamientos y certificaciones promueve la implementación de buenas prácticas de seguridad en entornos cloud.

Este trabajo se propone describir los elementos que hacen a la computación en la nube, los riesgos de seguridad asociados al consumo de estos servicios y la descripción de las principales guías de buenas prácticas de seguridad de la información en este ámbito.

A partir de esta labor, se plantea una arquitectura de implementación y un modelo de arquitectura de seguridad a dicha arquitectura que permita mediante la sugerencia de controles, buenas prácticas y lineamientos de

seguridad la aplicación del concepto seguridad de forma integral en un entorno cloud o la evaluación del entorno referente a seguridad.

2 - Marco Conceptual del Cloud Computing

Dependiendo de la perspectiva desde la cual se analice, cloud computing se puede definir de manera diferente. Desde un modelo de negocio, hasta una colección de tecnologías. Sin embargo, existen una serie de conceptos base que definen los aspectos más relevantes de este entorno. A continuación, se definirán los elementos que hacen a la computación en la nube, sus características y los diversos modelos que tiene para la prestación de los servicios que ofrece. Esto servirá como base conceptual para identificar las diferencias respecto de la computación tradicional y el manejo del correcto lenguaje en este entorno de trabajo. Así mismo, servirá como proceso introductorio para el análisis de los riesgos asociados.

2.1- Definición de Computación en la Nube

Existen varias definiciones de computación en la nube. La International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) en el estándar ISO/IEC 17788:2014 [4] proveen una visión general de computación en la nube junto con un conjunto de términos y definiciones, proporcionando así un vocabulario unificado para el resto de los estándares que traten sobre el tema. El mencionado estándar define la computación en la nube como: "*Paradigma para permitir el acceso de red a un conjunto de recursos compartidos, escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda*". En cambio el NIST, en el estándar SP 800-145 [17], la define de la siguiente manera: "*La computación en la nube es un modelo que permite el acceso ubicuo, conveniente y a demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo de esfuerzo de gestión o de interacción con el proveedor de servicios*".

Haciendo una abstracción de las definiciones previas, se puede definir la computación en la nube como un conjunto de tecnologías o modelo de negocio que brinda una gama importante de servicios a través de Internet y ofrece desde el acceso a recursos tecnológicos hasta aplicaciones personalizadas según las necesidades de los clientes y del negocio, basado en dos grandes ventajas, la fácil conectividad a nivel global y la escalabilidad. Esto le permite brindar fácil acceso a sus servicios y crear un modelo de negocio escalable y accesible para las pequeñas y medianas empresas, generando beneficios logísticos, de mantenimiento y económicos.

2.2- Participantes en el Modelo Cloud

Los principales actores en el entorno cloud son los **proveedores** y los **consumidores**. Una definición básica establece que el **proveedor** es quien se encarga de la entrega y gestión del hardware, recursos virtuales y servicios, mientras que el **consumidor** es quien solicita, usa y manipula los recursos de la nube.

Existen también otros actores intermedios asociados al ambiente cloud como lo son los auditores, operadores o los intermediarios de la nube. Asimismo, la ISO/IEC 17788:2014 [4] define una serie de roles como el de proveedor de servicios, servicio al cliente en la nube y socio de servicios en la nube. A continuación, se incluye una breve definición de los actores en la nube según el NIST [17].

- **Proveedor de la Nube**: Es la entidad que brinda los servicios en la nube. Dependiendo de los servicios ofrecidos, sus labores y responsabilidades en cada nivel son diferentes y generan diferente grado de compromiso. Se encarga de mantener los servicios ofrecidos a disposición de los interesados mediante el acceso a la red.
- **Consumidor de la Nube**: Son las entidades o personas que consumen los servicios ofrecidos por un proveedor en la nube. Sus actividades dependen de los servicios que utilice, en base a los cuales se establece una relación de negocio. De aquí en más utilizaremos lo términos usuario y cliente como sinónimo de consumidor.

- **Auditor de la Nube**: Es la persona o entidad que de forma independiente evalúa los controles implementados en la nube para la correcta y segura prestación de los servicios. Generalmente, el uso de pruebas de estos controles permite dar una valoración objetiva.

- **Broker de la Nube**: Son personas o entidades que funcionan como intermediarios entre el proveedor de la nube y el consumidor, administrando el uso, generando nuevos servicios, optimizando los recursos y servicios según la necesidad del usuario. Existen tres tipos de brokers: aquellas entidades que realizan la intermediación, la agregación o el arbitraje de los servicios.

- **Carrier de la Nube**: Son las entidades que permiten la conectividad y transporte de los servicios en la nube a través de la red, para su consumo eficiente, independientemente de la manera en la que se realice dicho consumo o los mecanismos que se usen para ello.

Se hace mención de estos como parte del contexto. Sin embargo, no se definen en profundidad debido a que no tienen mayor implicancia en el desarrollo de este documento.

A continuación, se presentará la definición de las principales características del entorno cloud.

2.3- Características

Es posible definir una amplia variedad de características de la computación en la nube. Sin embargo, ampliamente aceptadas son las citadas por el NIST [17], las cuales hoy en día son base de un gran número de guías y estándares de buenas prácticas, una de los cuales es la producida por el CSA [2]. El NIST [17] describe cinco características calificadas como esenciales:

- **Autoservicio Bajo Demanda**: Los usuarios pueden aprovisionarse recursos de cómputo de forma automática, sin dependencia del proveedor; convirtiéndolos así en los administradores de sus propios recursos.

- **Amplio Acceso a la Red**: Hace referencia a la capacidad de acceso a los recursos desde cualquier dispositivo conectado a Internet. Elimina la necesidad del acceso físico.

- **Agrupación de Recursos**: Los recursos informáticos (almacenamiento, procesamiento, ancho de banda, y más) son comunitarios, es decir, un mismo grupo de recursos configurado por el proveedor puede ser asignado a varios usuarios en la modalidad de Multi-Tenant[1]. Los recursos físicos o virtuales son aprovisionados y reasignados según la demanda del usuario.

- **Elasticidad Rápida**: Brinda la posibilidad a los usuarios de tomar o liberar los recursos fácilmente, con frecuencia de forma automática. Como la necesidad de recursos está directamente relacionada con la demanda, esta característica permite contar con recursos al instante y escalar fácilmente.

- **Medidores de Servicio**: Garantiza la correcta asignación de los recursos según lo configurado para su uso. Mediante los sistemas de control de la nube, se monitorea, controla, reporta y optimiza el uso de los recursos. Esto permite que el usuario solo pague por lo que usa.

Es posible definir otra serie de características que hacen a la computación y servicios en la nube. Sin embargo, en el marco de este documento se usarán las nombradas anteriormente.

[1] Multi-Tenant: Es la arquitectura de software multi-arrendatario, que permite a múltiples usuarios compartir una sola instancia de una aplicación de software y sus recursos subyacentes. Es la base de la mayoría de las ofertas de SaaS (Software as a Service).
En la arquitectura de software Multi-Tenant - también llamada Multitenancy de software - una sola instancia de una aplicación de software (y su base de datos y hardware subyacente) sirve a múltiples usuarios (o cuentas de usuario). Un usuario puede ser un usuario individual, pero con mayor frecuencia se trata de un grupo de usuarios -como una organización de clientes- que comparte un acceso común y privilegios dentro de la instancia de la aplicación. Los datos de cada inquilino están aislados de los demás inquilinos que comparten la instancia de la aplicación y son invisibles para ellos, lo que garantiza la seguridad y la privacidad de los datos de todos los inquilinos [36].

2.4- Modelo de Servicio

Los modelos de servicio del cloud computing se han desarrollado acorde a las necesidades de los usuarios, minimizando la carga laboral dedicada a temas como el mantenimiento, la planificación de capacidad y disponibilidad, aprovisionamiento y demás tareas asociadas, cubriendo diferentes niveles de administración, elasticidad y control. Hoy en día estos modelos ampliamente estandarizados y diferenciables entre sí, son el Software como Servicio, la Plataforma como Servicio y la Infraestructura como Servicio, (SaaS, PaaS e IaaS respectivamente por sus siglas en ingles). Estos pueden ser implementados estratégicamente como un conjunto de servicios o un híbrido de estos modelos según las necesidades del consumidor. A continuación, se describen los modelos de servicio, en base a las definiciones brindadas por el NIST [17].

- **Software como servicio (SaaS):** Ofrece al usuario el uso de aplicaciones del proveedor, que son administradas en su totalidad por este. Son accesibles mediante diversos recursos del cliente, como equipos móviles, navegadores, aplicaciones y demás.

- **Plataforma como servicio (PaaS):** Brinda la plataforma necesaria para la implementación de aplicaciones (propietarias o no), almacenamiento de datos, bases de datos, soluciones para el desarrollo de aplicaciones, y más, haciendo uso de herramientas soportadas y gestionadas por el proveedor. En este modelo se permite la personalización de la configuración de las plataformas según sea la necesidad de la aplicación desplegada por el usuario.

- **Infraestructura como servicio (IaaS):** Modelo de servicio que permite al usuario la manipulación de recursos informáticos como procesamiento, almacenamiento, redes y otros esenciales en los que este puede implementar y ejecutar software a su consideración. Permite la gestión de los sistemas operativos, el almacenamiento y las aplicaciones instaladas. En algunos entornos, también se permite la gestión limitada de algunas funcionalidades de red como el firewall del host.

En la siguiente gráfica se muestra la relación entre los diferentes servicios ofrecidos por los modelos descritos anteriormente, el modo de acceso (Internet) y las diferentes modalidades de acceso para el consumo de estos servicios, incluidos en el círculo denominado clientes cloud.

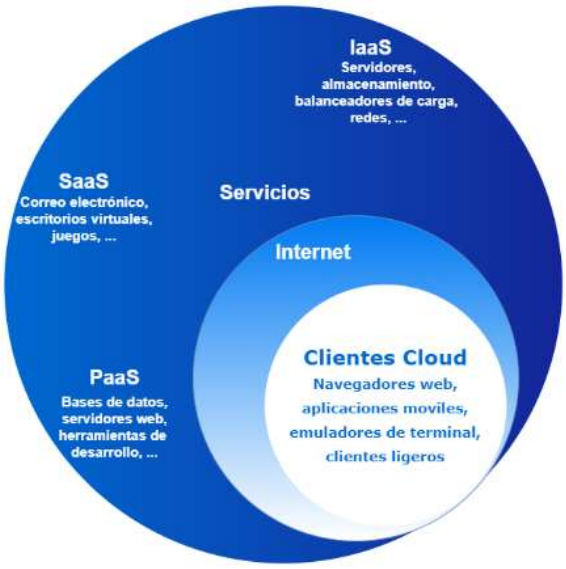

Ilustración 1: Ejemplos de Servicios de los diferentes modelos de servicio de la nube. Fuente: [23]

Para entender mejor las diferencias entre los mencionados modelos, en base a la gestión que es posible realizar y las responsabilidades que esto conlleva, en el siguiente gráfico se muestran las distintas responsabilidades que adoptan el proveedor y el consumidor.

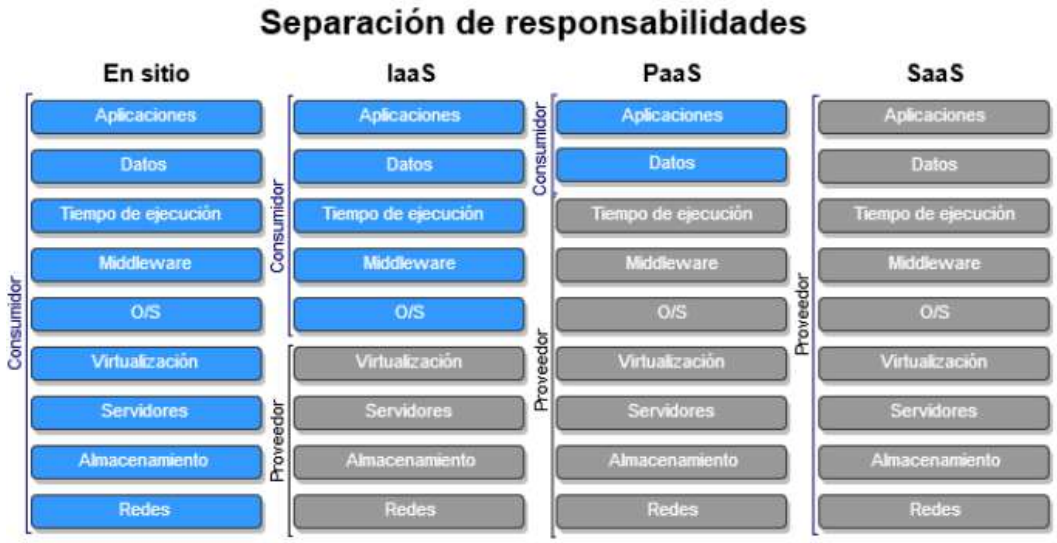

Ilustración 2: Segregación de responsabilidades a partir del modelo de servicio. Fuente: [23]

A partir de esta definición gráfica, se puede ver la evolución entre los diferentes modelos de servicio y cómo en cada uno de ellos la brecha de responsabilidades entre consumidor y proveedor es más notoria e importante.

El modelo “En sitio” u On-Premise, hace referencia al denominado hace unas décadas atrás, modelo estándar de servicio, ampliamente usado y hasta hoy vigente. En este modelo toda la infraestructura, componentes, plataformas, aplicaciones y servicios se instalan en una propiedad del consumidor y son su responsabilidad. De la misma manera lo son, los procesos, procedimientos y actividades asociados a los diferentes niveles de gestión.

En cambio, al hacer uso de los modelos de servicio ofrecidos por la nube, podemos identificar cómo la segregación de responsabilidades es más evidente. En el modelo IaaS, el consumidor no gestiona ni controla la infraestructura base que permite este servicio, ya que estas tareas son realizadas por el proveedor.

En el modelo PaaS, el proveedor toma aún más relevancia, controlando y administrando toda la base de la infraestructura, en donde el usuario solo es responsable de la gestión de los datos y las aplicaciones.

Por último, en el modelo SaaS, el consumidor pierde toda responsabilidad de gestión y control, siendo el proveedor el máximo responsable de cualquier suceso en este entorno.

Entender esta jerarquía de responsabilidades no es menor y se debe tener en cuenta a la hora de comprender las implicancias que conllevan para la gestión de la seguridad en entornos cloud; tema que se desarrollará con más detalle en los siguientes apartados de este documento.

2.5- Modelo de Despliegue

Los diferentes modelos de despliegue, también llamado de implementación, que usa la nube representan un tipo específico de entorno a partir de sus características y funcionalidades. Actualmente se consideran cuatro modelos de despliegue. Estos se diferencian principalmente por el tamaño de la infraestructura, el tipo de acceso a esta y su pertenencia.

En cualquier modelo de despliegue se puede implementar cualquiera de los modelos de servicio vistos anteriormente. A continuación, se realiza una breve descripción de cada modelo de despliegue, a partir de las definiciones brindadas por el NIST [17].

- **Nube Pública**: Es de acceso al público en general, en base a su red abierta. Su infraestructura, labores de mantenimiento, administración y gestión de los recursos son responsabilidad de los proveedores del servicio. Los servicios ofrecidos en este modelo pueden ser pagos o gratuitos. A partir de sus capacidades escalables y elásticas brinda toda clase de beneficios según la necesidad del usuario.

- **Nube Privada**: Como lo dice su nombre, es de uso y propiedad privada, orientada a la prestación de servicios exclusivos para una organización, por lo cual las actividades de operación, mantenimiento y administración de la nube son responsabilidad de dicha organización. Usualmente estas labores son tercerizadas y su locación puede o no estar en las instalaciones de las organizaciones.

- **Nube Comunitaria**: Las tecnologías de la información cloud brindan servicio a un grupo o comunidad de organizaciones que usualmente comparten necesidades similares como consideraciones legales, de cumplimiento, requisitos de seguridad y más. Esta comunidad se encarga de las actividades de gestión de la infraestructura, ya sean delegadas a un tercero o no. Pueden estar localizadas en las instalaciones de una o algunas de las entidades que conforman la comunidad, aunque no necesariamente debe ser de esta manera.

- **Nube Híbrida**: Hace referencia a los entornos cloud que están constituidos por uno o más modelos de despliegue. También, pueden coexistir diferentes proveedores de servicios en la nube según las necesidades del consumidor. En este modelo es imprescindible contar con la portabilidad de las aplicaciones y los datos. Haciendo uso de tecnologías patentadas o estándares para esto, se genera un equilibrio de la carga entre las diversas nubes. Otra definición para el término hibrido según el CSA [2], refiere a la conexión directa entre proveedores en la nube y los centros de datos físicos que no forman parte de la nube.

Para el CSA [2], los modelos de implementación de las tecnologías de la nube están definidos en base a qué tipo de usuario es el que las usa, ya que el resto de las características (el propietario, el tipo de gestión, si se ubica “en sitio” o es externa, etc.) pueden variar aún en un mismo modelo.

Ilustración 3: Modelos de despliegue según el usuario de la nube. Fuente: [2]

La ilustración anterior muestra que, para la nube privada y la comunitaria, su localización y las labores anteriormente nombradas pueden ser compartidas entre los clientes y el proveedor. En base al tipo de usuario que consume los servicios es definido como confiable. Es decir, según el punto cuatro (4) de la ilustración, los usuarios son parte del alcance legal / contractrual / político de una organización, incluidos empleados, contratistas y socios comerciales.

En la nube pública, debido a la naturaleza de su modelo, la propiedad de su infraestructura es de un proveedor externo, el cual se encarga de todas las labores de mantenimiento, seguridad, gestión y demás que demanda la solución cloud. Su localización es de propiedad de dicho proveedor como el control total de los recursos tecnológicos (telecomunicaciones, dispositivos de almacenamiento, centros de datos, etc.) y por el tipo de usuario que consume sus servicios, se define como no confiable. Es decir, según el punto 4 de la Ilustración 3, están autorizados para consumir algunos/todos los servicios, pero no son extensiones lógicas de la organización.

En cambio, la nube híbrida, en función de la definición de tipo de usuario ya mencionada, se considera confiable y no confiable.

2.6- Modelo Lógico

Según el CSA [2], el modelo lógico de la nube es la forma en la cual se logra identificar diferentes modelos de computación. Se basa en cuatro definiciones para la identificación de funciones.

- **Infraestructura**: Refiere a los elementos esenciales para el funcionamiento de un sistema computacional.
- **Meta-estructura**: Corresponde a la forma de comunicación y los elementos de uso para el enlace entre el nivel de infraestructura y los demás niveles.
- **Apli-estructura**: Son las aplicaciones, servicios y funcionalidades implementadas en la nube más funciones tales como análisis de datos, gestión de notificación, manejo de colas de datos, entre otras, integradas para su correcto funcionamiento.
- **Info-estructura**: La información y los datos independientemente de su formato.

2.7- Modelo de Arquitectura

Este tópico, de orden técnico, brinda las bases de la arquitectura en la nube. El conjunto de elementos que hacen al entorno cloud, usualmente es visto como una pila, donde desde su infraestructura física hasta las aplicaciones y los datos están dispuestos para que en cada nivel interactúen diferentes componentes y así mismo se brinden los diferentes servicios. Esa pila se divide en tres niveles: el de recursos físicos, el de abstracción y control, y el de servicio, como se puede ver en la ilustración siguiente.

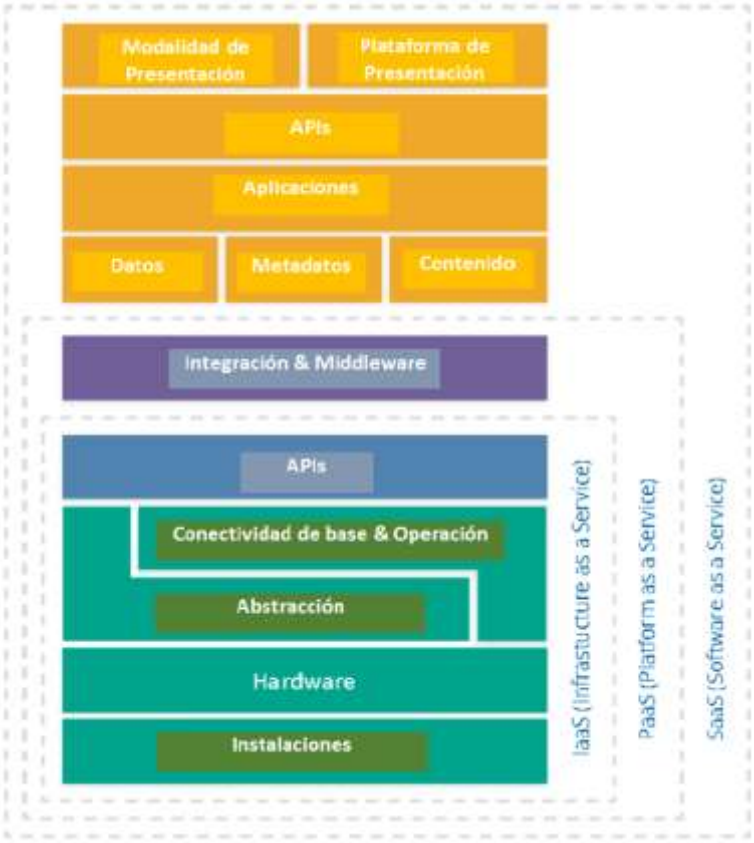

Ilustración 4: Servicio de Orquestación. Fuente: [2]

Cuenta con una interface para cada modelo de servicio y todas las secciones están estrechamente interrelacionadas. Sin embargo, existen entre ellas fronteras de control y acceso, tal como se muestra en el gráfico anterior.

En la base de la pila se encuentran los recursos físicos como el almacenamiento, los recursos de hardware, redes y otros elementos de la infraestructura. Estos se encargan de brindar los recursos de cómputo necesarios que sostienen a los entornos cloud.

Por encima de la capa de hardware, el nivel de abstracción y control es el que se encarga de la gestión y acceso de los recursos físicos. Mediante software orientado a la gestión de recursos, se realiza la abstracción de los recursos de cómputo y se los presenta de forma virtualizada para que puedan ser consumidos por el nivel siguiente. Aquí se emplean y generan elementos de software como dispositivos de red y

almacenamiento virtuales, máquinas virtuales, hypervisores[2] y otros más. En esta sección se lleva a cabo el proceso de control de los recursos físicos, aprovisionamiento dinámico, monitoreo y métricas de uso. Los recursos físicos más el software de gestión conforman el modelo IaaS.

Por arriba de este agrupamiento de capas, se integran plataformas de desarrollo de aplicaciones, motores de base de datos, funciones y funcionalidades, y en sí un amplio uso de middleware[3] que permiten la creación de nuevas soluciones informáticas. En conjunto con los recursos físicos y el software de gestión ya mencionados conforman el modelo PaaS.

En el extremo superior de la pila se encuentran las aplicaciones y datos. Al agregar este nivel la nube conforma el modelo de servicio SaaS.

Específicamente hablando de IaaS, los componentes fundamentales son las API´s[4]. Permiten a los usuarios, la gestión y configuración de sus recursos concediendo la posibilidad de la creación de entornos virtualizados. Aquí existe un punto de control fundamental, ya que estas API´s deben ser seguras para evitar cualquier incidente de seguridad que permita a un tercero acceder a la administración de sus implementaciones.

En un siguiente paso, PaaS hace uso también de API´s para la comunicación con el usuario. Sin embargo, haciendo uso de middleware, se hace la abstracción en un nivel más alto. Se pone a disposición del usuario el software y las herramientas necesarias generando la plataforma para el desarrollo de sus actividades sin tener que preocuparse por el entorno virtual subyacente, ya que el usuario no tiene acceso a la infraestructura y así mismo no tiene que gestionarla.

---

[2] Hypervisor (Monitor de máquina virtual): Es un software utilizado para poder ejecutar distintos sistemas operativos en un mismo ordenador y al mismo tiempo, utilizando para ello técnicas de virtualización [49].

[3] Middleware: Es un software que se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él. Básicamente, funciona como una capa de traducción oculta para permitir la comunicación y la administración de datos en aplicaciones distribuidas [40].

[4] API (Application Programming Interface): El concepto hace referencia a los procesos, las funciones y los métodos que brinda una determinada biblioteca de programación a modo de capa de abstracción para que sea empleada por otro programa informático. Es la forma como las aplicaciones pueden mantener una comunicación entre sí. Estas permiten que los distintos programas mantengan interacciones [43].

En última instancia, SaaS es la disposición de aplicaciones que pueden ser consumidas desde diferentes clientes como aplicaciones móviles, navegadores web, dispositivos específicos y más. En este punto el usuario solo hace consumo de las aplicaciones ofrecidas, muchas veces interrelacionando diferentes proveedores de entornos en la nube. Haciendo uso de nuevo de API´s públicas, permite la comunicación y acceso de los datos de forma inmediata.

3 - Riesgos del Cloud Computing

3.1- Definición de Términos

A continuación, se definirán los términos más relevantes a la hora de trabajar con riesgos de seguridad de la información. Esto permitirá definir un contexto y un lenguaje en común en pro de evitar inconvenientes de interpretación, así como facilitar la comprensión y desarrollo de este tópico.

- Objetivo: Resultado que debe alcanzarse. (ISO/IEC 27000:2018 [7])
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con su tratamiento (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.
- Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 27000:2018)
- Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización. (ISO/IEC 27000:2018)
- Consecuencia: Resultado de un acontecimiento que afecta a los objetivos (ISO Guide 73:2009 [6]). Una consecuencia puede ser cierta o incierta y, en el contexto de la seguridad de la información, suele ser negativa. (ISO/IEC 27000:2018)
- Probabilidad (likelihood): Posibilidad de que algo suceda. (ISO Guide 73:2009)
- Riesgo: Efecto de la incertidumbre sobre los objetivos. (ISO Guide 73:2009) El riesgo se caracteriza a menudo por la referencia a "acontecimientos" potenciales (tal como se definen en la Guía ISO 73:2009, 3.5.1.3) y "consecuencias" (tal como se definen en la Guía ISO 73:2009, 3.6.1.3), o una combinación de los mismos.
- Apetito de Riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a buscar o retener.
- Nivel de Riesgo: Magnitud de un riesgo o combinación de riesgos, expresada en términos de la combinación de consecuencias y su probabilidad. (ISO Guide 73:2009)

- Riesgo Residual: Riesgo remanente después de su tratamiento. (ISO Guide 73:2009)
- Control: Medida para modificar el riesgo (ISO Guide 73:2009). Puede incluir políticas y procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal.
- Confidencialidad: Propiedad de la información que indica que solo se pone a disposición de individuos, entidades o procesos autorizados. (ISO/IEC 27000:2018)
- Integridad: Propiedad de exactitud y completitud. (ISO/IEC 27000:2018)
- Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (ISO/IEC 27000:2018)

3.2- Vulnerabilidades y Amenazas del Cloud Computing

En todo entorno tecnológico se presentan desafíos a nivel de seguridad de la información que deben ser tratados. La gestión de riesgos permite identificar, analizar y responder a los riesgos que pueden afectar a la seguridad de la información y en beneficio de objetivos establecidos por cualquier entidad que desee conocer y tratar sus riesgos. Esto implica actuar de una forma preventiva, donde se busca tener el conocimiento y los recaudos necesarios al presentarse una eventual materialización del riesgo y minimizando en lo posible acciones reactivas. Teniendo en cuenta lo anterior, se deben conocer las vulnerabilidades y amenazas asociadas con la computación en la nube para poder implementar los controles necesarios para la mitigación de los riesgos. El entorno cloud presenta riesgos particulares asociados a los factores y características que hacen a estas tecnologías. A continuación, en base a las iniciativas del CSA [2] y el NIST [18], se describirán los principales riesgos de seguridad de la información en el entorno cloud.

3.2.1- Riesgos Descritos por el NIST

Una vista diferente y con un enfoque más normativo de los principales riesgos a nivel de seguridad de la información es brindada por el NIST [18] el cual describe los aspectos críticos de seguridad a tener en cuenta en un ambiente cloud. Esta organización a nivel de seguridad de la computación en la nube tiene como objetivo generar la innovación, creación y adopción de estándares para apoyar a la industria de los Estados Unidos. Trabajando colaborativamente con las principales entidades y organismos gubernamentales en la creación de estándares y buenas prácticas, ha generado una serie de documentos y modelos en los cuales se definen los elementos que componen la nube y se describen en detalle los riesgos. Asimismo, ha impulsado el uso de esta documentación para la implementación de soluciones seguras en la nube.

Su visión se basa en que el continuo crecimiento y la combinación de diferentes tecnologías hacen que esta nueva tendencia tecnológica presente retos antes no conocidos y que, con su constante evolución y cambio, aparezcan diferentes mecanismos de explotación de vulnerabilidades y nuevas amenazas en el ámbito de la seguridad de la información. El hecho de que la nube esté conformada por una amalgama de tecnologías ya existentes hace creer falsamente que sus debilidades y fortalezas ya son conocidas. Sin embargo, sus nuevas configuraciones y combinaciones dan paso a nuevos riesgos antes no contemplados.

Es aquí donde el NIST [18] brinda una visión integradora de este nuevo paradigma, buscando que no se reste importancia a la gestión del riesgo. Inicialmente describiendo todos los aspectos que hacen a la nube digital y posteriormente definiendo claramente roles y responsabilidades entre los diferentes actores. Es para este organismo muy importante que se entienda que la tercerización de los servicios de cómputo no equivale a una tercerización de la responsabilidad y gestión del riesgo. Sino a una responsabilidad incluso mayor, dependiendo del modelo de servicio y de despliegue que se adopte, ya que es posible la aparición de riesgos antes inexistentes en una arquitectura en sitio. A continuación, se listan lo que el NIST [18] denomina temas claves de seguridad y privacidad.

- Falta de Gobernanza.
- Riesgo de Cumplimiento.
- Exceso de Confianza.
- Propiedad de los Datos.
- Complejidad en los Servicios.
- Carencia de Visibilidad.
- Datos Auxiliares.
- Falta de la gestión de los riesgos.
- Problemas de Arquitectura.
- Superficie de ataque.
- Protección de Redes Virtuales.
- Definición de Roles Operativos.
- Imágenes de Máquinas Virtuales.
- Protección del lado del Cliente.
- Protección del lado de los Servidores.
- Problemas de Identidad y Control de Acceso.
- Aislamiento del Software.
- Protección de los Datos.
- Problemas de Disponibilidad.
- Respuesta a Incidentes.

La información detallada de los anteriores tópicos se encuentra descrita en el Anexo A de este documento.

3.2.2- Amenazas, Vulnerabilidades y Riesgos Descritos por CSA

El CSA ha publicado por varios años, diferentes informes sobre las amenazas asociadas a la nube. Con ello busca generar conciencia y mostrar la necesidad de preservar la seguridad de la información en los ambientes cloud, a partir de estudios de investigación enfocados en los principales peligros que genera el uso de estas tecnologías. A continuación, se listan amenazas descritas por el CSA en su último informe llamado Top Threats to Cloud Computing - The Egregious Eleven [1], en el cual compila las principales amenazas, vulnerabilidades y riesgos en la nube.

- Brecha de Datos.
- Problemas de Configuración e Inadecuado Control de Cambios.
- Falta de Estrategia y Arquitectura de seguridad en la Nube.
- Insuficiente gestión de identidades, credenciales, acceso y claves.
- Secuestro de Cuentas.
- Amenazas Internas.
- API´s Inseguras.
- Plano de Control Débil.
- Fallas en la Meta-estructura y la Apli-estructura.
- Visualización Limitada del Uso de la Nube.
- Abuso e Inadecuado Uso de los Servicios en la Nube.

La información detallada de cada una de las amenazas y sus respectivas recomendaciones para su tratamiento, se encuentran descritas en el Anexo A.

4 - Temas Clave de la Seguridad en la Nube

Como se vio anteriormente, si bien muchas de las vulnerabilidades, amenazas y riesgos asociados a los entornos en la nube suelen tener algún tipo de relación con lo ya conocido en la infraestructura tradicional, los múltiples elementos que hacen a esta tecnología generan nuevos desafíos y otros grados de complejidad.

En función de ello, es necesario conocer los modelos de seguridad dedicados a satisfacer esta necesidad para garantizar y salvaguardar los activos de los clientes, así como de los proveedores, mitigando los riesgos en la nube. Esto ayudará a tomar decisiones de negocio correctas y alineadas con los objetivos corporativos.

En este sentido, se debe entender que, respecto de la seguridad de la información en los entornos cloud, además de trabajar en temas como la seguridad física y lógica, también se deben abordar los temas legales y de gobierno. Temas de gran importancia y esenciales para garantizar la seguridad de los servicios contratados. Como es notorio, la seguridad en la nube es un campo de trabajo amplio y con varias aristas que deben ser trabajadas minuciosamente para dar respuesta a las necesidades anteriormente planteadas.

Para ello existen modelos, estándares de buenas prácticas y marcos de referencia que sirven como guía a la hora de pensar en la seguridad en la nube. Haciendo uso de estas normativas, se puede generar un plan según los objetivos propuestos. Sin embargo, el primer paso para abordar este reto es entender los alcances, limitaciones y roles según el modelo de servicio contratado. A continuación, se definirán algunos puntos claves para abordar el entendimiento de la seguridad de la información en la nube.

4.1- Roles y Responsabilidades en Entornos Cloud

Las funciones y responsabilidades que tienen cada una de las partes, en este caso el cliente y el proveedor de servicios en la nube, dependen de si se contrata software como servicio (SaaS), plataforma como servicio

(PaaS), infraestructura como servicio (IaaS) o algunas de sus variantes, donde cada una tiene diferentes alcances y limitaciones. A continuación, se hace referencia a la distribución de responsabilidades propuesta por ENISA (European Network and Information Security Agency) en su documento llamado “Computación en la nube - Beneficios, riesgos y recomendaciones para la seguridad de la información” [59] según el modelo de servicio adquirido:

Software como Servicio (SaaS)	
Cliente	**Proveedor**
Cumplimiento de la normativa vigente de protección de datos con respecto a los datos de cliente recabados y procesados	Gestión de la infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)
Mantenimiento del sistema de gestión de identidades	Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)
Administración del sistema de gestión de identidades	Gestión de parches del sistema operativo y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor)
Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)	Configuración de la plataforma de seguridad (políticas del firewall, ajuste de sistemas de detección y protección de intrusos, etc.)

Tabla 1 - Fuente: ENISA - Distribución de responsabilidades para Software como Servicio (SaaS). [59]

Plataforma como Servicio (PaaS)	
Cliente	**Proveedor**
Mantenimiento del sistema de gestión de identidades	Gestión de la infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)
	Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)
Administración del sistema de gestión de identidades	Gestión de parches del sistema operativo y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor)

Plataforma como Servicio (PaaS)	
Cliente	**Proveedor**
	Configuración de la plataforma de seguridad (políticas del firewall, ajuste de sistemas de detección y protección de intrusos, etc.)
	Monitoreo y supervisión de los sistemas.
Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)	Mantenimiento de la plataforma de seguridad (firewalls, sistemas de detección y protección de intrusos, antivirus, antimalware, antibots, filtrado de paquetes)
	Captura de registros y control de la seguridad

Tabla 2 - Fuente: ENISA - Distribución de responsabilidades para Plataforma como Servicio (PaaS). [59]

Infraestructura como Servicio (IaaS)	
Cliente	**Proveedor**
Mantenimiento del sistema de gestión de identidades	Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)
Administración del sistema de gestión de identidades	
Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)	
Gestión de parches del sistema operativo virtualizado y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo de seguridad del cliente y la política de seguridad del proveedor)	Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)
Configuración de la plataforma de seguridad del Tenant o del ambiente cloud del cliente (políticas del firewall, ajuste de sistemas de detección y protección de intrusos, etc.)	
Supervisión de los sistemas de invitado (Tenant)	Sistemas de alojamiento (hipervisor, firewall virtual, etc.)
Mantenimiento de la plataforma de seguridad (firewalls, sistemas de detección y protección de intrusos, antivirus, antimalware, antibots, filtrado de paquetes)	
Captura de registros y control de la seguridad	

Tabla 3 - Fuente: ENISA - Distribución de responsabilidades para Infraestructura como Servicio (IaaS). [59]

Como se puede ver en las tablas anteriores, y haciendo referencia a la imagen del punto 2.1.4 de este documento llamada separación de roles, es evidente que las actividades, roles y responsabilidades en lo que a seguridad de la información se trata, cambian según el modelo de servicio contratado. En síntesis, el proveedor debe encargarse de asegurar la protección de la infraestructura donde se despliegan los servicios ofrecidos, y va tomando aún más responsabilidades según el servicio contratado, así como garantizar la salvaguarda de la información de sus clientes. Por otro lado, los consumidores son los encargados de incrementar el nivel de seguridad, el fortalecimiento de los controles y salvaguardas de sus entornos cloud.

4.2- Ciclo de Vida de la Información

Para entender qué rol juega cada participante en la nube, así como la distribución de las responsabilidades es importante tener claro algunos ítems vitales de la seguridad de la información en este entorno. Uno de los temas prioritario es el tratamiento de los activos de información. Es imprescindible entender cómo se gestionan los datos de los clientes en la infraestructura y servicios cloud, quiénes los gestionan y qué controles protegen los datos, además de los cumplimientos normativos y legales. Por lo tanto, el primer tema clave es la clasificación de los activos de información, conocer su ciclo de vida y en base a esto desarrollar una postura de seguridad de la información, en línea con los objetivos organizacionales.

Ciclo de vida de los activos de la información: En la nube, la información tiene 6 fases o estados en los cuales enmarca su ciclo de vida, el cual puede ser lineal o no, y no necesariamente pasar por todas sus fases. Estás fases permiten definir con claridad el estado de los activos de información y en base a esto qué se debe tener en cuenta en cada uno de ellos. A continuación, se describe brevemente dichos estados según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) [13]:

- **Creación**: En esta fase se generan nuevos activos de información o se transforma, actualiza, modifica o altera la información existente.
- **Almacenamiento**: Hace referencia a los datos en reposo en cualquier medio de almacenamiento.
- **Uso**: Se refiere a la información utilizada para procesamiento, visualización o cualquier tipo de acción sin incluir la modificación de los datos.
- **Compartir**: Se le llama información en estado de compartición, a los datos accesibles por usuarios, consumidores o proveedores.
- **Archivado**: Es la información que deja de ser usada de forma activa y entra a un estado de retención.
- **Destrucción**: Esta suele ser su última fase, son los datos que pasan a ser eliminados de cualquier repositorio o copia de seguridad de forma permanente.

4.3- Gestión de Riesgos en la Nube

La gestión de riesgos de seguridad de la información independientemente de su entorno, es decir, ya sea dentro de la corporación o en un ambiente cloud, necesita un enfoque sistemático que permita identificar las necesidades con respecto a la seguridad de la información y crear un efectivo sistema de gestión de la seguridad de la información (SGSI).

Este enfoque debería ser adecuado para el entorno de la organización y, en particular, debería estar alineado con la gestión general de riesgos empresariales.

La gestión de riesgos de seguridad de la información debe ser un proceso continuo que puede ser aplicado a la organización como un todo, a un área en particular, a cualquier sistema de información o a aspectos particulares de un sistema complejo.

Cabe destacar que no todas las áreas/sistemas demandan un análisis completo y detallado. Muchas veces es suficiente con un análisis de alto nivel para poder tener los resultados esperados. Usualmente en ámbitos corporativos donde se focaliza el esfuerzo a partir de objetivos claros y un alcance definido se procede a realizar un análisis global donde para los hallazgos de alta criticidad, o en los cuales no se pueda brindar una solución sencilla, se realiza un análisis más detallado generando un grado más amplio a nivel de amenazas y posibilidades de mitigación.

La gestión de riesgos es un proceso iterativo, ya que es necesario realizar todos los pasos hasta obtener el nivel del riesgo y así poder compararlo con el apetito predefinido. Si el nivel de riesgo lo excede, se iniciará nuevamente el proceso hasta que dicho nivel quede por debajo.

También podría suceder que al aplicar determinado tratamiento del riesgo no se obtenga un nivel correcto de riesgo residual, lo cual demandará una nueva iteración. Esta vez relacionada con la aplicación de nuevos controles o cambios de estrategia en el tratamiento del riesgo.

Por otro lado, encarar la gestión de riesgos desde un enfoque iterativo, permitirá aumentar la profundidad y el grado de detalle de la evaluación en cada iteración.

Los criterios a utilizar en cada parte del proceso deben ser una decisión exclusiva de los responsables de la entidad contratista del servicio en la nube, es decir, del consumidor cloud.

Asimismo, una comunicación efectiva de la evaluación de riesgos a todas las partes interesadas posibilita una correcta implementación de controles y seguimiento de los mismos.

Por último, la documentación del proceso es esencial, así como el correcto registro de los resultados obtenidos, necesarios para llevar control y seguimiento de la gestión realizada.

Una de las normativas referente en este tema es el estándar ISO/IEC 27005:2018 [10], en el cual se provee una serie de directrices y un marco

para la gestión de riesgos de seguridad de la información en el ámbito de un sistema de gestión de la seguridad de la información.

Así mismo, la ISO/IEC 27017:2015 [4] complementa la información emitida en la ISO/IEC 27002:2013 en referencia a la orientación de la implementación de salvaguardas de seguridad de la información para clientes y proveedores de servicios en la nube. También brinda una serie de controles adicionales relacionados específicamente con los servicios en la nube.

4.4- Modelo de Seguridad en la Nube

Toda solución o modelo de seguridad de la información implementada en la nube debe ser diseñada en base al conocimiento de las amenazas de Internet y, además, debe tener en cuenta la responsabilidad compartida que existe entre el cliente y el proveedor.

Tomando esto en cuenta, se deben considerar dos enfoques según las actividades a realizar por cada una de las partes.

El **proveedor** tiene responsabilidad en la gestión de la seguridad física y lógica de la infraestructura sobre la que brinda sus servicios. Las siguientes son algunas de sus responsabilidades.

- Virtualización: El proveedor debe garantizar el aislamiento de las diferentes instancias virtuales, la detección, control y eliminación de cualquier tipo de malware en cada instancia en ejecución sobre el ambiente cloud de la organización, sobre otras cuentas de clientes asociadas en ejecución, sobre el ambiente de virtualización, así como sobre el hipervisor.
- Segmentación de los datos: El proveedor debe alojar los datos en diferentes sitios físicos, mantener un fuerte sistema de respaldo y recuperación de la información en pro de una rápida respuesta ante un incidente de seguridad.

El **cliente** tiene las siguientes responsabilidades:

- Control Perimetral: Debe asegurar todo el tráfico entrante, saliente e interno de su entorno. Mantener vigilancia activa sobre todas las comunicaciones generadas, así como detectar y proteger la implementación contra cualquier actividad maliciosa sobre el perímetro de la nube.

- Gestión criptográfica: Esta actividad tiene dos aristas que buscan que los datos en dispositivos de almacenamiento y en tránsito se encuentren cifrados, evitando así que sean fácilmente accedidos y conocidos por terceros no autorizados.

  En primer lugar, se debe cifrar con un método adecuado, toda la información, en sus diferentes estados, y garantizar la correcta autenticación del personal y recursos que acceden a los datos.

  En segundo lugar, se deben implementar protocolos de comunicación seguros que garanticen el cifrado de los datos en tránsito. Esto aplica también para la gestión y administración de los diferentes sistemas y servicios en la nube.

- Gestión de Eventos: El cliente debe capturar, procesar y analizar los logs generados en los diferentes sistemas y servicios en su entorno para poder detectar y actuar ante la identificación de un evento de seguridad. La correlación de esta información es vital para poder determinar los comportamientos inusuales o no esperados del ambiente cloud. Adicionalmente, debe garantizar el almacenamiento y respaldo de estos para propósitos de investigación de ser necesario.

La gestión de estas actividades está fuertemente correlacionada con el modelo de servicio adquirido ya que, dependiendo de esto, los recaudos y labores a realizar están distribuidos de manera diferente entre el proveedor y el cliente.

- Seguridad en el modelo de Infraestructura como Servicio: El proveedor en este modelo no toma responsabilidad sobre las instancias virtuales del cliente. El cliente debe implementar los procedimientos, controles necesarios para garantizar la seguridad desde el punto de vista operativo

como, el aseguramiento de la infraestructura virtual, comunicaciones, perímetro, aplicaciones, autenticación, autorización, servicios y más. De la misma manera, de la seguridad del personal que administra los recursos en la nube y de terceros.

- Seguridad en el modelo de Plataforma como Servicio: En este modelo de servicio, el cliente se encarga de asegurar las plataformas en las cuales se soporta y se gestionan sus aplicaciones. Sin embargo, ya no tiene responsabilidad sobre la seguridad operativa asociada con la infraestructura virtual.

- Seguridad en el modelo de Servicios como Servicio: En este punto la responsabilidad del cliente se limita al control de accesos, gestión de usuarios y el cifrado de los datos consumidos desde la nube. En este sentido, la gestión de accesos e identidades debe evaluarse bajo la autenticación, autorización y gestión de datos personales. El cliente debe tomar las medidas necesarias para evitar el robo de credenciales.

  Por otra parte, el cliente debe gestionar los activos de información. Si bien en el ambiente cloud las funciones operativas sobre los datos recae en el proveedor, el cliente debe tener pleno conocimiento de todos sus datos y de la manera en que se gestionan. Así mismo, debe tener el control sobre el procesamiento de datos en los diferentes dispositivos, y repositorios de los usuarios, como equipos móviles, equipos de cómputo, memorias de almacenamiento extraíble, entre otros, así como del almacenamiento y portabilidad de los datos corporativos.

Un tema transversal a los modelos de servicio es la continuidad del negocio. En esta parte se definen los acuerdos de servicio donde se pactan los valores de tolerancia para la disponibilidad de los servicios contratados. Hoy en día los proveedores cloud mantienen una disponibilidad del 99.9%.

Esto quiere decir que los servicios contratados están habilitados para su uso prácticamente en cualquier momento.

Concatenado a esto, la respuesta a incidentes es vital para la continuidad del servicio. Garantizar un correcto proceso, contención y

respuesta ante cualquier incidente de seguridad minimiza la posibilidad de tener consecuencias sobre los activos de información.

Por último, para el modelo de seguridad en la nube, todo lo anterior debe estar claramente estipulado en el contrato de servicios, declarando los niveles de servicio y los detalles a tener en cuenta de acuerdo con cada cliente. Es aquí donde el marco regulatorio aplicable para las partes toma relevancia. No solo al definir los detalles de gestión de seguridad según el modelo de servicio contratado, sino también los de la gestión de datos, que abarca entre muchos otros temas la protección, transferencia, respaldo y uso de los datos en los diversos procesos.

5 - Estándares de Buenas Prácticas Vigentes

Para el mundo cloud existen una serie de iniciativas y estándares de referencia para la seguridad de la información, en los que se busca que los clientes puedan implementar de forma estructurada y sistemática todas las actividades que comprenden la gestión de la seguridad de la información.

Estos estándares brindan una guía y una línea base con los requisitos mínimos a cumplir por parte de cualquier proveedor o cliente. Ofrecen una serie de actividades, controles, directrices y buenas practicas que buscan el aseguramiento de los servicios y activos de información.

La decisión de optar por un estándar específico no es una decisión asociada a costos sino de orden técnico. Por ello, se debe entender en profundidad las necesidades del cliente, los requerimientos de cumplimiento a nivel contractual, legal y normativo. Esta es la base con la cual se debe contar para poder determinar el grado de cumplimiento al que debe responder el proveedor y los requerimientos de seguridad asociados.

A continuación, se describirán los principales referentes en este tema para proporcionar una visión global de los aspectos a tener en cuenta en la gestión de la seguridad en ambientes cloud, tener control del entorno y garantizar la privacidad de los datos y metadatos.

5.1- CiberSecurity Framework del NIST

El Marco para la Mejora de la Ciberseguridad en las Infraestructuras Críticas del NIST (CSF, por sus siglas en inglés) [63], fue creado por los Estados Unidos como respuesta a la necesidad detectada por el gobierno para el fortalecimiento de la seguridad cibernética de las redes federales y las infraestructuras críticas. Esta iniciativa busca ayudar a las organizaciones a mejorar la gestión de riesgos y la protección de sus sistemas tecnológicos. Si bien en sus inicios fue orientado hacia las infraestructuras críticas, hoy en día es ampliamente usado por diversas compañías, ya que brinda una guía flexible y cíclica para la priorización de objetivos y el rendimiento de este tipo de infraestructuras. Cuenta con una serie de definiciones y metodologías

para la evaluación, gestión y alcance de resultados en base a este marco de trabajo. En el caso de la computación en la nube es aplicable tanto para el consumidor como para el proveedor.

Basado en estándares reconocidos mundialmente de gestión de la seguridad de la información y ciberseguridad, presenta una estructura de tres unidades fundamentales: el núcleo, los niveles de implementación y los perfiles.

- **Núcleo**: Son los procedimientos, prácticas, salvaguardas de seguridad que se encuentran agrupados en tres partes: funciones, categorías y subcategorías. Dichas funciones son: Identificar, Proteger, Detectar, Responder y Recuperar. Veinte y tres (23) categorías que velan por los objetivos de seguridad de la organización, enfocados en los resultados, capital humano y los aspectos técnicos. Por último, ciento ocho (108) subcategorías son los estamentos necesarios para el mejoramiento de la ciberseguridad de la organización. Estas están enfocados al alcance de resultados y a la mitigación de los riesgos relevados en la evaluación de riesgos.

- **Niveles de Implementación**: Es la fase en la cual la organización determina un nivel de implementación según las actividades y procesos que una compañía implementa para la gestión de la seguridad. Estos niveles muestran una escalabilidad según su maduración en el proceso, desde respuestas reactivas y de orden informal hasta sistemas con un enfoque orientado a la agilidad y retroalimentados en base a la gestión de riesgos. Son cuatro niveles, Parcial, Riesgo Informado, Repetible y Adaptado.

- **Perfiles**: Conforman la postura que la organización toma frente al riesgo, requerimientos y objetivos corporativos. Aquí se define el apetito de riesgo y los recursos necesarios para obtener los resultados esperados. Mediante una comparativa entre el estado actual y el futuro permite la mejora continua en pro del alcance de los objetivos trazados.

El CSF [63], a partir de una visión integral y una estrategia con base en la identificación del contexto, protección de los activos de información, la

detección temprana y respuesta ante eventos de seguridad, al mismo tiempo que la recuperación de la operatividad y funcionalidad del negocio, desarrolla conceptos para llevar adelante la gestión de los riesgos de ciberseguridad, así como la implementación de sistemas de gestión de seguridad o el mejoramiento y optimización de los sistemas ya implementados. Su uso también puede orientarse hacia la valoración de la realidad de la organización y la efectividad de los controles.

Es importante destacar que las previamente mencionadas subcategorías son comparables con otras normativas como la ISO/IEC 27002:2013 [9], permitiendo facilidad a la hora de su implementación, así como a la de su integración.

La adaptación de este marco a la nube se basa en la necesidad de estar en línea con la industria y la seguridad de los servicios en ese entorno, generando la posibilidad de afirmar a cualquier cliente que los proveedores cuentan con las mejores prácticas de gestión de riesgos definidas en el CSF [63] y así mismo, hacer uso de los controles para su propio entorno en la nube, así como cumplir con los requerimientos del sistema de gestión de la seguridad de la información de la organización.

5.2- ISO/IEC 27017:2015 Código de práctica para los controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube

La ISO/IEC 27017:2015 [5] es una norma internacionalmente aceptada de buenas prácticas, modificada a partir de la ISO/IEC 27002:2013 [9], para la implementación de controles en ambientes cloud. Brinda las directrices, lineamientos y buenas prácticas necesarias para la seguridad de la información de la entidad, sea esta proveedor o consumidor.

Esta norma se enfoca del lado de las organizaciones como parte de la gestión de la seguridad de la información en el cumplimiento de requisitos de seguridad a partir de la evaluación de riesgos y la implementación de los controles y directrices correspondientes para la satisfacción de las exigencias contractuales y legales, haciendo entendible los roles y

responsabilidades de los actores en la nube y minimizando los riesgos asociados con estas tecnologías. Esto conlleva a nivelar y ajustar la relación cliente-proveedor.

Del lado del proveedor, provee información relacionada a los controles de seguridad fuertemente reconocidos que los Proveedores de Servicios en la Nube (CSP. por sus siglas en inglés) pueden implementar. Por lo cual, es habitual que los proveedores estén alineados con esta normativa y que los clientes tomen como parámetro a la hora de evaluar la contratación de servicios. Dichas exigencias adicionales permiten estandarizar todas las relaciones entre el cliente y el proveedor de servicios en la nube.

A partir de la generación y modificación de controles específicos para la nube, la ISO/IEC 27017:2015 se centra en las vulnerabilidades y amenazas asociadas a estas tecnologías, de manera holística. Puntualmente mediante la sugerencia de 44 controles busca brindar guía sobre temas como los siguientes:

- Correlación de las funciones y responsabilidades compartidas en el marco de la nube.
- Tratamiento de activos de información una vez terminado el contrato de servicios.
- Cumplimiento de requerimientos tecnológicos sobre la infraestructura virtual según las necesidades y particularidades de la organización.
- Acuerdos de acceso, monitoreo y análisis de los eventos generados en el entorno cloud del cliente.
- Gestión de los ambientes cloud mediantes procesos y procedimientos orientados a la parte operacional.
- Correcto aislamiento y aseguramiento de los ambientes virtuales de los diferentes clientes del proveedor, así como gestión de la seguridad de las redes virtuales y físicas.
- Acuerdo común entre las partes tanto de la gestión de la seguridad de la capa de comunicación física como la virtual.

- Alineación y guía adicional para la aplicación de los controles que especifica la norma ISO/IEC 27002:2013.

5.3- Guía De Seguridad del CSA

En esta publicación, la CSA [2] brinda los lineamientos, directrices y buenas prácticas para hacer uso de la computación en la nube de manera segura.

Este documento se encuentra dividido en 13 dominios enfocados en cómo solventar los desafíos que impone la nube a nivel de seguridad sin importar el modelo de despliegue o de servicio implementado. Estos dominios están divididos en dos grandes grupos, gobierno y operaciones. En el primero de estos, se abordan los temas estratégicos y relacionados con la política y gestión. El grupo de operaciones trata los temas técnicos y se enfoca en la implementación de salvaguardas según la arquitectura de la solución cloud.

A efectos de este documento, la siguiente tabla tomada del documento del CSA [2] muestra las áreas de enfoque crítico.

Áreas de enfoque crítico - Guía de seguridad de áreas críticas para la computación en la nube V4.0	
Dominio	**Descripción**
Gobierno	
Gobernanza y gestión de riesgos empresariales	La capacidad de una organización para gobernar y medir el riesgo empresarial introducido por la computación en la nube. Elementos como la precedencia legal para infracciones de acuerdos, capacidad de las organizaciones de usuarios para evaluar adecuadamente el riesgo de un proveedor de nube, responsabilidad de proteger datos confidenciales cuando tanto el usuario como el proveedor pueden tener la culpa, y cómo las fronteras internacionales pueden afectar estos problemas.
Asuntos legales, Contratos y descubrimiento electrónico	Posibles problemas legales al usar la computación en la nube. Las cuestiones que se abordan en esta sección incluyen los requisitos de protección para la información y los sistemas informáticos, las leyes de divulgación de violaciones de seguridad, los requisitos reglamentarios, los requisitos de privacidad, las leyes internacionales, etc.

Áreas de enfoque crítico - Guía de seguridad de áreas críticas para la computación en la nube V4.0	
Dominio	**Descripción**
Gestión de cumplimiento y auditoría	Mantener y probar el cumplimiento cuando se utiliza la computación en la nube. Aquí se tratan cuestiones relacionadas con la evaluación de cómo la computación en la nube afecta al cumplimiento de las políticas de seguridad interna, así como los diversos requisitos de cumplimiento (normativo, legislativo y de otro tipo). Este dominio incluye alguna dirección para probar el cumplimiento durante una auditoría.
Gobierno de la información	Gobernando los datos que se colocan en la nube. Aquí se discuten los elementos que rodean la identificación y el control de los datos en la nube, así como los controles de compensación que se pueden usar para lidiar con la pérdida de control físico cuando se mueven datos a la nube. Se mencionan otros elementos, como quién es responsable de la confidencialidad de los datos, la integridad y la disponibilidad.
Operación	
Plano de Gestión y Continuidad del Negocio	Asegurar el plano de gestión y las interfaces administrativas utilizadas al acceder a la nube, incluidas las consolas web y las API. Garantizar la continuidad del negocio para implementaciones en la nube.
Seguridad de Infraestructura	Seguridad del núcleo de la infraestructura de la nube, incluidas las redes, la seguridad de la carga de trabajo y las consideraciones de la nube híbrida. Este dominio también incluye fundamentos de seguridad para nubes privadas.
Virtualización y contenedores	Seguridad para hipervisores, contenedores y redes definidas por software.
Respuesta a incidentes, notificación y remediación	Detección, respuesta, notificación y reparación adecuada de incidentes. Esto intenta abordar los elementos que deberían estar en su lugar, tanto a nivel de proveedor como de usuario, para permitir el manejo adecuado de incidentes y análisis forense. Este dominio lo ayudará a comprender las complejidades que trae la nube a su programa actual de manejo de incidentes.
Seguridad de aplicaciones	Asegurar el software de la aplicación que se ejecuta o se está desarrollando en la nube. Esto incluye elementos tales como si es apropiado migrar o diseñar una aplicación para que se ejecute en la nube y, de ser así, qué tipo de plataforma en la nube es la más adecuada (SaaS, PaaS o IaaS).
Seguridad y cifrado de datos	Implementando la seguridad y el cifrado de datos, y garantizando la administración escalable de claves.
Identidad, derecho y administración de acceso.	Administrar identidades y aprovechar los servicios de directorio para proporcionar control de acceso. La atención se centra en los problemas que se encuentran al extender la identidad de una organización a la nube. Esta sección proporciona información sobre cómo evaluar la

Áreas de enfoque crítico - Guía de seguridad de áreas críticas para la computación en la nube V4.0	
Dominio	**Descripción**
	preparación de una organización para llevar a cabo una Gestión de acceso, idoneidad e identidad (IdEA) basada en la nube.
Seguridad como servicio	Proporcionar aseguramiento de seguridad facilitado por terceros, administración de incidentes, certificación de cumplimiento y supervisión de identidad y acceso.
Tecnologías relacionadas	Tecnologías establecidas y emergentes con una estrecha relación con la computación en la nube., incluidas el Big Data, el Internet de las cosas y la informática móvil.

Tabla 4 - Fuente: CSA - Áreas de Enfoque Crítico. [2]

La información en detalle de las áreas de enfoque crítico se encuentra descrita en el Anexo C de este documento, con el fin de realizar un abordaje y descripción de este estándar de seguridad para su posterior uso.

6- Implementación de una Arquitectura y Modelo de Seguridad en la Nube Desde el Punto de Vista del Consumidor

Un parámetro esencial en el momento de pensar la implementación de soluciones en la nube es la responsabilidad compartida entre el cliente y el proveedor de servicios cloud. Esto determina la estrategia de despliegue, migración de servicios y activos de información a un entorno cloud. Dicha estrategia debe contar con el concepto de seguridad desde su concepción y permitir la introducción de este desde el primer paso, sin que llegue a ser un determinante negativo para la implementación de nuevas soluciones cloud.

Si bien los grandes proveedores cuentan con aplicaciones, infraestructura, herramientas, procedimientos, procesos, normativas y políticas que hacen a la seguridad de la nube, esto no garantiza una mitigación de los riesgos asociados a las implementaciones realizadas en este entorno. Es responsabilidad del consumidor de la nube determinar cuál es la mejor estrategia de implementación de sus servicios, aplicaciones, infraestructura y demás de manera segura en la nube y cómo hacer uso de las herramientas y funcionalidades que esta ofrece para la satisfacción de sus requerimientos.

A fin de cumplimentar dicha estrategia, es necesario pensar en la arquitectura de implementación a utilizar. Esta se define como: el nivel inicial del proceso de construcción de un sistema de información que hace hincapié en aspectos del diseño y de la especificación de la estructura global del sistema de forma lógica, buscando satisfacer una serie de requisitos dado un escenario especifico; en este caso, la nube.

A partir de lo descrito anteriormente, se realizará la propuesta de un enfoque para sumar el factor seguridad a la arquitectura de implementación de soluciones en la nube o una base para la evaluación de implementaciones cloud a partir de un enfoque sencillo y fácil de aplicar a la hora de determinar el nivel de seguridad que tiene el entorno a utilizar.

Para ello, este documento presenta una arquitectura de implementación segura en la nube, a partir de principios y conceptos de patrones de diseño para la implementación de seguridad (definido en el punto 6.2) y haciendo uso de las ventajas que brindan los entornos cloud, para lograr soluciones seguras a la medida de las necesidades del negocio. Esto requiere un enfoque integral de seguridad en todos los niveles, visibilidad y trazabilidad de todos los eventos generados en la nube, gestión de identidades, diseño seguro y a la medida, centralización de los datos y quizás lo más importante, generar implementaciones basadas en la automatización, que garanticen el cumplimiento y la gobernanza del entorno cloud del consumidor implementado en el CSP.

Se tomará una arquitectura de implementación teórica, de forma que pueda ser homologable y extensible a la computación en la nube. Posteriormente, basados en principios de seguridad y la definición de controles, se brindarán los puntos clave para incorporar el concepto de seguridad con base en lo descrito en los capítulos anteriores.

6.1- Propuesta de Enfoque de una Arquitectura de Implementación Segura en la nube

El concepto de arquitectura de implementación teórica significa que, a partir de una serie de elementos, funcionalidades, mecanismos y haciendo uso de políticas, normativas, estándares de buenas prácticas, procesos y procedimientos se logre la implementación de sistemas de información que, con el agregado de componentes de seguridad, puedan ser usados de forma segura, eficaz y eficiente por los consumidores.

Existen varias iniciativas que buscan brindar una arquitectura de implementación segura en la nube, desde el CSA [2] hasta NIST [57] o Jericho [32], las cuales despliegan una gran cantidad de información alrededor del proveedor de servicio y el usuario de la nube. Ahora bien, la necesidad de entender la seguridad de una forma fácil y sencilla en toda la ruta de consumo de la nube y la interacción del cliente es el reto que se busca afrontar basado en la información expuesta en este documento y en

un enfoque innovador, haciendo uso de conceptos de la ingeniería de sistemas.

Diagramar de una manera sencilla y clara todo lo que integra la nube y la relación entre sus componentes es una labor que requiere de un amplio conocimiento de los productos y servicios ofrecidos por los diferentes proveedores de la nube, lo cual no es el objetivo de este trabajo de posgrado.

En cambio, se busca poder hacer uso de una arquitectura de implementación teórica simple de un servicio o aplicación, y a partir de allí, poder extrapolar la seguridad para esta arquitectura, buscando así la generalización y posterior abstracción a un caso puntual.

Para esto se hace uso de la arquitectura cliente-servidor clásica adaptada a la nube donde, a partir de la definición de los componentes que participan en esta arquitectura, se plantean los retos a asumir en torno a la seguridad de la información. La siguiente imagen representa la versión básica de esta arquitectura adaptada a la nube.

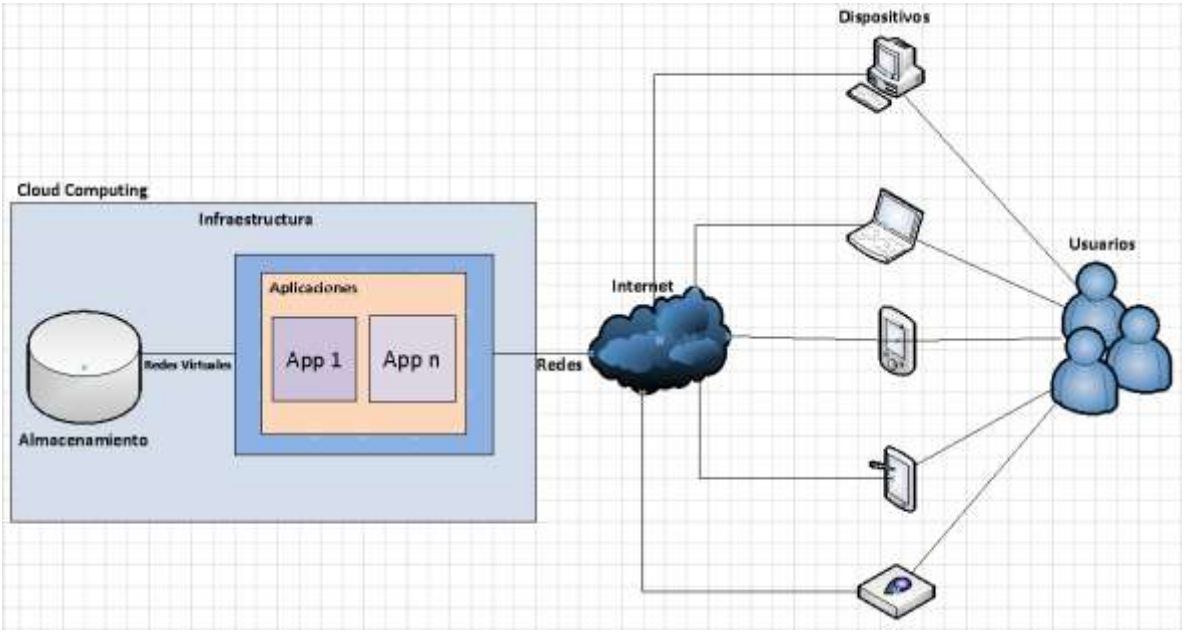

Ilustración 5: Arquitectura Cliente-Servidor adaptada a la nube. Fuente: Propia

Como se puede identificar, se encuentran seis elementos o componentes básicos: usuarios, dispositivos, redes, aplicaciones, infraestructura y almacenamiento. Estos cuatro últimos se encuentran agrupados en lo que básicamente sería el Cloud Computing teniendo en cuenta que forman parte de una serie de componentes que en detalle generan la complejidad en la nube.

Cada componente agrupa de forma general, las diferentes tecnologías asociadas a él. Por ejemplo, al hablar de almacenamiento, se asocia a cualquier tecnología usada para el resguardo de información, ya sea tecnología para el almacenamiento de datos binarios, archivos, audio, video y demás. Otro ejemplo claro es la infraestructura: en el mundo cloud no se habla únicamente de servidores y sus sistemas operativos; adicionalmente a estos se encuentran los contenedores. En el grupo de redes sucede lo mismo: son todas aquellas tecnologías que operan en la comunicación de la nube dentro y fuera de ella, es decir, conmutadores, conmutadores virtuales, corta fuegos, balanceadores de carga, enrutadores de red, enlaces de comunicaciones y demás, que hacen al mundo de las telecomunicaciones cloud.

El modelo de la Ilustración 5 es ampliamente usado para la construcción de sistemas de información los cuales, haciendo uso de la distribución del tratamiento de los datos por todo el sistema informático, permiten optimizar el sistema global. Como se puede deducir del gráfico anterior, en el entorno cloud, los temas referidos al control de acceso, procesamiento, almacenamiento, datos en tránsito y en sí la carga computacional del sistema de información, están asociados al CSP y comparten un grado de responsabilidad con el consumidor de la nube según el modelo de servicio y despliegue implementados.

En una arquitectura clásica cliente-servidor, el usuario cuenta con el acceso a los servicios, aplicaciones, datos y recursos mediante los dispositivos y plataformas habilitadas para dicho acceso, a través de la entidad. Extrapolando este concepto y entendiendo que ahora la capacidad tecnológica de las organizaciones que adoptan el paradigma de la nube se

encuentra alojadas en el proveedor de servicios cloud, la gestión de este acceso será compartida con el CSP.

Los proveedores de servicios en la nube se basan en la eficiencia operacional, generación de confianza a sus clientes, optimización de costos, alto rendimiento y seguridad para poder hacerse cargo de las necesidades de capacidad tecnológica de cualquier entidad. Sin embargo, esto no garantiza que el CSP entienda las necesidades y cumpla en detalle los requerimientos asociados a la realidad de cualquier organización. Este proceso de ajuste y optimización de los recursos y herramientas, es una responsabilidad exclusiva de la entidad que contrata y consume los servicios de la nube. De la misma manera, un tema ineludible es garantizar que los servicios tercerizados funcionen según lo contratado, incluyendo los requerimientos de seguridad.

Por otro lado, y como es conocido, una funcionalidad de la arquitectura de implementación teórica propuesta es que permite el uso de ambientes distribuidos, lo que quiere decir que todos los requerimientos generados por los usuarios mediante sus dispositivos y plataformas soportadas podrán ser procesados por la infraestructura alojada en la nube.

Es en relación a los componentes mencionados previamente (usuarios, dispositivos, telecomunicaciones, infraestructura, aplicaciones y almacenamiento), y cómo estos operan, que se generan los desafíos de seguridad. Cada una de estos grupos genera preocupaciones de seguridad de diferente índole, las que deben ser trabajadas en detalle en diferentes niveles por parte de la entidad que consume los servicios de la nube según su rol y grado de responsabilidad.

6.2- Patrones de Diseño para la Implementación de Seguridad

En el ámbito de la ingeniería de software, un patrón de diseño se define como: una solución general y reutilizable para un problema común de acuerdo a un contexto dado, el cual puede aplicarse a cualquier dominio del software y se hacen presentes en determinadas fases del ciclo de vida del

software: análisis/diseño, construcción/desarrollo. Un patrón es aplicable según el tipo de problema a resolver [64].

Los patrones de diseño trabajan de la mano con los principios y estándares de arquitectura, los cuales son usados en varios campos de la tecnología, desde el desarrollo de software hasta la implementación de modelos de servicio. En el mundo de la seguridad existen varias iniciativas que buscan abordar esta temática en base a modelos de diferente índole y a variados patrones de diseño de acuerdo con enfoques distintos. Entidades como el SANS Technology Institute [31], cuentan con amplia información sobre cómo diseñar soluciones tecnológicas en la nube de forma segura, orientados a los principales proveedores de servicios en la nube. Sin embargo, es posible extrapolar principios generales para el diseño de una arquitectura de implementación segura, de aquí en más denominada “diseño seguro”, independientemente del proveedor en el cual se implemente el entorno tecnológico de cualquier organización.

Los patrones de diseño seguro permiten que en el momento de emprender la implementación de un sistema de información se introduzca y se tenga en cuenta el factor seguridad en cada paso y así sea posible definir los requerimientos a cumplir en esta materia. Por ejemplo, al desarrollar un sistema de información en la nube, entre los temas a tener en consideración está la generación de un ciclo de vida de desarrollo seguro, en donde se especifique la seguridad embebida en el código de la aplicación. También, tener control de las plantillas de creación y configuración usadas para la implementación de máquinas virtuales o contenedores que van a soportar el sistema de información, los cuales deben contar con la seguridad requerida según la labor a realizar. Estas actividades van de la mano con la automatización de los procesos que permiten validar el cumplimiento de los requisitos de seguridad, así como el monitoreo activo de los eventos y el comportamiento de los componentes de la nube. De esta manera es posible detectar temprana y proactivamente cualquier desvío a nivel de seguridad.

Definida la arquitectura de implementación con la cual se va a abordar la temática, se usarán los patrones de diseño seguro que agrupen los

aspectos necesarios para la protección integral de esta arquitectura según los componentes básicos mencionados previamente (usuarios, dispositivos, redes, aplicaciones, infraestructura y almacenamiento) que hacen a la arquitectura de implementación segura. A continuación, se describe cada uno de los patrones de diseño.

Seguridad por niveles: Toda infraestructura cuenta con una serie de componentes que trabajan de forma diferente en niveles o capas claramente identificables. Por ejemplo, en el mundo de las telecomunicaciones, una guía de la definición de estas capas es el modelo OSI[5], donde cada capa entendiendo su modo de operación y elementos claves, genera requerimientos de seguridad y soluciones diferentes.

En el mundo cloud, una abstracción válida de las capas a garantizar su seguridad se obtiene a partir de la arquitectura definida por el CSA [2]. A continuación, se listan dichas capas:

1. Nivel de Aplicaciones (API´s, Aplicaciones Corporativas, etc.).
2. Nivel de Servidores y Plataformas (Máquinas Virtuales, Contenedores y Middleware).
3. Nivel de Almacenamiento y Datos.
4. Nivel de Telecomunicaciones.
5. Nivel de Plataforma de Virtualización.

Todos los componentes de una infraestructura cuentan con algún tipo de seguridad integrada. Sin embargo, a nivel de cada capa se deben agrupar los componentes e implementar salvaguardas haciendo uso de normativas y buenas prácticas como también la generación de políticas que dicten el comportamiento de estos componentes. Otro tema que se debe contemplar es el lugar de aplicación de estos controles y políticas, ya que

[5] Modelo OSI: El modelo de referencia de interconexión de sistemas abiertos (OSI) divide el proceso de conexión de red en siete capas administrables. Cada capa del modelo OSI define una función específica de la red. Estas funciones están definidas por la Organización Internacional de Normalización (ISO) y son reconocidas en todo el mundo. El modelo de referencia OSI se utiliza a nivel mundial como método de enseñanza y comprensión de la funcionalidad de las redes. Si se sigue el modelo OSI cuando se diseña, construye, actualiza o cuando se diagnostican fallas, se logrará mayor compatibilidad e interoperabilidad entre los diversos tipos de tecnologías de red [66].

esto dependerá de la arquitectura puntual desplegada y de cada organización, ya sea en instalaciones o ambientes controlados por la organización o en el ambiente cloud.

Seguridad en los componentes: Como se ha mencionado anteriormente, el dinamismo de la nube hace pensar que los modelos de seguridad estáticos no sean efectivos. Por lo cual, se debe adaptar la forma de abordar este reto. Para esto, analizar los componentes que intervienen en un sistema de información y cómo ellos interactúan entre sí es fundamental ya que, de este análisis, se generarán los requerimientos de seguridad necesarios.

El entorno cloud brinda por cada CSP una importante gama de aplicaciones, servicios, plataformas, infraestructura, entre otras, donde cada producto cuenta con diferentes componentes que no son fáciles de categorizar y agrupar. Esto hace que se requieran diferentes y diversos controles de seguridad según cada componente y su funcionalidad. Por ejemplo, las bases de datos (subcategoría) o el almacenamiento (categoría) ofrecido por los CSP, son tan diversos a nivel de componentes, orientados a solucionar requerimientos muy diferentes entre sí, que no se podría reducir solamente a la implementación de controles orientados únicamente a dicha categoría/subcategoría.

Es claro que existe un reto enorme a nivel de gestión de la seguridad. La definición de políticas claras apoyadas en herramientas para la nube debe mantener bajo control este parámetro.

Respuesta a fallas: Si bien, al hablar de nube se piensa en la alta disponibilidad de servicios y muchas garantías brindadas por los proveedores de servicio, estos no son ajenos a los incidentes que todo sistema de información e infraestructura tecnológica puede sufrir. La responsabilidad compartida toma especial valor en este sentido, porque el control parcial del ambiente hace que haya limitaciones a la hora de tratar las fallas. Sin embargo, esto no exime la responsabilidad de la entidad consumidora a la hora de la implementación de soluciones cloud, de pensar en la respuesta a este tipo de eventos.

Para esto, se debe diseñar la arquitectura en base a los posibles puntos de falla, ya sea por componentes o el ambiente en general. En lo que concierne a la seguridad, se deben crear ambientes redundantes y de alta disponibilidad en el entorno cloud, apoyado en las características esenciales de la nube, ya que estas brindan otra forma de afrontar estas fallas. Diseñar soluciones cloud basándose en el rápido despliegue, el crecimiento horizontal como vertical y la automatización, para optimizar la respuesta a los incidentes.

Diseño en base a la Elasticidad: De la mano con el punto anterior, la elasticidad es quizás una de las características más valoradas por la nube. Esta provee de una solución rápida a la hora de crecer o decrecer, ya sea de forma horizontal o vertical según sean las necesidades del negocio. Es decir, en el ambiente cloud se puede incrementar o reducir la cantidad de recursos que necesita un dispositivo en particular para un óptimo funcionamiento o, de ser necesario, la cantidad necesaria de un mismo tipo de dispositivo para cumplir con una demanda de forma rápida y sin mayores cambios a nivel de configuración.

Del lado de la seguridad, esto permite tener una rápida respuesta ante cualquier incidente, aislar ambientes completos o simplemente generar nuevos recursos para reponer algún dispositivo que haya sido afectado dada una incidencia de seguridad. Por lo cual, a la hora de desplegar ambientes se debe integrar este principio en el diseño pensando en las condiciones que deben cumplirse para crecer o decrecer la infraestructura en la nube y siempre en mantener gestión y control de los nuevos dispositivos y la correcta eliminación de estos, una vez que ya no sean necesarios.

Por otro lado, como se mencionó antes, a nivel de Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS), se crean los recursos a partir de plantillas que deben ser validadas y controladas para que cumplan con los requisitos de seguridad establecidos por la organización, no solo a nivel de configuración del dispositivo, sino también como parte del sistema. Es decir, control de accesos, aislamiento de red, reglas de acceso, políticas aplicables según la labor a realizar, entre otros,

que se consideren pertinentes. Esto forma parte del concepto de diseño de la seguridad en los componentes y funciona como un ejemplo de cómo los patrones de diseño trabajan juntos.

Diseño del Almacenamiento: Un punto ineludible a la hora de pensar en diseño de seguridad es el tratamiento de los datos. La nube ofrece una gama bastante amplia de almacenamiento según la naturaleza de los datos, desde información correlacionada como una base de datos hasta archivos binarios. Cada tipo de archivo tiene su propio tipo de almacenamiento orientado a la optimización y tratamiento de la información alojada allí. Por otro lado, también la clasificación de los activos de información, según la importancia que tenga para la entidad, genera nuevos requerimientos de seguridad.

Esto trae consigo definiciones necesarias de seguridad que deben ser apoyadas por un correcto inventario de activos de información y una política de tratamiento de datos, ya que dependiendo de lo anterior y el tipo de almacenamiento que se necesite, son diversas y muy diferentes las funcionalidades de seguridad a habilitar.

Dado que el cifrado de datos es un gran consumidor de recursos computacionales, impactando en todo el ciclo de vida de los datos y en la velocidad de trabajo, se debe ser muy cuidadoso al definir qué datos deben ser cifrados. Para ello se debe tener en cuenta el sistema de información de que se trate y la clasificación de los datos que se procesan, respecto de su confidencialidad, integridad y disponibilidad. Por otro lado, se debe considerar la implementación de las buenas prácticas en gestión de la criptografía.

Gestión de Eventos: Un proceso transversal a toda la infraestructura de la nube es la visibilidad de los eventos de los dispositivos que la componen, cómo estos interactúan entre ellos y la generación de comportamientos definidos para la concepción de límites reales. Este elemento de diseño es ineludible y es el único que puede brindar una visión de lo que sucede en la nube, ya sean actividades de la organización o del CSP.

Haciendo referencia a la arquitectura mostrada en la Ilustración número 5, este patrón de diseño no solo se debe concentrar en el entorno de la nube, sino abordar todos los caminos posibles que brinden información de valor para la detección de eventos y comportamientos atípicos. Desde los dispositivos que se conectan a la nube hasta la interacción del hipervisor con el entorno cloud de la organización.

El monitoreo y la gestión de eventos en ambientes de propiedad de la organización tiene también un alto valor. Sin embargo, este concepto debe ser abordado en la nube entendiendo el dinamismo de esta y distinguiendo de forma detallada y veraz qué eventos se producen por el cambio constante de la nube y, por otro lado, los posibles eventos que confirmen un incidente en curso.

Teniendo lo anterior en mente, se debe analizar constantemente la información procesada, definir los mecanismos de llegada, procesamiento, almacenamiento, correlación de los datos y crear tableros de control y sistemas de alarmas confiables basados en la mejora continua para que estas herramientas reflejen la realidad del ambiente cloud.

Por otro lado, también se debe efectuar la gestión de los eventos generados por los dispositivos móviles y equipos de cómputo destinados para las labores de los colaboradores de la entidad. Estas fuentes de datos pueden determinar cuándo un ataque de seguridad se puede estar llevando a cabo, a partir de la detección de un comportamiento inusual del usuario o procesos en ejecución desde el dispositivo. Esto explica la importancia de adoptar este principio de gestión de eventos en los dispositivos finales de los usuarios de la entidad, con ello se puede obtener información de valor y entendimiento del comportamiento del sistema en general.

La gestión de la seguridad se hace vital en este punto, se debe tener gestión centralizada de la visualización de los eventos generados en la nube, así como de los controles implementados. Esta visualización no se debe limitar al ambiente cloud, sino pensar también fuera de este. Es decir, romper el paradigma de seguridad según el perímetro, ya que esta visión es limitada y deja por fuera componentes como los dispositivos móviles,

dispositivos propios de los consumidores que hacen uso de los servicios cloud, dispositivos de infraestructuras críticas y más. Por lo cual, los controles, y la visualización de los eventos generados por estos, deben ser gestionados centralizadamente para poder detectar comportamientos no habituales y ataques cibernéticos para su remediación.

Automatización: Este es el principio primordial de la nube, la automatización de procesos, procedimientos y actividades de manera sencilla, eficaz y eficiente. Por lo tanto, se debe actuar en el ámbito de la seguridad en base a dicho principio como se mencionó anteriormente y lo indica el CSA [2]. Así mismo, de la mano de la automatización se debe pensar en la estandarización y centralización.

La estandarización es un proceso fundamental para la mejora continua y en particular para la automatización. Con la amalgama de tantas tecnologías en un mismo ambiente, donde cada una de estas tiene formas particulares de hacer un mismo proceso y de presentar la información de tan diversas maneras, se hace necesario buscar la forma de homogenizar una forma de trabajo y gestión de estas tecnologías. Para ello, hay tecnologías como el Security Assertion Markup Language (SAML[6] por sus siglas en inglés), por ejemplo, que permiten la estandarización de la autenticación. Bajo este principio, se debe optar por diseñar ambientes que puedan ser estandarizados para que posteriormente se realice su automatización.

La centralización requiere tener claramente definida la mejora continua ya que, dependiendo de cada tecnología, CSP, producto y demás detalles a tener en cuenta, la información que se brinda es mostrada en formato y con herramientas y maneras de gestión totalmente diferentes entre sí y debe ser constantemente tratada y optimizada para que pueda brindar información de valor por si misma o correlacionada con más datos. Por ello, la centralización apoyada en la mejora continua brinda un estado final y grado de madurez donde toda esta información representada de forma

[6] SAML (Security Assertion Markup Language): Significa Lenguaje de Marcado de Seguridad. Es un estándar abierto basado en XML para la transferencia de datos de identidad entre dos partes: un proveedor de identidad (IdP) y un proveedor de servicios (SP) [35].

diferente pueda ser controlada y gestionada desde una única interfaz gráfica, por ejemplo, mediante un tablero de control maestro.

De la mano de lo anterior, el parámetro de diseño de la automatización de los controles resuelve muchas de las necesidades y retos a gestionar en ambientes cloud. Partiendo de abordar de manera rápida y segura actividades de configuración, respuesta a incidentes, gestión, auditoría, entre otros, de modo ágil como lo requiere la nube.

En el concepto DevSecOps [65] se incluye el concepto del manejo del radio de daño a partir de una incidencia. Esto quiere decir, tener conocimiento y control del posible daño ocasionado dada la materialización de una amenaza o de un incidente de seguridad. Para lo cual, la automatización es una herramienta fundamental para controlar y limitar este radio de perjuicio que se podría generar mediante la activación de procedimientos automáticos a partir de disparadores o similares que den solución o mitiguen cualquier incidencia.

Dados los principios de diseño seguro, estos permitirán dar forma y gestión a la seguridad en cada nivel del modelo de seguridad propuesto. Desde el diseño de la arquitectura hasta la aplicación de controles, estos patrones son aplicables y garantizarán un correcto diseño de seguridad en cada etapa de la implementación de un ambiente computacional en la nube.

6.3- Modelo de Seguridad Aplicable a la Arquitectura Propuesta

Habiendo definido la arquitectura de implementación y los patrones de diseño para asegurar dicha arquitectura, se presenta el siguiente modelo teórico de seguridad aplicable por parte del consumidor de la nube, buscando priorizar las labores a realizar por cualquier organización que desee implementar seguridad o evaluar el nivel de seguridad de su entorno cloud. Este modelo está orientado a las labores que debería realizar el consumidor de servicios cloud, buscando garantizar la seguridad en un ambiente de responsabilidad compartida con el CSP como lo es la nube. A continuación, se presenta el esquema general del modelo de arquitectura de

seguridad generado en base a la información recopilada, analizada y descrita en este documento.

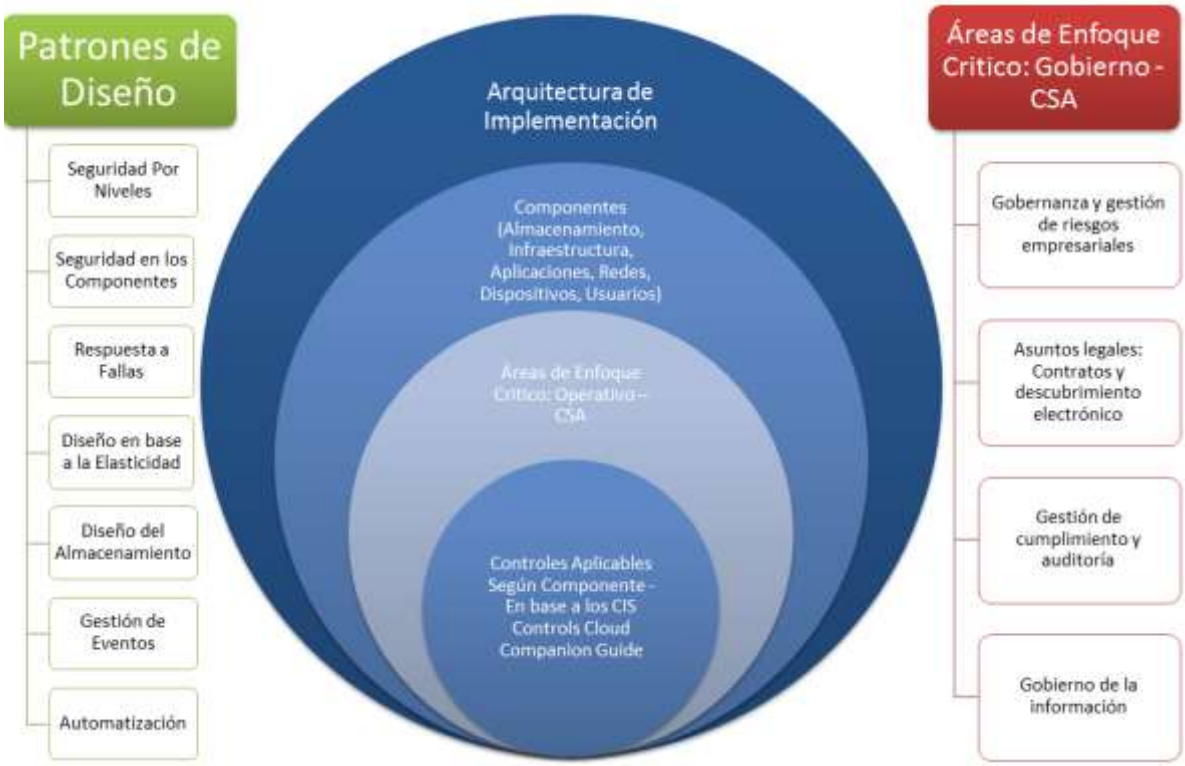

Ilustración 6: Esquema General del Modelo de Arquitectura de Seguridad Propuesto. Fuente: Propia

El modelo propuesto cuenta con seis grupos de trabajo, dos de estos grupos son transversales a todo el modelo; estos son los patrones de diseño y áreas de enfoque crítico a nivel de gobierno del CSA [2]. Los cuatro restantes, expresados de forma jerárquica, son la arquitectura, los componentes, las áreas operativas de enfoque crítico del CSA [2] y los controles propuestos. Estos últimos concuerdan con los definidos por el CIS [24].

Los dos grupos transversales señalados previamente actúan en cada nivel de los expresados jerárquicamente con el fin de que se genere una arquitectura basada en las prácticas de diseño de seguridad generalmente aceptadas, como a su vez se garantice la gobernabilidad, gestión de riesgos y control de la información en cada paso de la contratación, diseño, implementación y gestión de una solución cloud en donde el concepto

“seguridad” se encuentre desde el primer paso y en cada uno de sus grupos de trabajo.

Este modelo en base a la arquitectura de implementación teórica se desglosa según sus componentes fundamentales, almacenamiento, infraestructura, aplicaciones, redes, dispositivos y usuarios. Estos a su vez, se agrupan visualmente según el modelo de servicio contratado con el proveedor de servicio cloud. Esto permite determinar la mayor o menor carga operativa por parte del consumidor del servicio. Por ejemplo, al contratar un servicio de software como servicio, el consumidor de servicios cloud tendrá una menor carga operativa y a su vez una responsabilidad más limitada a partir del componente aplicación frente a los operadores funcionales que consuman el servicio implementado en la nube. Por otro lado, si el consumidor implementa una solución de Infraestructura como servicio, este tendrá que tener en cuenta todos los componentes esenciales mencionados y su responsabilidad y carga operativa será proporcional a este nuevo alcance.

Posteriormente a esta primera definición, se hace uso de las áreas de enfoque crítico del orden operativo definidas por el CSA [2], brindando el enfoque de seguridad a tener en cuenta sobre cada componente y sus relaciones, ya sea específico para dicho elemento como lo es la seguridad de la infraestructura, o transversal como lo es el área de identidad, derecho y administración de acceso.

En la base de la Ilustración 6 se encuentran los controles específicos a implementar por componente según las áreas críticas definidas en el nivel inmediatamente superior. Estos controles pueden ser modificables, ampliados o cambiados, a conveniencia de la organización que implemente sus sistemas de información en la nube. Por ejemplo, en el caso del almacenamiento, se define como crítica la seguridad y el cifrado de los datos, para lo cual, se podría proponer de acuerdo a la necesidad del negocio y los requerimientos de seguridad, hacer uso de los controles de encriptación de datos, gestión y control del respaldo de información, implementación de soluciones de prevención contra pérdida de datos,

establecimiento y gestión claves criptográficas, pruebas de penetración y auditorías, siendo estos parte de los posibles controles y sub-controles aplicables al almacenamiento.

Además de lo mencionado anteriormente, la implementación de los controles está unida fuertemente a los requerimientos legales y normativos aplicables y de los detalles técnicos necesarios para poder determinar cuál es la mejor relación costo-beneficio. Esto significa que se debe tener en cuenta de forma integral, desde las facilidades, características y funcionalidades que brinda el proveedor de servicios cloud hasta los componentes de la solución que se busque proteger, para así poder establecer cuál es la mejor opción en cada caso.

Para el modelo de seguridad propuesto, se toma como base los veinte (20) controles definidos por el CIS [24] expuestos en la tabla denominada "Resumen de la Aplicabilidad de cada Modelo de Servicio", incluida a continuación. Esta tabla muestra el grado de aplicabilidad de los controles, expresado en porcentaje, según el modelo de servicio contratado en la nube. Se realizó una modificación a dicha tabla para que sea identificable qué control es aplicable a cada componente definido en el modelo de arquitectura de seguridad propuesto.

Resumen de la aplicabilidad de cada modelo de servicio	
	Más del 60% de los subcontroles del CIS aplican
	Entre el 60% y el 0% de los subcontroles del CIS aplican
	0%

Aplicabilidad al Modelo de Servicio - CIS Controls Cloud Companion Guide Version 7 Ajustado a la Implementación del Modelo de Seguridad Propuesto según cada Componente					
Control	**Título del Control**	**IaaS**	**PaaS**	**SaaS**	**Componentes Involucrados por Control según el modelo de Seguridad Propuesto**
1	**Inventario y control de los activos de hardware**				Dispositivos
2	**Inventario y control de los activos de software**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
3	**Gestión continua de la vulnerabilidad**				Todos

4	**Uso controlado de los privilegios administrativos**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
5	**Configuración segura para el hardware y el software de los dispositivos móviles, portátiles, estaciones de trabajo y servidores**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
6	**Mantenimiento, supervisión y análisis de los registros de auditoría**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
7	**Protección del correo electrónico y del navegador web**				Dispositivos, Aplicaciones.
8	**Defensas contra el malware**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
9	**Limitación y control de los puertos, protocolos y servicios de la red**				Redes, Infraestructura, Dispositivos
10	**Capacidades de recuperación de datos**				Almacenamiento, Infraestructura
11	**Configuración segura para los dispositivos de red, como cortafuegos, enrutadores y conmutadores.**				Redes.
12	**Defensa de los límites**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
13	**Protección de datos**				Dispositivos, Redes, Infraestructura, Almacenamiento, Aplicaciones.
14	**Acceso controlado basado en la necesidad de saber**				Todos.
15	**Control de acceso inalámbrico**				Dispositivos.
16	**Vigilancia y control de cuentas**				Todos.
17	**Poner en marcha un programa de concienciación y capacitación en materia de seguridad**				Usuarios.
18	**Seguridad del software de aplicación**				Aplicaciones.
19	**Respuesta y gestión de incidentes**				Todos.
20	**Pruebas de penetración y ejercicios de Red Team**				Todos.

Tabla 5 - Fuente: CIS - Applicability Overview for each Service Model. [24]

Cabe aclarar que en el alcance de este documento no se encuentra un análisis detallado de los posibles controles por cada componente o una propuesta a nivel de controles. Actualmente existen varias iniciativas abordando este tema con un alto grado de detalle. Entre las más conocidas se puede citar, por ejemplo, la del CIS [24], la del CSA [25] y la del NIST [42], por mencionar algunas, donde se puede realizar una extrapolación a partir de la arquitectura a implementar, los requerimientos legales y normativos a cumplir y los controles propuestos por estas entidades.

Tomando en consideración lo expresado hasta aquí, se procede a unir todos los conceptos en el modelo de arquitectura de seguridad propuesto. La siguiente tabla muestra integralmente la constitución del modelo de seguridad cloud propuesto, desde el punto de vista del consumidor de soluciones en la nube.

En ella se muestra la relación entre los seis grupos de trabajo definidos previamente. Asimismo, se identifica el orden jerárquico de los módulos de arquitectura, componentes, área de enfoque crítico a nivel operativo y los controles propuestos. Y, por último, se toma en cuenta el flujo de trabajo y aplicación del modelo propuesto y las consideraciones de los principios de diseño y gobierno que trabajan de forma transversal en cada paso de la implementación o evaluación de un ambiente computacional en la nube.

<table>
<tr><td colspan="8">Arquitectura de Implementación</td></tr>
<tr><td rowspan="4">Enfoque desde el punto de vista del consumidor de la nube según el modelo de servicio cloud</td><td colspan="5">Modelo de Servicio en la Nube</td><td rowspan="4">Áreas de Enfoque Critico: Gobierno - CSA</td></tr>
<tr><td colspan="5">Infraestructura como Servicio (IaaS)</td></tr>
<tr><td></td><td colspan="4">Plataforma como Servicio (PaaS)</td></tr>
<tr><td colspan="2"></td><td colspan="3">Servicio como Servicio (SaaS)</td></tr>
<tr><td>Patrones de Diseño</td><td colspan="5">Componentes</td><td></td></tr>
<tr><td rowspan="11">Seguridad Por Niveles

Seguridad en los Componentes

Respuesta a Fallas

Diseño en base a la Elasticidad

Diseño del Almacenamiento

Gestión de Eventos

Automatización</td><td>Almacenamiento</td><td>Infraestructura</td><td>Aplicaciones</td><td>Redes</td><td>Dispositivos</td><td>Usuarios</td><td rowspan="11">Gobernanza y gestión de riesgos empresariales

Asuntos legales: Contratos y descubrimiento electrónico

Gestión de cumplimiento y auditoría

Gobierno de la información</td></tr>
<tr><td colspan="6">Áreas de Enfoque Critico: Operativo - CSA</td></tr>
<tr><td>Seguridad y cifrado de datos</td><td>Seguridad de Infraestructura</td><td>Seguridad de aplicaciones</td><td>Seguridad de Infraestructura</td><td>Seguridad de Infraestructura</td><td>Concientización de Usuarios en Seguridad</td></tr>
<tr><td>Gestión de Claves Criptográficas</td><td>Virtualización y contenedores</td><td>Seguridad y cifrado de datos (En Uso)</td><td>Seguridad y cifrado de datos (En Movimiento)</td><td>Seguridad y cifrado de datos (En Movimiento)</td><td>Acuerdos de Confidencialidad</td></tr>
<tr><td></td><td></td><td>Seguridad de Infraestructura</td><td></td><td></td><td>Gestión del Recurso humano</td></tr>
<tr><td colspan="6">Identidad, derecho y administración de acceso.</td></tr>
<tr><td colspan="6">Respuesta a incidentes, notificación y remediación</td></tr>
<tr><td colspan="6">Plano de Gestión y Continuidad del Negocio</td></tr>
<tr><td colspan="6">Seguridad como servicio</td></tr>
<tr><td colspan="6">Tecnologías relacionadas</td></tr>
<tr><td colspan="6">Controles Aplicables Según Componente - En base a los CIS Controls Cloud Companion Guide</td></tr>
</table>

	Gestión de la vulnerabilidad continua	Inventario y control de los activos de software	Inventario y control de los activos de software	Inventario y control de los activos de software	Inventario y control de los activos de hardware	Vigilancia y control de cuentas	
	Uso controlado de los privilegios administrativos	Gestión de la vulnerabilidad continua	Gestión de la vulnerabilidad continua	Gestión de la vulnerabilidad continua	Inventario y control de los activos de software	Poner en marcha un programa de concienciación y capacitación en materia de seguridad	
	Configuración segura para el software de los dispositivos	Uso controlado de los privilegios administrativos	Uso controlado de los privilegios administrativos	Uso controlado de los privilegios administrativos	Gestión de la vulnerabilidad continua	Respuesta y gestión de incidentes	
	Mantenimiento, supervisión y análisis de los registros de auditoría	Configuración segura para el software de los dispositivos	Configuración segura para el software de los dispositivos	Configuración segura para el hardware y el software de los dispositivos	Uso controlado de los privilegios administrativos	Pruebas de penetración y ejercicios del Red Team	
	Defensas contra el malware	Mantenimiento, supervisión y análisis de los registros de auditoría	Mantenimiento, supervisión y análisis de los registros de auditoría	Mantenimiento, supervisión y análisis de los registros de auditoría	Configuración segura para el hardware y el software de los dispositivos móviles, portátiles, estaciones de trabajo y servidores		
	Capacidades de recuperación de datos	Defensas contra el malware	Protección del correo electrónico y del navegador web	Defensas contra el malware	Mantenimiento, supervisión y análisis de los registros de auditoría		
	Defensa de los límites	Limitación y control de los puertos, protocolos y servicios de la red	Defensas contra el malware	Limitación y control de los puertos, protocolos y servicios de la red	Protección del correo electrónico y del navegador web		
	Protección de datos	Defensa de los límites	Defensa de los límites	Configuración segura para los dispositivos de red, como cortafuegos, enrutadores y conmutadores	Defensas contra el malware		
	Acceso controlado basado en la necesidad de saber	Protección de datos	Protección de datos	Defensa de los límites	Limitación y control de los puertos, protocolos y servicios de la red		

	Vigilancia y control de cuentas	Acceso controlado basado en la necesidad de saber	Acceso controlado basado en la necesidad de saber	Protección de datos	Capacidades de recuperación de datos		
	Respuesta y gestión de incidentes	Vigilancia y control de cuentas	Vigilancia y control de cuentas	Acceso controlado basado en la necesidad de saber	Defensa de los límites		
	Pruebas de penetración y ejercicios del Red Team	Respuesta y gestión de incidentes	Seguridad del software de aplicación	Respuesta y gestión de incidentes	Protección de datos		
		Pruebas de penetración y ejercicios del Red Team	Respuesta y gestión de incidentes	Pruebas de penetración y ejercicios del Red Team	Acceso controlado basado en la necesidad de saber		
			Pruebas de penetración y ejercicios del Red Team		Vigilancia y control de cuentas		
					Seguridad del software de aplicación		
					Respuesta y gestión de incidentes		
					Pruebas de penetración y ejercicios del Red Team		

Tabla 6 - Modelo de Arquitectura de Seguridad Cloud desde el punto de vista del Consumidor. Fuente: Propia.

7- Conclusiones

Como se describió a lo largo de este documento, el paradigma cloud computing cambió la forma de trabajo y consumo de las soluciones tecnológicas, habilitando cada vez más recursos, nuevas tecnologías y soluciones a problemas que anteriormente no eran posibles de remediar. Esto trae consigo nuevos desafíos y retos de seguridad que deben ser tratados de forma integral en cada campo, ya sea técnico o de gestión. Es aquí donde el uso de modelos de seguridad sobre la arquitectura de implementación permite aplicar de forma metódica el concepto seguridad en cualquier sistema de información. Estos brindan una forma fácil y definida de cómo abordar y atacar los problemas de seguridad mediante un proceso estructurado y organizado, apoyado en las buenas prácticas y estándares que las diversas iniciativas nombradas en este documento brindan.

Es esencial conocer todos los aspectos relacionados con la nube, considerando las implicancias de implementar estas tecnologías según las definiciones y características descritas. Esto permite hacer un análisis detallado y pormenorizado de todo lo necesario para la aplicación de la seguridad y ahorrar costos asociados al uso de los servicios.

El constante cambio y complejidad asociado a la nube generan nuevas vulnerabilidades y amenazas que demandan una postura estratégica y holística de la seguridad en todos los campos de acción. Para lo cual, es obligatorio hacer uso de novedosos enfoques que permitan simplificar la complejidad del entorno cloud y generen los requisitos específicos en cada campo de acción.

No es posible implementar la seguridad de forma tradicional en entornos cloud debido a su constante cambio. Por lo cual es ineludible el uso de patrones de diseño seguro que direccionen las soluciones de seguridad y garanticen que son acordes a los retos que propone un ambiente tan dinámico y cambiante como es la nube.

Lo anterior aplicado en base al modelo de arquitectura de seguridad propuesto, responde a la necesidad de integrar el factor seguridad en cada paso del proceso, aprovechar las facilidades de la nube y manejar las

implicancias de seguridad que tienen las implementaciones en este ambiente.

El factor de corresponsabilidad sobre la infraestructura tecnológica entre el consumidor y el proveedor de servicios es un factor de riesgo decisivo para la adopción del cloud computing. Por ello, tener en consideración el alcance y los límites de los proveedores de servicios en la nube, la responsabilidad propia según el modelo de servicio contratado y conocer en detalle las funcionalidades y características de los entornos cloud, permiten tener un contexto claro y hacer uso de la mayor cantidad de herramientas posibles para garantizar el cumplimiento de los requisitos de seguridad por parte del CSP sobre los servicios contratados, así como, tener control, visión y gestión de la infraestructura en la nube.

El modelo de arquitectura de seguridad propuesto permite desglosar por componentes básicos e identificar de una manera simple los objetivos y requisitos a nivel de seguridad que deban satisfacerse. Con ello, también facilita detectar las relaciones entre estos componentes y cómo dicha relación implica nuevos riesgos de seguridad, sin dejar de lado un enfoque holístico de todo el sistema.

El modelo propuesto establece un proceso de análisis y gestión de la seguridad de la información en entornos cloud de manera integral, sin dejar de lado los aspectos como la gobernabilidad, la gestión del riesgo, el marco legal y normativo aplicable o la mejora continua. Dado su modo de abstracción sencillo, basado en componentes y la aplicación de seguridad a partir de patrones de diseño, permite la aplicación de este modelo en cualquier sistema de información en la nube, convirtiéndose así en una herramienta esencial para el sistema de gestión de la seguridad de la información de cualquier entidad.

Dicho modelo de seguridad, además de aplicar un concepto sencillo y de fácil implementación para cualquier arquitectura de implementación teórica, aplica el concepto de cero confianza, garantizando que la implementación de soluciones cloud cuente con un enfoque orientado a los factores críticos que hacen a la seguridad. Esto ayuda a la priorización de

los requerimientos a nivel técnico, normativo, legal, operativo y de gobierno sin que esto impida la implementación de soluciones cloud.

La información recopilada y descrita en este documento, brinda información de valor a las organizaciones para la gestión de los nuevos riesgos de alto grado de complejidad asociados al entorno cloud, los factores críticos de éxito y lineamientos de seguridad a considerar, ya sea para la implementación de soluciones cloud seguras o para la evaluación de seguridad de estos ambientes. Estos elementos permiten mejorar la competitividad y alinearse con el avance acelerado del cloud computing.

8- Anexos

Anexo A

El NIST [18] brinda las consideraciones necesarias para la seguridad en la nube. A continuación, se describen y se detallan dichos riesgos usados para este trabajo.

Falta de Gobernanza: Como lo cita el NIST [18], en la sección 4.1, el concepto de gobernanza implica el control y la supervisión, por parte de la organización cliente, de las políticas, procedimientos y normas para el desarrollo de aplicaciones y la adquisición de servicios de tecnología de la información, así como el diseño, la aplicación, el ensayo, la utilización y la vigilancia de los servicios desplegados o contratados. Esto refiere a que en el entorno cloud esta gestión es de especial relevancia. La falta de control y visibilidad de los procedimientos, desarrollo e implementaciones en la nube implican un riesgo general. Por lo cual las herramientas de auditoría y monitoreo, el conocimiento en detalle del proceso de gestión de los activos de información, el cumplimiento de las políticas de seguridad y el conocimiento de los roles y responsabilidades son elementos esenciales.

Otro tema a destacar es la gestión del riesgo en el entorno cloud. Es necesaria la implementación de un correcto proceso de gestión de riesgos que entienda y vaya de la mano con la flexibilidad y constante evolución de estas tecnologías y que, de la misma manera, asegure el cumplimiento de los requerimientos de la entidad en todos los campos de trabajo.

Riesgo de Cumplimiento: Para el NIST [18], el cumplimiento de las normas, marcos legales y cláusulas contractuales son un tema que difiere según la locación de cada organización. Por lo cual se hace difícil llevar a cabo el correcto cumplimiento de estos requisitos. Las leyes y regulaciones de cada país especifican normativas y necesidades diferentes frente a cómo debe efectuarse el tratamiento de la información. Entendiendo lo explicado anteriormente, uno de los temas más importantes es la ubicación de los datos y los mecanismos de protección. Por la propia naturaleza de la nube, este tópico muchas veces es muy difícil de satisfacer. Al transportar los datos entre diferentes países, aplican diferentes marcos legales y esto afecta

al tratamiento de los datos. Esto también implica términos diferentes de la privacidad de la información, por lo cual acarrea riesgos a nivel de privacidad, acceso y manipulación de los datos.

Otro punto de alta relevancia es la investigación electrónica. En este ítem se maneja la identificación, colección, procesamiento, análisis y producción de información electrónicamente almacenada para procedimientos judiciales. El cumplimiento de requerimientos de auditoria y acceso a información bajo un entorno jurídico, implica el acceso a datos y metadatos[7] en diferentes formatos. En un ambiente cloud no es fácilmente rastreable y gestionable este requerimiento por el constante movimiento de la información, además de temas como la sobre-escritura de los metadatos, falta de trazabilidad o en ocasiones, acciones deliberadas por parte de los proveedores cloud, de la información almacenada, hacen que la labor de investigación electrónica no pueda ser cumplida.

Exceso de Confianza: Como se mencionó antes, un aspecto vital es la clara definición de los roles y responsabilidades en la nube. La confianza en la tercerización no indica mayor seguridad de la información. En este aspecto, el acceso a los datos por personal no autorizado es uno de los riesgos con mayor presencia. Se debe tener en cuenta que las amenazas y vulnerabilidades son parte de los servicios de este entorno. Terceros, otros clientes de los proveedores de servicios cloud, consumidores de servicios, externos y los usuarios internos pueden vulnerar y amenazar la seguridad de la organización cliente. Por lo cual, se amplía la cantidad de los posibles actores en un fallo de seguridad sobre los datos. Los incidentes causados por usuarios internos o terceros como proveedores o similar, son cuantificados por el NIST [18], como uno de los riesgos más comunes. De este conjunto, los incidentes de privacidad e indisponibilidad son los más presentados.

Propiedad de los Datos: La definición clara de los derechos y deberes sobre los datos son el eje principal para la propiedad de los datos.

[7]Metadatos: Son un conjunto de datos que describen el contenido informativo de un recurso, de archivos o de información de los mismos. Es decir, es información que describe otros datos. [47]

La falta de entendimiento y no declaración explicita de la propiedad de los datos genera ambigüedad y se presta para el uso de la información para otros fines. Por lo cual es imprescindible que el consumidor declare expresamente la propiedad de los datos y metadatos y de la misma manera, revise en detalle cualquier medio posible del que el proveedor pueda hacer uso para la utilización de los datos de la organización.

Complejidad en los Servicios: Otro tema a tratar es el control de los servicios compuestos de la nube. Como se vio anteriormente, estos servicios en sí, están compuestos y dependen de otros servicios para su funcionamiento. Esto se convierte en sí mismo en un problema para el entendimiento de responsabilidad de los terceros dueños de los servicios que hacen parte de un servicio compuesto, en caso de presentarse incidencias asociadas a estos servicios. Esto requiere de un marco que garantice la disponibilidad y control de cualquier tercero que esté involucrado con la prestación de los servicios y gestión y propiedad de los datos.

Carencia de Visibilidad: La tercerización de la infraestructura y servicios no significa trasladar la competencia sobre estos ítems. Usualmente al migrar centros de datos y servicios a la nube, también se debe ceder la gestión de procesos operativos y de seguridad, perdiendo visibilidad de estas labores. De la misma manera, los proveedores de servicios en la nube no brindan información en detalle de los procedimientos que se realizan para el mantenimiento de los servicios contratados. Esto recae en una falta de visibilidad y pérdida de control sobre los activos de información. Para esto, determinar los límites, conocimiento de alertas e incidencias, informes de gestión, cumplimiento de las políticas corporativas, entre otros, deben ser estipulados por las partes antes de adquirir servicios en la nube.

Datos Auxiliares: Para el control y gestión de los consumidores de los servicios cloud, los proveedores controlan datos que pueden ser usados para ataques, accesos no permitidos, explotación de vulnerabilidades y otros. Otro uso de estos datos puede ser el conocimiento de la operatividad de los clientes a partir de los registros operativos que se generan del propio

uso del servicio. Esto implica una violación a la privacidad de la entidad y uso indebido de los datos. Por lo cual, en este punto se debe tener una definición clara de la propiedad de los metadatos adquiridos y creados por el proveedor y definir los derechos de esta sobre ellos.

Falta de la gestión de los riesgos: La gestión del riesgo es un pilar fundamental en la seguridad de la información que no debe depreciarse al contratar servicios en la nube. Dicha gestión presenta desafíos tales como la falta de control de los sistemas de información, el manejo de expectativas equivocas, el exceso de confianza y la falta de definición de los requerimientos de seguridad de la organización cliente. Dado que una vez presentado algún incidente de seguridad, las consecuencias no podrán evitarse, el consumidor debe hacer conocer y acordar con el proveedor de servicios los requisitos de seguridad y la implementación de controles que mantengan el nivel de riesgo por él definido.

Problemas de Arquitectura: Como ya se describió en el capítulo anterior, la arquitectura cloud hace uso de varios componentes, tanto físicos a nivel de hardware como virtuales y de software, que permiten brindar los servicios. Esto requiere una orquestación general en diferentes capas y una comunicación integral en todos los niveles, inherente a lo cual se presentan una serie de vulnerabilidades. Esta complejidad tecnológica requiere implementación de fuertes controles y procedimientos de seguridad sobre todo el sistema, además del uso de estándares y buenas prácticas de seguridad. De la misma manera, la parte contratante debe tener pleno conocimiento y seguridad de que el proveedor hace uso e implementa correctamente estos marcos de referencia.

Superficie de ataque: En los servicios en la nube, la virtualización genera nuevas vulnerabilidades a explotar, ya que hipervisor, componente que permite la virtualización, se encuentra entre los recursos físicos y los virtuales, siendo punto crucial para la prestación de los servicios. Interfaces de programación y comunicación forman parte de estos puntos que aumentan la superficie de ataque que puede ser usada para generar incidentes de seguridad. Muchos de estos elementos y características son

vulnerables a ataques de diferentes índoles o podrían tener vulnerabilidades aun hoy sin descubrir. Por lo tanto, deben ser protegidas con especial cuidado por el grado de criticidad que tiene al presentarse una falla en ellos.

Protección de Redes Virtuales: La virtualización permite no solo la creación de servidores, sino la creación de redes y elementos de red virtuales para la comunicación entre los dispositivos que hacen a la infraestructura cloud de los clientes. Esto deriva en problemas de visualización de los datos en tránsito sobre estas redes virtuales y así mismo no es posible detectar incidencias de seguridad por los controles de seguridad físicos implementados.

Definición de Roles Operativos: Una mala práctica que se utiliza en entornos cloud es la falta de definición de roles operativos para la administración es este tipo de ambientes. Usualmente se agrupan las responsabilidades de telecomunicaciones, infraestructura, almacenamiento y hasta seguridad en un solo rol. Esto genera falta de controles operativos y técnicos.

Imágenes de Máquinas Virtuales: Las imágenes virtuales permiten la implementación rápida de servidores configurados de una forma estándar. Sin embargo, estas imágenes deben ser actualizadas constantemente ya que si se hace uso de imágenes desactualizadas es posible tener vulnerabilidades ya conocidas y resueltas. Así mismo, estas imágenes podrían contener código embebido con vulnerabilidades asociadas que podrían ser explotadas por una amenaza. Este proceso debe ser controlado por el cliente en pro de la corrección de esta vulnerabilidad.

Protección del lado del Cliente: Este riesgo hace referencia a las amenazas y vulnerabilidades asociadas a los dispositivos y aplicaciones que utilizan los clientes para acceder a los recursos en la nube. Extensiones, librerías, plugins y otros elementos cuentan con vulnerabilidades, las cuales en muchos casos este estado se agudiza al no ser dispositivos actualizados y gestionados a nivel de seguridad. Adicionalmente, el nuevo auge de hacer uso de los dispositivos personales para la gestión corporativa hace aún más difícil el control de la información gestionada en estos dispositivos. Desde la

pérdida de los dispositivos hasta la posibilidad de que sean vulnerados por algún tipo de malware, podría provocar fuga o perdida de información sensible.

Protección del lado de los Servidores: Usualmente no se utilizan buenas prácticas en la administración de servidores tales como la configuración correcta y a medida, según los servicios brindados, la separación de ambientes, la segmentación de las redes y la aplicación de controles fuertes de seguridad, entre otros. Del mismo modo, procedimientos de actualización débiles o inexistentes, carencia de auditorías y de control de cambios, y otros, generan nuevas brechas de seguridad.

En este punto, es también importante resaltar que en muchos casos los clientes de la nube no cuentan con planes de recuperación ante desastres y continuidad de negocio, tampoco se piensa en alta disponibilidad que debería tener todo entorno productivo según su criticidad. Por último, el desconocimiento del uso de las herramientas que tienen los diferentes proveedores de la nube o la mala configuración de estas, generan más problemas que soluciones.

Problemas de Identidad y Control de Acceso: Uno de los riesgos más habituales en el uso de esta tecnología es el acceso no autorizado. La falta de mecanismos fuertes de identificación y autenticación de los usuarios, tales como el uso de múltiples factores, así como la falta de implementación de control sobre los accesos a todos los recursos, ya sea por impedimento técnico o dificultad de implementación, hacen que se genere este riesgo. Para este tema se deben considerar los siguientes tópicos:

Autenticación: Los proveedores cloud hoy en día se orientan a la federación de la identidad mediante servicios alineados con la arquitectura de sus sistemas. Estas soluciones hacen uso de una serie de protocolos, como por ejemplo el SAML, para la comunicación e intercambio de información, los cuales deben ser configurados de forma detallada en lo que se refiere a seguridad. Estos protocolos son fuertemente atacados en búsqueda de nuevas vulnerabilidades y así ganar acceso a los recursos que se valen de ellos para la autenticación entre diferentes entornos.

Control de Acceso: En este sentido, es necesario que se mantenga controlado el acceso a los recursos. Es decir, que el usuario solo pueda utilizar el acceso otorgado y que no le sea posible elevar sus privilegios o acceder a recursos no permitidos inicialmente. Políticas no específicas, diseño de protocolos débiles y falta de controles efectivos para el control de acceso hacen que el tráfico generado para comunicar, validar y brindar permisos pueda ser manipulado y usado para otros fines.

Aislamiento del Software: Una labor compleja en todo sentido y es una de las características fundamentales del cloud computing. El proveedor debe ser capaz de mantener el ambiente de cada uno de sus clientes separados entre sí y, además, de mantener control y gestión sobre todas las capas de la prestación de los servicios de la nube. La alta tasa de conexión a un solo recurso físico, la separación de ambientes de forma virtual y la ejecución de una gran cantidad de servicios generan que estas características y funcionalidades sean objeto de ataques de diferentes formas. A continuación, se nombra los más importantes.

Ataques al Hipervisor: Se refiere a los ataques dirigidos al kernel[8] ya que este controla y ejecuta todos los procesos que son necesarios para llevar a cabo la virtualización. También se encarga de generar la separación entre las diferentes máquinas virtuales que se ejecutan sobre el dispositivo físico, además de efectuar labores de monitoreo, optimización y administración central. En consecuencia, el hipervisor es un dispositivo complejo en todos los aspectos y a nivel de seguridad informática. Esta complejidad hace que sea difícil de entender, caracterizar y gestionar sus riesgos asociados.

Ampliación de Vectores de Ataque: La capacidad de que la nube sea multiusuario a nivel de máquinas virtuales y la relación estrecha que se tiene con los recursos físicos aumenta las posibles fuentes de amenaza. Además, se debe tener en cuenta la portabilidad que tienen las máquinas virtuales

[8] Kernel: Es un software que constituye una parte fundamental del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora. Es el encargado de gestionar recursos, a través de servicios de llamada al sistema. También se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. [28]

entre los recursos físicos, lo cual aumenta la potencial materialización del riesgo y su propagación. Por ejemplo, la ejecución de código malicioso desde los servidores virtuales puede llegar hasta el hipervisor, generando una falla de seguridad masiva sobre los servicios gestionados por este. Otro elemento común como vector de ataque son las interfaces de programación de los servicios cloud. Estas interfaces cuentan con ciertas debilidades al hacer el procesamiento de código. Por ejemplo, falta de cifrado de datos, vulnerabilidades asociadas a la inyección de código mal intencionado o autenticación débil.

Otro tipo de ataques como el del Hombre en el Medio (Man-in-the-middle, en inglés), modificación de memoria, explotación de vulnerabilidades Zero-day[9], ataques de movimiento lateral, ataques indirectos a los servicios cloud, entre otros, pueden generarse en el entorno cloud.

Los ejemplos anteriores permiten identificar que muchas de las nuevas funcionalidades y tecnologías adoptadas en la nube generan una ampliación de los posibles vectores de ataque. Por lo cual, se debe tener conocimiento en detalle del ambiente cloud como de las funcionalidades usadas para así poder mitigar los riesgos asociados.

Protección de los Datos: Como se indicó anteriormente, los datos de todos los clientes de la nube son almacenados en diferentes sitios compartidos. En esta práctica se presenta un riesgo en el procedimiento de acceso y gestión de los datos y es necesario asegurar su correcto aislamiento y protección. Se debe tener en cuenta lo siguiente:

Aislamiento de los datos: La información se presenta en un sinfín de formatos, tanto en los correspondientes a entradas y salidas de las aplicaciones al momento de la ejecución, como el usado en el código de la aplicación, o los de las bases de datos, archivos y demás. Asimismo, su procesamiento y ciclo de vida genera cambios en ella y usualmente debe ser accedida por usuarios en un momento y estado especifico. Esto genera que

[9] Zero-Day: Es una nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre 0-day (día cero) se debe a que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad. Estas a veces se usan junto a los troyanos, rootkits, virus, gusanos y otros tipos de malware, para ayudarlos a propagarse e infectar más equipos. [29]

la autenticación de los usuarios tome especial relevancia. Típicamente, en los entornos cloud, las bases de datos son accedidas desde una única instancia y se controla el acceso a los datos mediante etiquetas en estos. Esto genera una falsa seguridad de segregación de acceso a los datos ya que, una configuración errónea puede generar un acceso no controlado a información sensible. Otro tema crucial es la protección y control de acceso de los datos dependiendo de su estado. Una mala configuración o los excesos de confianza muchas veces generan que los datos vayan sin cifrar o cifrados con configuraciones débiles, lo cual es un riesgo latente.

Saneamiento de los Datos: Tanto para el consumidor como para el proveedor es importante que se realice una correcta eliminación de los datos cuando un repositorio deja de ser utilizado. Esto es válido para todos los repositorios, ya sea los de uso recurrente, de respaldo, con finalidad de migración y demás. En este caso, el riesgo se encuentra en la incorrecta o parcial eliminación de la información ya que, en la nube por su propio dinamismo, la información en diferentes estados puede ubicarse en diferentes equipos de almacenamiento, lo cual hace que su eliminación sea compleja. La no trazabilidad o el uso de herramientas para la recuperación de información eliminada con anterioridad hacen de esta labor un factor crítico de riesgo.

Concentración de valor: Los datos en sí mismos son y generan un alto valor y al estar concentrados masivamente son objetivo de ataque por excelencia. Hoy en día se hace uso de una amplia gama de ataques en pro del robo de información, desde el uso de malware, ingeniería social, phishing o el uso en conjunto de diferentes ataques. Desde el acceso a los repositorios de información hasta el robo de las cuentas administrativas de los ambientes en la nube son los riesgos más comunes. También, los datos de otros clientes pueden verse afectados y los nuevos ataques ser dirigidos a otros consumidores.

Problemas de Disponibilidad: Esto refiere a la imposibilidad de acceso a los recursos y servicios de un cliente. La disponibilidad puede ser afectada por inconvenientes de acceso temporal o permanente. Las

amenazas por ataques Zero-day o ataques de denegación de servicio a infraestructuras críticas son las más comunes, u otras, como desastres naturales, se encuentran como riesgos potenciales. A continuación, se detallan algunos de estos incidentes:

Incidentes temporales: Si bien las infraestructuras cloud están construidas de tal forma que cumplan con un alto nivel de disponibilidad, pueden verse afectadas por temas de rendimiento y fallos sobre sus elementos principales como los centros de almacenamiento, inconvenientes por actualizaciones, fallos sobre los hipervisores o los canales de conexión. Usualmente la disponibilidad está garantizada contractualmente por los acuerdos de servicios especificados. Sin embargo, esto no asegura que se cumpla.

Incidentes permanentes o prolongados: Estos incidentes están más relacionados con incidentes legales, como puede ser el decomiso de equipos de la infraestructura cloud por temas de investigación judicial, la seguridad financiera de los proveedores de servicios o pérdida de las relaciones contractuales con los proveedores de la nube.

Denegación de servicio: El objetivo de un ataque de denegación de servicio es lograr la saturación de un servicio o dispositivo para que este no pueda prestar los servicios de forma adecuada degradando su calidad o produciendo una interrupción completa. Usualmente se hace uso de Botnets[10] que buscan a partir de diversas formas como, por ejemplo, el envío de múltiples solicitudes desde diferentes puntos y en un corto tiempo de forma repetitiva a un único objetivo, buscando que este degrade su servicio. Esto no implica que solo se presenten este tipo de ataques de forma externa, también se puede presentar de forma interna, usualmente bajo la misma filosofía.

Respuesta a Incidentes: Como se mencionó antes, la seguridad no es un tópico que se terceriza. Es común que los proveedores de servicios en

[10] Botnets: Es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un usuario malicioso o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. Los ordenadores son parte del botnet, llamados “bots” o “zombies”. [27]

la nube tengan una respuesta básica y limitada ante los incidentes de seguridad presentados. Por lo cual, actividades como el análisis, respuesta y contención, análisis forense, recolección de evidencias, aplicación de controles, implementación de soluciones y restauración del servicio, usualmente sean responsabilidad del cliente. Esta labor toma un nivel de complejidad más alto por la gestión compartida que se tiene y la propia complejidad de la nube. Usualmente una inadecuada segregación de funciones y términos débiles en la gestión de incidentes en el proceso contractual, se convierte en un riesgo en este tema. Por otro lado, la gobernabilidad sobre los datos, según su lugar físico, es otro tema que debe ser declarado tácitamente a nivel contractual. Es aquí donde se debe asegurar la colaboración y participación de las partes para la resolución de cualquier incidente que pudiera presentarse.

Anexo B

A continuación, se describen y se detallan las amenazas, vulnerabilidades y riesgos descritos por el CSA [2] usadas para este documento.

La siguiente información forma parte de una serie de publicaciones del CSA en la cual se busca informar y concientizar sobre las principales amenazas, vulnerabilidades y riesgos del cloud computing. Esta es la CSA Top Threats to Cloud Computing [1]. A continuación, se describen los 11 puntos en consideración.

Brecha de Datos: Se refiere al acceso no autorizado, divulgación, robo o uso no adecuado de la información de cualquier entidad. Usualmente generada a partir de un incidente de seguridad tal como un error; de un proceso provocado, el cual puede hacer uso de vulnerabilidades, por ejemplo, sobre los servicios que se consumen; o bien por malas prácticas de seguridad. Como resultado se puede perder información sensible, afectar la reputación de la entidad, acarrear costos monetarios generados por diferentes conceptos tales como, respuesta y recuperación del incidente,

aspectos legales, contractuales y de regulación. Para la mitigación de este riesgo, se recomienda lo siguiente:

1. Clasificación de los activos de información.
2. Correcto control de acceso a la información clasificada en todo el ciclo de vida.
3. Asegurar la información accesible desde Internet buscando falencias de configuración o vulnerabilidades asociadas a la tecnología en uso.
4. Cifrado de los datos.
5. Asegurar el correcto funcionamiento de un plan de respuesta dado un incidente de seguridad y contar con un plan de continuidad del negocio.

Problemas de Configuración e Inadecuado Control de Cambios: Dado el dinamismo y ventajas con el que cuenta la nube, también permite con una mayor facilidad generar errores de configuración sobre las tecnologías en uso. Algunos ejemplos son: el uso de credenciales por defecto, la falta del adecuado manejo de los permisos según el rol que se desempeñe o bien el almacenamiento de datos de manera insegura. Asimismo, los tradicionales controles de cambio muchas veces no son suficientes para manejar la complejidad que se encuentra en los entornos cloud. Esto conlleva a trasgresiones o incidencias, por no contar con un proceso de cambio sólido, como la falta de controles de seguridad estándar o configuraciones débiles como las anteriormente nombradas que derivan según el ambiente afectado a diferentes impactos para la entidad. En este punto el CSA recomienda lo siguiente:

1. Automatización de procedimientos en diferentes niveles asegurando la aplicación de controles de seguridad según la necesidad de la entidad.
2. Uso de tecnologías que continuamente busquen problemas de configuración sobre los recursos en la nube.
3. Solución de los problemas en tiempo real.

4. Hacer uso de seguridad a nivel de aplicación e interface.
5. Mejora de los procesos de control de cambios y configuración adaptados a la nube.

Falta de Estrategia y Arquitectura de seguridad en la Nube: Este riesgo se presenta cuando las entidades encaran el reto de migrar parte o toda su infraestructura y servicios implementados “en sitio” a un entorno cloud. Con ello se plantea la necesidad de la creación de una arquitectura de seguridad acorde para este nuevo entorno. En muchos casos, no se cuenta con el conocimiento ni los procedimientos adecuados, lo cual provocará decisiones estratégicas erróneas y arquitectónicamente deficientes, muchas de ellas generadas por la necesidad de una rápida migración, dejando en un segundo plano la seguridad.

Otro tema relevante es la responsabilidad compartida que se encuentra implícita en el uso de esta tecnología. No tener en claro los alcances y limitaciones como las responsabilidades de los actores en la nube, dan lugar a brechas de seguridad fácilmente explotables. En relación a lo mencionado anteriormente se recomienda lo siguiente:

1. Hacer uso de las herramientas brindadas por la nube como aplicaciones e interfaces de seguridad.
2. Plantear una arquitectura acorde al entorno cloud y alineada con los objetivos del negocio.
3. Crear y establecer un marco de seguridad de la información en el cual se cuente con la gobernanza y una correcta gestión del riesgo.
4. Mantener actualizada toda la infraestructura y herramientas de virtualización, con especial atención a la infraestructura de seguridad.
5. Mantener un monitoreo constante ante las nuevas amenazas y un lineamiento claro de seguridad.

Insuficiente gestión de identidades, credenciales, acceso y claves: A partir del cambio de entorno, las tradicionales formas de manejo de identidades y accesos cambian. Este proceso en sí tiene su propia complejidad en la nube privada, y aún más en la nube pública por su característica de amplio acceso a la red y la necesidad de confiar en múltiples entidades que cuentan con procedimientos diferentes para la gestión de identidades y accesos, además de la complejidad del mantenimiento que requiere. Es de vital importancia ser estrictos, verificar la identidad y dar autorización a los recursos y accesos correctos. Errores típicos en esta labor como hacer uso de contraseñas débiles, no contar con múltiples factores de autenticación, la falta de cambio continúo de las contraseñas y certificados, no contar con herramientas informáticas escalables de gestión de identidad, credenciales y acceso derivan en no poder verificar de forma íntegra la identidad de la parte que solicita el acceso al servicio de la nube, y asignar los derechos incorrectos al conceder los accesos. En este punto se deberá tener en cuenta lo siguiente:

1. Correcta federación y preservación de la integridad del proveedor de identidad y sus fuentes autorizadas.
2. Niveles adecuados de confianza entre los actores de la nube.
3. Claves criptográficas y credenciales deben ser resguardadas correctamente bajo una fuerte infraestructura de claves.
4. Manejo de múltiples factores de autenticación y hacer uso de políticas de contraseñas fuertes y de rotación periódica.
5. Los sistemas de gestión de identidades deben ser automatizados asegurando que las tareas operativas como la baja, alta y modificación de usuarios, así como las de mantenimiento sean realizadas a tiempo.
6. Protección y monitoreo sobre los sistemas de gestión y protección de identidades.

Secuestro de Cuentas: Esta amenaza hace uso de varios métodos para lograr el objetivo de obtener cuentas de acceso a la nube, tales como

phishing[11], cross-site scripting[12] y un gran número de vectores de ataque y vulnerabilidades que se descubren día a día. Usualmente, cuando se adquiere una cuenta legítima de acceso a la nube, se hace uso de ella para ejecutar otros ataques que derivan en el compromiso de información sensible, incidencias de integridad y disponibilidad de la información y los servicios, daño en la reputación de la entidad y más. Teniendo en cuenta esto, las cuentas asociadas con la gestión, control y administración de la nube son las de mayor riesgo por sus niveles de acceso y autorización. En este sentido, se debe implementar controles de defensa en todos los niveles para minimizar el riesgo de robo de cuentas o suplantación de identidad. Esto incluye la correcta concientización de los usuarios sobre este tipo de amenazas. Se recomienda tener en cuenta lo siguiente:

1. Contar con un plan de continuidad del negocio.
2. Control sobre la gestión y el ciclo de vida de las credenciales.
3. Aplicaciones para análisis de eventos, de detección y prevención de intrusiones.
4. Correcto aislamiento de ambientes.
5. Segregación a detalle de permisos según sus roles.
6. Capacitación de los usuarios.

Amenazas Internas: Entendiendo a la nube como una infraestructura crítica para cualquier organización. Se debe hacer un correcto análisis de riesgos teniendo en cuenta cualquier tipo de amenaza, ya sea externa o interna. Las amenazas internas son aquellas que potencialmente pueden

[11] Phishing: El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. [55]

[12] Cross-Site Scripting (XSS): Es una vulnerabilidad de seguridad que permite a un atacante colocar scripts del lado del cliente (normalmente JavaScript) en páginas web. Cuando otros usuarios cargan las páginas afectadas, los scripts del atacante se ejecutan, lo que permite al atacante robar cookies y testigos de sesión, cambiar el contenido de la página web mediante la manipulación de DOM o redirigir el navegador a otra página. Las vulnerabilidades del XSS suelen producirse cuando una aplicación toma las entradas del usuario y las envía a una página sin validarlas, codificarlas o escapar de ellas. [41]

materializar un riesgo a partir de los accesos autorizados. Dichas amenazas, muchas veces desconocidas por la organización cliente, tienen un alcance y repercusiones en varias ocasiones no cuantificables. Se hace demandante, antes de confiar en cualquier proveedor de servicios en la nube, hacer un análisis pormenorizado de los activos de información de la entidad en la nube. De la misma manera, se debe tener presente que estas amenazas también pueden ser internas dentro del círculo de confianza de la compañía cliente, ya sea personal contratado directamente o un tercero. No necesariamente intencional, muchas veces por desconocimiento o negligencia, se hacen realidad estos eventos generando un impacto negativo para dicha organización cliente como degradación o pérdida de información, eventos de indisponibilidad, y otros. Es importante tener en consideración las siguientes recomendaciones:

1. Estrategia de confianza cero en lo posible.
2. Correcta capacitación de los usuarios y acuerdos de responsabilidad.
3. Segregación de funciones y roles con la mayor granularidad posible.
4. Gestión del ciclo de vida de la información y seguridad de los datos.
5. Gestión de cifrado de la información y manejo de claves de cifrado.
6. Correcto aislamiento de ambientes.
7. Auditorias de terceras partes.
8. Apoyo contractual para asegurar el control y la autoridad efectiva sobre el proveedor de servicios según las necesidades del consumidor.

APIˊs Inseguras: Las API permiten gran parte de la interacción, funciones e intercomunicación entre los diferentes sistemas y aplicaciones que se usan diariamente y el acceso e interconexión entre los diferentes servicios. En la nube son ampliamente usadas, ya sea para la gestión y comunicación interna como para la gestión con los consumidores. Esta solución intrínsecamente cuenta con una amplia gama de vulnerabilidades y amenazas asociadas, ya sea por su mala codificación, sus interfaces

inseguras, o la falta de verificación; razón por la cual se convierte en un perfecto vector de ataque.

1. Verificación y aprobación de las API´s.
2. Cifrado de las comunicaciones.
3. Monitoreo de eventos generados.
4. Análisis en detalle de las API´s a usar.
5. Uso de prácticas seguras de desarrollo para la creación de API´s.

Plano de Control Débil: Esta amenaza se define como un servicio de la nube que no cuenta o no proporciona controles de seguridad adecuados para los requerimientos del cliente. Por lo cual, dichos clientes deben hacerse cargo de la implementación y la responsabilidad de estos controles antes de migrar su información y hacer uso de los servicios contratados. Tener un correcto plan de protección basado en una apropiada evaluación de riesgos se hace vital para minimizar cualquier riesgo asociado. Hacer un análisis del plano de control en la nube, conocer el flujo de los datos, entender sus vulnerabilidades y amenazas e implementar los controles adecuados en todos los niveles, dará un grado de confiabilidad a la hora de migrar y hacer uso de la nube. Así mismo, asegurarse que los proveedores de la nube cuenten con un entorno seguro para la prestación de los servicios y apoyarse a nivel contractual y legal sobre las responsabilidades adquiridas por estos, es esencial como apoyo para la solución de varios frentes de amenazas. En este punto, Se sugieren los siguientes controles:

1. Correcta arquitectura de la solución en la nube.
2. Plan de auditoria y conocimiento de la regulación aplicable según sea el caso.
3. Correcta documentación de procesos y procedimientos.
4. Gobierno y Gestión de riesgos.
5. Implementación de controles adecuados según sea la necesidad.

6. Análisis de eventos y monitoreo constante.

Fallas en la Meta-estructura y la Apli-estructura: Dada la complejidad del cloud computing y su rápida evolución, es difusa en muchos aspectos la responsabilidad entre el cliente y el proveedor. Dependiendo del tipo de servicio consumido, se generarán duplicación de responsabilidades a nivel de seguridad. Un ejemplo de esto es la contratación de infraestructura como servicio (IaaS) ya que, si bien el proveedor es responsable sobre la infraestructura física y lógica, el cliente es responsable de la infraestructura virtual que yace encima de esta. Así mismo, las API´s juegan un papel transversal en la nube, ya que estas pueden desplegar y ejecutar diferentes tareas de seguridad necesarias y de interacción con el consumidor en múltiples niveles. Es aquí donde se observa con mayor claridad la necesidad de la segregación y delimitación de roles y responsabilidades. Como referencia, el CSA indica que para el proveedor de servicios cloud, el límite será la capa de la meta-estructura.

Teniendo en cuenta lo anterior, una mala implementación por parte del cliente como una incorrecta migración de su infraestructura hasta implementación de API´s inseguras por parte del proveedor, concluirá en incidencias de seguridad con repercusiones a nivel de servicio y de la información. Para esta amenaza se recomienda lo siguiente:

1. Correcta implementación de aplicaciones, servicios y controles orientados a la nube.
2. Correcta visibilidad y conocimiento de los mecanismos de mitigación ofrecidos por el proveedor.
3. Conocimiento del sistema de reporte de incidencias.
4. Buenas prácticas de seguridad como implementación de API´s seguras, correcta segmentación en todos los niveles, protección de datos, cifrado, gestión de acceso, control de configuración y gestión del ciclo de vida de la información, entre otros.

5. Auditorías y pruebas de penetración sobre las implementaciones de los clientes, exigiendo al proveedor que realice las mismas actividades sobre el ambiente cloud.

Visualización Limitada del Uso de la Nube: Se debe tener visibilidad sobre la nube como principio para una correcta gestión de la seguridad, ya que solo se puede asegurar lo que se conoce. Es decir, para poder asegurar cualquier ambiente tecnológico se debe conocer el sistema como un todo, los elementos que lo componen en detalle y cómo estos elementos interactúan entre sí.

El CSA hace hincapié en conocer en detalle tanto el uso autorizado como el no autorizado de los servicios contratados en la nube. Las grandes facilidades y la rapidez con las que se pueden implementar ambientes para procesar los activos de la información de cualquier consumidor, impiden tener un control granular sobre las actividades realizadas en la nube.

Adicionalmente a esto, se debe tener en cuenta que la nube minimiza la necesidad de garantizar la alta disponibilidad de la infraestructura que procesa los datos ya que el proveedor, dado un incidente, puede desplegar de forma rápida toda una infraestructura y llevar a cabo todas las actividades necesarias para su resolución. Sin embargo, este tipo de acciones deben estar en conocimiento del consumidor y alineadas con sus objetivos, así como implementadas según sus requerimientos de seguridad.

Un ejemplo de visibilidad limitada es el desconocimiento de alguna característica que no fue tenida en cuenta al inicio de la implementación, lo cual la puede retrasar porque el proveedor no tiene la capacidad de adaptación necesaria a los nuevos requerimientos o eventos. Otro ejemplo es el uso inadecuado del amplio acceso a la red y la falta de control sobre los dispositivos propios de los colaboradores del cliente, ya que muchas veces la información corporativa se almacena en estos dispositivos o en otros sistemas, fuera del alcance y control de la organización.

De nuevo, una buena arquitectura de seguridad se hace vital para evitar este tipo de eventos. La definición clara de políticas, alcance, procesos y procedimientos al trabajar en la nube es esencial, la concientización y compromiso de los usuarios y las partes interesadas, el uso de agentes de seguridad para el acceso a la nube o Cloud Access Security Broker (CASB por sus siglas en inglés)[13], para ganar visibilidad y control, además de otras soluciones de seguridad. En este punto se debería considerar lo siguiente:

1. Gobierno y Gestión de Riesgos.
2. Inventario de activos de información y conocimiento de su flujo de trabajo.
3. Seguridad sobre los datos y gestión sobre el ciclo de vida de la información.
4. Cifrado de datos y gestión de claves de cifrado.

Abuso e Inadecuado Uso de los Servicios en la Nube: Es común que se haga uso de los beneficios otorgados por la nube para la perpetración de ataques dirigidos y estructurados como lo son los llamados ataques de Denegación de Servicio Distribuido (DDoS por sus siglas en ingles)[14], phishing, distribución de malware[15], entre otros. La gran variedad de ataques que pueden generarse y el uso de información legitima para realizarlos, por ejemplo, utilizar un dominio conocido, real y de confianza, hacer uso de alojamiento en la nube y las funcionalidades que la nube ofrece

[13] Cloud Access Security Broker (CASB): Según Gartner, son los puntos que refuerzan las políticas de seguridad, bien sea una solución on-premise o basada en la nube, que se sitúan entre los consumidores de servicios de nube y los proveedores de servicios de nube a fin de combinar e interponer políticas de seguridad corporativas a medida que se acceda a los recursos en la nube. [44]

[14] DDoS: Los ataques de red distribuidos a menudo se conocen como ataques de denegación distribuida de servicio (DDoS). Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa. El ataque DDoS envía varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes y de evitar que este funcione correctamente. [37]

[15] Definición de Malware: Es la abreviatura de “Malicious software”, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc. [52]

entre otros, hacen del cloud computing una tecnología efectiva y eficaz para generar ataques cibernéticos.

Mediante técnicas de seguridad, siguiendo estándares de seguridad y haciendo uso correcto de los recursos con los que se cuenta como base para el uso seguro de servicios en la nube, se deben implementar controles que satisfagan la necesidad de evitar ataques de ciberseguridad. Las mitigaciones no son solo de los clientes sino también de los proveedores. Los proveedores de servicios en la nube deben contar con una infraestructura sólidamente protegida, un proceso de gestión de incidentes, controles para que las partes puedan conocer en cada momento el estado de los servicios implementados, rendimiento, almacenamiento de datos y telecomunicaciones, entre otros. Para esta amenaza se debe tener en cuenta lo siguiente:

1. Inventario de los activos de información.
2. Gestión de riesgos de seguridad de la información.
3. Gestión de vulnerabilidades y amenazas.
4. Cifrado de datos y gestión de claves de cifrado.
5. Procedimientos de identificación, acceso, autorización y gestión del ciclo de vida de las credenciales.
6. Seguridad en dispositivos móviles y personales con los que se acceden y consumen los servicios
7. Procedimientos de control y gestión de cambios.
8. Gestión de logs y detección temprana de comportamientos no habituales en todos los niveles. Auditoría de eventos.
9. Plan de continuidad del negocio.

Anexo C

En este anexo se desarrollarán las áreas de enfoque crítico de la del CSA [2], citadas en el documento principal. La conforman 13 dominios que tratan las áreas de enfoque divididos en dos grandes grupos, el grupo de gobierno que contiene cuatro tópicos y el operacional que cuenta con nueve ítems. Estos buscan cubrir los dominios de seguridad en la nube que deben ser considerados. A continuación, se describen y dichas áreas usadas en el documento principal.

Gobierno:

Gobernanza y gestión de riesgos empresariales: Si bien como ya se ha mencionado la nube propone un esquema de responsabilidad compartida, esto no indica que la responsabilidad de gobierno se tercerice. La gobernanza sobre todos los parámetros que se deseen trabajar en la nube debe ser claramente definida en el contrato y en los acuerdos de servicio según las necesidades y objetivos de la organización, ya que es la única forma de resguardarse legalmente frente al incumplimiento por parte del proveedor.

Además del contrato, se cuenta con otras herramientas para asegurar el gobierno en la nube como lo son los informes de cumplimiento legal, evaluaciones a los proveedores cloud y auditorías.

Otro punto clave es la gestión del riesgo empresarial. Debido a que la nube se basa en un sistema de responsabilidad compartida en donde los riesgos deben ser claramente identificados y asignados para su gestión a alguna de las partes, según su responsabilidad. Sin embargo, lo anterior no elimina la responsabilidad sobre sus riesgos.

En el contrato se debe tratar la gestión del riesgo empresarial donde se especifique la segregación de roles, responsabilidades compartidas y se identifique los posibles riesgos que están asociados a los activos de información y cuál es su tolerancia a la materialización de estos riesgos. Esto no quiere decir que en este documento se deba tratar temas de orden

técnico, pero sí es importante conocer y evaluar toda la información para que se pueda realizar las aclaraciones pertinentes y se tenga un contexto claro de los alcances y límites de cada una de las partes.

La gestión de riesgo, depende del modelo de servicio y despliegue que se quiera adquirir. Por lo cual, se deberá tener en cuenta desde los acuerdos de servicio hasta la definición de la gestión de riesgos e implementación de controles aplicables según la necesidad de la organización.

Se debe tener en cuenta la gran importancia que tiene una gestión proactiva para garantizar el cumplimiento del contrato y las clausulas a llevar a cabo. Será necesario llevar a cabo un convenio de trabajo bajo los estándares de buenas prácticas y reglamentos que aplique.

Por último, se debe evaluar detalladamente cómo un contrato con un proveedor de servicios cloud interactúa con el modelo de gobierno de la organización cliente y así realizar las modificaciones que sean necesarias.

Asuntos legales, Contratos y descubrimiento electrónico: Con la manipulación de los datos en infraestructuras cloud se deben tener en cuenta los requisitos legales, términos que sean aplicables y el llamado descubrimiento electrónico a partir de cualquier requerimiento judicial. En este dominio aborda los posibles problemas concernientes a las leyes y regulaciones aplicables a los datos.

Dado la relación de obligación entre los clientes de la nube y sus propios clientes se debe entender cómo aplica y afecta el tratamiento de los datos propios o de sus clientes alojados en la nube según el país de jurisdicción del contrato, ubicación de los servicios de procesamiento de datos, normativa, legislación y tratados aplicables, así como los estándares de gestión de datos.

Estos guardan una alta dependencia entre la ubicación del cliente, del proveedor cloud, ubicación de los repositorios de datos, ubicación del dueño

de los datos y la legislación, normativa, tratados y leyes aplicables entre las diferentes ubicaciones.

Por lo anterior, los clientes deben realizar un estudio detallado de los aspectos legales, términos y condiciones, políticas y demás que influya en el tratamiento de los datos desde el punto de vista funcional, obligaciones de ley y contractual. Mediante el análisis de la documentación provista por los proveedores de servicio según el servicio a contratar. Posterior a esto se deberá evaluar el funcionamiento de dichos requisitos a sus propios requerimientos jurisdiccionales y contractuales.

En gestión de un correcto contrato de servicios, se deberá tener en cuenta la ubicación de los datos para el cumplimiento normativo y legal aplicable. También, tendrá que ser regularmente evaluado para la verificación del cumplimiento del mismo y los compromisos legales que den lugar, entendiendo que los requerimientos legales están en constante cambio.

El conocimiento de la ley aplicable sobre el descubrimiento electrónico, es parte del ejercicio de elección de dónde se alojarán los datos y la capacidad para cumplir con estos requerimientos, dado el caso de parte del cliente como del proveedor.

Gestión de cumplimiento y auditoría: Las auditorias funcionan como mecanismo de validación y verificación del cumplimiento de las políticas y normas de cualquier organización como de los requerimientos legales, estándares de buenas prácticas, normativa y demás aplicables. En el área de la seguridad de la información es una herramienta vital para la gestión de riesgos, gobierno y la validación del cumplimiento legal aplicable.

Cabe indicar que el cumplimiento legal es un proceso a satisfacer de forma conjunta entre el proveedor y el cliente, donde según el servicio contratado se separan las auditorías a realizar. Sin embargo, para los entornos cloud es notorio que la auditoria tradicional debe ser modificada según este nuevo ambiente. Debe ser un proceso continuo en el tiempo,

apoyado por los estándares de buenas prácticas en esta materia, los cuales buscan adaptarse a la nube.

Las auditorias por parte del proveedor son usualmente generales para todos sus clientes buscando satisfacer una regulación o estándar. Por lo cual muchas veces no tienen en cuenta los requerimientos específicos de cada cliente. Es aquí importante que el proveedor de servicio comunique claramente el alcance y limitaciones de las auditorias, como se debería llevar a cabo implementaciones alineadas con el cumplimiento de los requisitos legales y regulaciones que tengan lugar.

Así mismo, presentar evidencia y los mecanismos e información necesarios para el cumplimiento del marco regulatorio y legal aplicable al cliente.

Por otro lado, las auditorías por parte del cliente son únicamente enfocadas en lo que él controla y gestiona según los servicios contratados, generando una visión limitada del proceso a evaluar. Es aquí donde el cliente debe asegurase de tener toda la información, comprender los alcances y limitaciones de las auditorías del proveedor para evitar el incumplimiento de los requisitos legales.

Adicionalmente a esto, es importante evaluar los controles impuestos por el proveedor en el ámbito del alcance de los servicios contratados para garantizar el correcto funcionamiento de estos. Así mismo, llevar un control de los proveedores de la infraestructura cloud y validar que estos también cumplan con lo requerido en un marco de cumplimento legal.

Gobierno de la información: Se le llama gobierno de la información a la validación y verificación sobre la gestión adecuada de los datos según los lineamientos y directrices de cada organización. Esto se realiza mediante actividades, procedimientos y procesos que certifican el cumplimiento de los requerimientos internos como externos aplicables.

Para la gestión en la nube, es necesario tener en cuenta qué datos estarán en la nube y cómo serán tratados en ese ambiente. Para esto, es

indispensable contar con un inventario de datos, conocer su ciclo de vida y las políticas de gobierno de datos que enmarcaran su tratamiento. Así mismo, conocer la ubicación de los datos una vez almacenados en la nube y el marco legal al cual se acoge la información.

Dado los cambios de migración al mundo cloud, los clientes podrían necesitar reevaluar y modificar sus procedimientos de seguridad, normativas internas y políticas en aras del correcto gobierno de los datos en la nube. A nivel de actividades y procedimientos, la definición de propiedad, custodia, grado de privacidad entre otros, determinarán los niveles de autorización, salvaguardas aplicables, tanto de orden técnico como contractual.

El CSA [2] no recomienda hacer un traspaso de información sin hacer una evaluación consciente de la arquitectura de información y la corrección de los errores encontrados y conocidos. Esto para no trasladar errores ya conocidos a ambientes de responsabilidad compartida.

Plano de Gestión y Continuidad del Negocio: Con la centralización de la administración de los entornos tecnológicos que brinda los servicios cloud, las API´s son las herramientas que permiten el control y gestión de todo el ambiente. Esto lleva a un cambio de paradigma de cómo gestionar la seguridad teniendo ventajas como el conocimiento de todos los activos tecnológicos, su estado y asignación.

En el plano de gestión, además de la consolidación de poder administrar todos los recursos y servicios mediante una única aplicación y grupo de interfaces web o consolas de comandos, también es desde donde se realiza toda la segregación y aislamiento de los elementos que integran la nube. Es aquí donde es imprescindible tener control sobre las API´s y cualquier tipo de consola de gestión de servicios para evitar cualquier fallo de seguridad y hacer una correcta separación de los ambientes y restringir detalladamente la comunicación entre estos.

En relación a la gestión de la seguridad se debe realizar el control del perímetro, implementar procesos robustos de autenticación de los usuarios,

crear un proceso confiable y dinámico de alta baja y modificación de cualquier tipo de usuario, control y auditoría de los permisos de autorización, monitoreo de cualquier evento de seguridad y una correcta gestión de alertas.

Es muy importante poner énfasis en que el proveedor cloud es responsable por la disponibilidad de los recursos, brindar funciones y funcionalidades que permitan garantizar la seguridad, el control de acceso y autorización, también herramientas para la gestión y monitoreo de los elementos en la nube.

Sin embargo, la configuración correcta de los servicios es una dependencia netamente del cliente. Por ejemplo, mantener control y seguridad de las credenciales de acceso a los recursos en la nube es uno, entre otros, de los muchos temas de los cuales el cliente debe hacerse responsable y gestionar adecuadamente.

En el plano de continuidad de negocio, si bien es una responsabilidad compartida entre el cliente y el CSP, en última instancia, el cliente debe ser consciente que la responsabilidad sobre las cuentas es suya. Por lo cual es importante evaluar aspectos como la recuperación y continuidad ante desastres en el proveedor en la nube, la portabilidad de los servicios para restauración en otro proveedor en la nube y la preparación y administración para llevar a cabo este tipo de tareas dado un desastre.

Para lo anterior es importante crear una arquitectura que considere posibles fallos que afecten a la continuidad del negocio, tener en mente soluciones implementadas en alta disponibilidad que incluyan en lo posible varios proveedores en la nube, garantizar la portabilidad entre proveedores de los recursos. Del mismo modo, considerar usar las diversas funcionalidades y funciones destinadas para esto por parte de cada proveedor.

Mantener una correcta gestión del riesgo y un enfoque orientado a estar preparado para evento de disrupción del servicio o desastre. Esto asegura siembre tener una postura preventiva y llevar a cabo las pruebas

correspondientes para garantizar que un plan de continuidad o un plan de recuperación ante desastres funcione según lo esperado

Operación:

Seguridad de Infraestructura: En este dominio se busca asegurar la infraestructura física (recursos físicos, lógicos y de comunicación) y redes e infraestructura virtual soportada. La seguridad sobre la orquestación y disposición de los recursos para los diferentes modelos de servicio es una labor del proveedor. Por otro lado, el cliente tiene la responsabilidad de velar por la seguridad de sus servicios, plataformas e infraestructura virtual según sea el servicio contratado.

En la seguridad de la infraestructura virtual es esencial la correcta separación y control del perímetro de comunicación mediante la segmentación detallada de todos los ambientes. De la misma forma, el perímetro debe tener controles orientados a la detección y prevención de cualquier intrusión sin que estos se conviertan en puntos de falla. Por lo cual, deben cumplir con las características asociadas a la nube como el auto-escalado, alta disponibilidad, tolerancia a fallas, ajustable al cambio y demás.

Los dispositivos de seguridad además de tener que ajustarse a la dinámica de la nube, también tienen que ser resilientes al cambio. Esto quiere decir que se debe entender cómo funciona la nube para que estos dispositivos cumplan con los requerimientos de trabajo y gestión asociados a la nube. Por ejemplo, en los entornos privados de cada compañía se suele configurar las telecomunicaciones basado en el concepto de IP[16] estática para la identificación de un dispositivo en la red corporativa. En cambio, en la nube se adopta el cambio de paradigma de trabajo por IP´s dinámicas y cambio constante y rápido de IP, compatibilidad de trabajo con la gestión de redes definidas por software.

[16] Definición de IP: La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (Internet Protocol) o, que corresponde al nivel de red del modelo TCP/IP. [61]

Hacer uso de las herramientas, funcionalidades y funciones para la seguridad de la infraestructura como firewalls y aislamiento de redes, brinda granularidad y micro-segmentación, confidencialidad de los datos en tránsito, definición de políticas a medida entre otros.

Otro punto esencial en la seguridad de la infraestructura es la carga de trabajo, es decir, las unidades de procesamiento y la memoria que estos usan. Las máquinas virtuales, contenedores, plataformas de desarrollo y ejecución como la ejecución de funciones, hoy en día llamada función como servicio (FaaS[17], por sus siglas en inglés) o ejecución de código sin servidor. Estas cargas de trabajo sin un correcto control pueden generar sobrecarga y alto consumo de recursos generando falta de disponibilidad no solo para este elemento en procesamiento sino para los demás que dependan de la misma pila de procesamiento y hardware.

Los dispositivos de seguridad para estas cargas de trabajo deben ajustarse a los nuevos elementos de la nube y sus modos de operación deben cambiar y no convertirse en posibles puntos de falla. Un correcto y rápido proceso de monitoreo y sistema de alarma dinámico, con análisis de comportamiento y enfocado en los cambios no esperados.

La correcta ejecución de procesos y procedimientos para garantizar que las cargas de trabajo y elementos de red virtuales se encuentren actualizados, análisis de eventos que suceden en el entorno entre otros deben estar definidos y optimizados, preferiblemente de ejecución automática. Así mismo, crear planes y programas de auditoria que garanticen la seguridad de este ambiente y evaluar que el proveedor cuente con los elementos de seguridad y procedimientos que salvaguarden el entorno corporativo en la nube.

A nivel de evaluación de vulnerabilidades, la disposición para esto debe ser consensuada con el proveedor y se encontrará limitada y ceñida al

[17] Definición de FaaS: Una arquitectura sin servidor es una manera de crear y ejecutar aplicaciones y servicios sin tener que administrar infraestructura. Su aplicación continúa ejecutándose en servidores, pero el proveedor de servicio se encarga de toda la administración de los servidores. Ya no tiene que aprovisionar, escalar ni mantener servidores para ejecutar sus aplicaciones, bases de datos y sistemas de almacenamiento. [20]

contrato de servicios. Usualmente esta actividad se encuentra denegada por defecto. Es aquí donde se debe conocer en detalle los controles, salvaguardas y mecanismos de seguridad de la nube contratada según el modelo de servicio adquirido.

Virtualización y contenedores[18]: Como ya se informó anteriormente, un proceso esencial de la nube es la virtualización, permite la agrupación y abstracción de los recursos para su uso según las necesidades. Por tal motivo se debe garantizar la seguridad de toda la infraestructura que permite la virtualización como de los elementos virtuales creados.

De nuevo es un proceso de responsabilidad compartida entre el proveedor quien debe encargarse de asegurar la tecnología usada para la virtualización como el hipervisor, la infraestructura física y demás, y la separación de todos los elementos y recursos entre las diferentes cuentas de los clientes, procedimientos alineados con las mejores prácticas que garanticen la seguridad del entorno virtual, red, almacenamiento y físico. Parte de esta responsabilidad es brindar los mecanismos necesarios para que sus clientes puedan configurar capas de seguridad adicionales a los elementos virtuales y contenedores.

De parte del cliente es esencial la gestión de los activos de información, captura de eventos, monitoreo, gestión de autorización y acceso y demás.

En este control se empieza a trabajar y entender el concepto de almacenamiento virtual, tema que el cliente debe velar por la integridad, disponibilidad y confidencialidad de los datos en el entorno virtual. Una práctica altamente recomendada es el cifrado de los datos en reposo como en tránsito y separación de esta actividad de los procesos de administración de datos para evitar falta de control de acceso. A nivel de red se deben

[18] Contenedores: Los contenedores constituyen un mecanismo de empaquetado lógico en el que las aplicaciones pueden extraerse del entorno en que realmente se ejecutan. Esta desvinculación facilita el despliegue uniforme de las aplicaciones basadas en ellos con independencia de que el entorno sea un centro de datos privado, la nube pública o el portátil personal de un desarrollador. [34]

implementar los controles correspondientes para mitigar incidencias de seguridad dentro y afuera de la nube, aislamiento a nivel de red, análisis y control de tráfico, políticas de acceso y demás aplicables.

Los contenedores son entornos que permiten la ejecución de código y cuenta con un controlador/planificador, repositorio de imagen de contenedores y un sistema de orquestación para su funcionamiento. Esta tecnología requiere que se trabaje en diferentes niveles la seguridad. Desde la infraestructura física hasta el código que se ejecuta en cada contenedor. El correcto aislamiento, control de acceso, parámetros de configuración segura del contenedor, almacenamiento y de red. Se debe entender cómo funciona y sus componentes permiten implementar los controles adecuados y a la medida. Garantizar el despliegue de contenedores previamente probados y seguros.

Respuesta a incidentes, notificación y remediación: La respuesta ante incidentes en entornos cloud cambia en sus fases, preparación, detección y análisis, contención, erradicación y recuperación, y por último las actividades posteriores al incidente. La nube al estar en gran medida compuesta por procesos automatizados, cambia la forma de reacción ante un incidente de seguridad. Muchos de estos procesos son los que logran mantener en alto grado de cumplimiento los acuerdos de servicio.

Sin embargo, no todos los procesos son cubiertos de esta manera y según el modelo de servicio, la responsabilidad y actividades a realizar por parte del proveedor como del cliente cambian. Es muy importante declarar en detalle el rol, la responsabilidad, tipo de respuesta ante un incidente y los acuerdos de servicio para cada fase de la respuesta a incidentes en el contrato. Adicionalmente a esto, es importante tener conocimiento y que se encuentre definido el protocolo de comunicación de incidentes.

Entre estas definiciones también debería encontrarse las definiciones necesarias para los simulacros de recuperación ante desastres y el plan de continuidad, donde se acuerde y coordine los procedimientos entre las partes y se evalúe con cierta periodicidad los cambios en el entorno tanto del

proveedor como del cliente. De la misma manera, se debe generar los mismos acuerdos con cualquier proveedor adyacente que sea contratado para hacer uso del servicio en la nube.

De parte del cliente, es importante implementar arquitecturas de sus servicios en la nube haciendo uso de todas las bondades de la nube como el auto-escalamiento, tolerancia a fallas, alta disponibilidad, automatización y demás para, dado un incidente, la respuesta sea tan rápida como sea posible en todo sentido.

De la misma forma, un proceso adecuado de monitoreo y alarma sobre toda la infraestructura cloud brindará visibilidad y rápida respuesta ante la detección de un incidente. Hacer uso de los registros de auditoria, análisis de comportamiento y correlación de datos darán una visión global de lo que sucede en el entorno. Hacer uso de los datos de monitoreo del proveedor y garantizar que se cuente con la información suficiente para cumplir cualquier requerimiento corporativo y legal. Por otro lado, la información recolectada debe ser correctamente almacenada para poder reconstruir incidentes generados y en los casos que se solicite como prueba legal.

Seguridad de aplicaciones: La nube proporciona un grado de abstracción mayor que brinda una serie de ventajas que hacen a la seguridad de las aplicaciones en todos los niveles y trabajan de la mano con el ciclo de desarrollo de software de una manera segura. Desde el aislamiento a nivel de comunicación y recursos hasta ejecuciones totalmente aisladas y controladas de porciones de código.

La nube ayuda a implementar arquitecturas seguras y hacer desarrollos y despliegues seguros de las aplicaciones. La corresponsabilidad entre el proveedor y el cliente para esta labor está en todo el ciclo del desarrollo. La nube impone siempre un proceso de desarrollo seguro y una implementación de aplicaciones con las características que definen a la nube, es decir, implementación segmentada, uso de contenedores y micro-servicios, aislamiento, automatización y demás.

Es claro que, bajo este panorama, la seguridad debe ser tomada en cuenta desde el primer paso del desarrollo de aplicaciones. Se debe conocer en profundidad las funciones y funcionalidades que brindan los proveedores en la nube para la seguridad de las aplicaciones y así sean tomadas en cuenta para los nuevos desarrollos como para los existentes.

Buenas prácticas en el desarrollo, cabeceras seguras, validación de datos entrantes, configuración de cookies, gestión de depuración de fallas, etc., deben ser aplicadas. Se debe tener en cuenta la construcción de cadenas de conexión de manera segura y control de accesos a nivel en base al principio de mínimo privilegio. Es preferible trabajar por eventos, desactivar la información de errores detallada, hacer uso de mensajes breves.

A nivel de implementación, el proceso de pruebas de la aplicación y análisis de vulnerabilidades debe estar contemplado desde el principio. El cambio de ambiente para el desarrollo hace que la definición de los controles de seguridad esté inmersa en las aplicaciones y la automatización de estos controles.

Seguridad y cifrado de datos: La gestión de los datos en entornos cloud es quizás la mayor preocupación que los consumidores tienen. Dado el valor que tienen estos activos de información, son parte vital de cualquier entidad. Por esto, un punto clave a la hora de migrar a la nube es el gobierno sobre estos. Sin embargo, se debe entender que las medidas a tomar sobre los datos deben estar basadas en un análisis de riesgo consciente que indique cómo deberán ser tratados.

Teniendo en cuenta lo anterior, toda entidad busca tener control de la información migrada a la nube, la protección de estos y garantizar que, en todo el ciclo de vida de la información indicado en el capítulo anterior, cuente con las medidas de seguridad acordes.

Otro tema de igual importancia es el cumplimiento de requisitos legales según la naturaleza del cliente y normativa aplicable. Un inventario detallado de activos de información apoyado con políticas solidas que determinen en donde se podrá hacer uso de estos activos es vital en este

punto. Por lo cual, antes de poder trabajar con los datos en la nube, se deben modificar las políticas y satisfacer los requerimientos impuestos con la colaboración del proveedor según el modelo de servicio y despliegue cloud.

Es importante conocer el comportamiento habitual de los datos y su dinámica, para así poder generar un sistema de alarma ajustado a la realidad del consumidor y evitar posibles fugas de datos una vez migrada la información. La implementación de sistemas de análisis de eventos y generación de alarmas para esta labor debe ser lo más cercana a la realidad de dicho consumidor.

A nivel de control de acceso a la información es indispensable conocer quien accede a los datos y basado en el principio de mínimo privilegio hacer la asignación de premisos. Llevar a cabo la identificación y aplicación de controles para la información a nivel de aplicación, gestión y de trabajo conjunto a nivel interno y externo.

Los datos en tránsito y reposo deben ser cifrados independientemente de su origen o destino, hacer uso de protocolos y métodos de cifrado seguro. También asegurar una correcta gestión del sistema de claves y tener pleno acuerdo y conocimiento con el proveedor en la nube si se opta por los servicios de cifrado de datos.

Como en el punto anterior, es importante implementar arquitecturas fuertes para la gestión de los datos, validando y verificando el correcto acceso y autorización a los datos. Diseño de consultas a los datos y cadenas de conexión seguras como sistemas de verificación brindan una capa adicional de seguridad. Se debe hacer control de las API´s y la información que usan para su ejecución.

Implementación de soluciones para la prevención de fugas de datos deben ser considerados en cualquier servicio. La generación de controles en todos los niveles en los cuales los datos se manipulen es una labor de corresponsabilidad con el proveedor, por lo cual apoyarse en las herramientas que brinda la nube para esto y entenderlas es sustancial. Cabe recordar que la organización cliente, quien contrata los servicios cloud, dado

un incidente de seguridad siempre será la única responsable en última instancia.

Identidad, derecho y administración de acceso: En este punto, quizás es donde más se manifieste el trabajo conjunto y la corresponsabilidad para la gestión de la Identidad y control de acceso partiendo de la delegación de responsabilidades y relación necesaria para su correcto funcionamiento. El cliente siempre debe ser quien administre las identidades y propiedades de estas, fundamentada de su propio gestor de identidades, ya sea en su centro de datos o inclusive si este se encuentra en su ambiente cloud.

La adopción de la nube hace imprescindible tener políticas para esta labor que se encuentren contextualizadas para el trabajo en la nube y la correcta técnica de federación de identidades en un contexto de gestión compartida, buscando asociar y consolidar la gestión de identidades. De la misma forma conocer los protocolos de gestión de identidades para un empalme correcto contra la nube acorde a las necesidades y restricciones del cliente. Esto para poder definir arquitectura, roles, responsabilidades y protocolos para la gestión de identidades internas y externas.

Para la identificación de credenciales es imperativo hacer uso de múltiple factor de autenticación robusta para la mitigación de suplantación, en especial con las cuentas administrador o de mayor privilegio, considerar el uso de tokens[19] o tecnologías similares para la identificación y conocimiento de estado en las comunicaciones establecidas.

Para la autorización es importante entender los alcances que se tienen por cuenta, las gestionadas por parte del proveedor como del cliente. Siempre orientado en una gestión de permisos granular para evitar acceso a recursos que no sean necesarios. Si se considera necesario, hacer uso de terceros que intermedien la gestión de identidades. Otra buena práctica es

[19] Token: Un token de seguridad (también llamado llave digital o llave electrónica) es un dispositivo físico utilizado para acceder a un recurso restringido electrónicamente. El token se utiliza como complemento o en lugar de una contraseña. Actúa como una llave electrónica para acceder a algo. Por ejemplo, una tarjeta de acceso inalámbrica que abre una puerta cerrada, o en el caso de un cliente que intenta acceder a su cuenta bancaria en línea, el uso de un token proporcionado por el banco puede probar que el cliente es quien dice ser. [62]

hacer uso de matrices de correlación para identificar que permisos deben ser generados según los atributos que deba ser para cada usuario dentro de la nube, sustento para la generación de políticas técnicas asociadas a la gestión de identidad, derecho y administración de acceso.

Seguridad como servicio (SecaaS): Se considera seguridad como servicio a los diversos productos de seguridad orientados a la nube gestionados como servicio que cuentan con las características como el talento humano, facilidad y maleabilidad en implementación y otras más. Así mismo las características que hacen a la nube. Por ejemplo, las nombradas en el capítulo primero de este documento. De la misma forma presenta posibles inconvenientes al hacer uso de estos servicios. Estos podrían ser, posible disconformidad de manejo de datos, fuga de datos, no cumplimiento de reglamentación y normativa legal entre otros.

La guía en este dominio busca centrarse en los servicios sobre la nube, es decir, plataforma como servicio (PaaS) y software como servicio (SaaS). En este sentido los servicios ofrecidos son de diferentes índoles y trabajan en diferentes niveles con los servicios en la nube. Desde sistemas de identificación y protección de intrusos, los llamados agentes de acceso a la nube (CASB por sus siglas en ingles) que se encargan de analizar, gestionar y manipular las comunicaciones del cliente contra la nube, firewall de aplicaciones, consolas de gestión de seguridad para servicios corporativos como el mail hasta gestores de identidad, escáneres de vulnerabilidades y validación de estándares de implementación de soluciones en la nube.

La oferta y proveedores de esta clase de productos y servicios son amplios. Sin embargo, no todos son funcionales para el cliente dada su realidad, requerimientos del negocio, normativos, legales o de los propios objetivos organizacionales. Por lo cual, antes de proceder a contratar este tipo de servicios se debe hacer una consolidación de requerimientos que dicho proveedor de seguridad como servicio debe cumplir.

El manejo de los datos tiene especial detenimiento, dichos activos de información de carácter confidencial, por conformar datos personales o del

negocio, se debe conocer en detalle el proceso de acceso, manipulación y almacenamiento.

Tecnologías relacionadas: Son aquellas tecnologías que con el nuevo paradigma de la nube han tomado una mayor fuerza y auge; Su implementación y resultados se han visto acrecentados gracias a las funcionalidades y características que la computación en la nube brinda. Según el Cloud Security Alliance pueden dividirse en dos grupos, tecnologías con alta dependencia de la nube para su operación y las que, si bien no tienen gran dependencia, son fácilmente relacionadas con la nube.

Quizás, la tecnología con mayor crecimiento con la ayuda de la nube es la ejecución de aplicaciones sin necesidad de servidores (Serverless por su traducción al inglés). Esto quiere decir que, mediante solo la ejecución de código y funciones, haciendo uso de las múltiples características y funcionalidades del servicio PaaS (Plataforma como Servicio) brindan servicios sin necesidad de tener en cuenta temas como los recursos tecnológicos, comunicación, plataformas de ejecución de demás asociadas para el funcionamiento de una aplicación.

Es evidente que la carga de seguridad en este tipo de tecnología es de mayor peso para el proveedor de función como servicio (FaaS), no indica en ningún caso como se ha informado a lo largo de este documento que el cliente no tenga la responsabilidad final.

Es por esto que es imprescindible garantizar que se cumplan los requerimientos jurisdiccionales y legales que haya a lugar, modificar los procedimientos, procesos, normativas y políticas para la adopción de esta nueva tecnología. En lo que se refiere a la parte técnica, hacer un correcto análisis del código que se ejecuta y un fuerte sistema de monitoreo, alarma y análisis de correlación de eventos de la aplicación.

El internet de las cosas (Internet of Things - IoT por sus siglas en ingles)[20] y la tecnología móvil, son una tecnología en crecimiento que no

[20] IoT: Hace referencia a los sistemas de dispositivos físicos que reciben y transfieren datos a través de redes inalámbricas sin la intervención humana. Lo que lo hace posible es la integración de dispositivos informáticos sencillos con sensores en todo tipo de objetos. [48]

sería posible sin la nube. La capacidad de alta disponibilidad y amplio acceso desde internet permiten poder generar los beneficios de este nuevo paradigma. Sin embargo, genera nuevos desafíos de seguridad, ya que literalmente cualquier cosa podría ser un vector de ataque. Hacer uso de las API´s de comunicación para vulnerar los servidores en la nube mediante diferentes formas de ataque.

Teniendo en cuenta lo anterior, seguir estándares de desarrollo seguro es de un alto impacto en esta tecnología a lo que seguridad se refiere. Inspeccionar y filtrar todas las conexiones, mantener cifrado las comunicaciones entre los dispositivos y la nube, automatizar la actualización de software, proceso de autenticación y autorización segura federado son parte de las medidas usualmente tomadas y que la guía de seguridad del CSA [2].

En lo que se refiere explícitamente a la tecnología móvil es un poco más complejo, ya que estos dispositivos funcionan de forma muy similar a una computadora, por lo cual amplía el rango de posibles ataques que pueden ser generados desde allí, y de la misma forma aplican salvaguardas específicas para cada tecnología en particular. El vector de ataque más común son las API´s, ya que muchos desarrollos de estas conexiones son vulnerables o mal programadas, permitiendo el envío de información confidencial sin cifrar o hacer uso de librerías o métodos discontinuados o débiles para su ejecución y comunicación.

Por ello, contar con un ciclo de vida de desarrollo seguro, gestión de pruebas específico para la seguridad, hacer uso de las buenas prácticas en todos los ámbitos, hacer uso de certificados, correcta implementación de la autenticación y autorización, cifrado de datos y canal de comunicación, etc., son parte de los controles necesarios al hacer uso de este tipo de tecnologías.

Otro tema vital, es el almacenamiento y federación de la información corporativa en estos dispositivos. Cada organización debe garantizar mantener control y gestión de los datos corporativos en estos dispositivos y tener medidas ante cualquier eventualidad como puede ser el robo de estos

dispositivos. En este punto, es crucial tener control de qué información se trasfiere y el cifrado de los datos en tránsito, reposo y en uso.

Entre estas se encuentra el Big Data[21], dado el alto poder de cómputo y capacidad de auto crecimiento que posee la nube, permite el procesamiento de grandes volúmenes de datos variados a una alta velocidad. Necesidades fundamentales para esta tecnología como la recopilación, almacenamiento y procesamiento de datos de forma distribuida son satisfechas con creces.

Estas necesidades no son solo de orden funcional, sino de seguridad. Usualmente este tipo de implementaciones deben cumplir estándares de buenas prácticas para su correcto uso y privacidad de los datos, además de la normativa legal asociada que el cliente de la nube debe garantizar su cumplimiento. Por lo cual hacer uso de todas las herramientas de seguridad disponibles como el cifrado de datos en todas sus instancias, autenticación y autorización integrada y única, monitoreo y gestión de alarmas, entre otros, es indispensable para salvaguardar este tipo de implementaciones y sus aplicaciones subyacentes que cooperan o consumen los servicios generados por el Big Data.

[21] Big Data: El big data está formado por conjuntos de datos de mayor tamaño y más complejos, especialmente procedentes de nuevas fuentes de datos. Estos conjuntos de datos son tan voluminosos que el software de procesamiento de datos convencional sencillamente no puede administrarlos. Sin embargo, estos volúmenes masivos de datos pueden utilizarse para abordar problemas empresariales que antes no hubiera sido posible solucionar. [46]

9- Bibliografía Específica

[1]. CSA, Top Threats to Cloud Computing The Egregious 11, https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/, recuperado el 15 de 04 de 2020

[2]. CSA, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, https://cloudsecurityalliance.org/download/security-guidance-v4/, recuperado el 15 de 04 de 2020.

[3]. ICONTEC, Compendio, sistema de gestión de seguridad de la información (SGSI). Bogota, Cundinamarca, Colombia, 2009.

[4]. ISO and IEC, ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary, https://www.iso.org/standard/60544.html, recuperado el 26 de 03 de 2020.

[5]. ISO and IEC, ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, https://www.iso.org/standard/43757.html, recuperado el 26 de 04 de 2020.

[6]. ISO, ISO Guide 73:2009 Risk management – Vocabulary, https://www.iso.org/standard/44651.html, recuperado el 12 de 04 de 2020.

[7]. ISO and IEC, ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary, https://www.iso.org/standard/73906.html, recuperado el 05 de 05 de 2020.

[8]. ISO and IEC, ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements, https://www.iso.org/standard/54534.html, recuperado el 15 de 03 de 2020.

[9]. ISO and IEC, ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls, https://www.iso.org/standard/54533.html, recuperado el 19 de 03 de 2020.

[10]. ISO and IEC, ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management, https://www.iso.org/standard/75281.html, recuperado el 14 de 04 de 2020.

[11]. ISO and IEC, ISO/IEC 31000:2018 Risk management – Guidelines, https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en, recuperado el 12 de 04 de 2020.

[12]. ITU, I. T., Global Cybersecurity Index, www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx, Recuperado el 16 de Agosto de 2019.

[13]. MINTIC, Seguridad y Privacidad de la Información, Seguridad en la Nube, https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf, Recuperado el 20 de 04 de 2020.

[14]. NIST, SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, https://csrc.nist.gov/publications/detail/sp/800-39/final, recuperado el 14 de Marzo de 2020.

[15]. NIST, SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, recuperado el 11 de Marzo de 2020.

[16]. NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, recuperado el 06 de 05 de 2020.

[17]. NIST, SP 800-145, The NIST Definition of Cloud Computing, https://csrc.nist.gov/publications/detail/sp/800-145/final, recuperado el 03 de 04 de 2020.

[18]. NIST, Guidelines on Security and Privacy in Public Cloud Computing - Special Pulication SP 800-144, https://csrc.nist.gov/publications/detail/sp/800-144/final, recuperado el 12 de 04 de 2020.

[19]. Agustín López Neira, J. R. (2012). iso27000.es El portal de ISO 27001 en Español, http://www.iso27000.es/glosario.html, recuperado el 16 de 05 de 2020

[20]. Amazon Web Services, Serverless, Cree y ejecute aplicaciones sin preocuparse por los servidores, https://aws.amazon.com/es/serverless/, recuperado el 02 de 07 de 2020.

[21]. Barry Briggs, E. K., Enterprise Cloud Strategy - 2nd Edition, Microsoft Press - A division of Microsoft Corporation. Redmond, Washington, 2017.

[22]. Bond, J., The Enterprise Cloud - Best Practices for Transforming Legacy IT, O'Reilly Media, Inc, Las Vegas, Nevada, 2015.

[23]. Castro, A. Cloud Computing: Modelos de servicio, https://blog.bi-geek.com/cloud-computing-modelos-de-servicio/, recuperado el 05 de 04 de 2020.

[24]. CIS, CIS Controls Cloud Companion Guide Version 7, https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/, recuperado el 10 de 10 de 2020.

[25]. CSA, Cloud Controls Matrix v3.0.1, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/, recuperado el 03 de 06 de 2020.

[26]. MINTIC, Computación en la nube, https://mintic.gov.co/portal/inicio/Normatividad/Documentos-guias/75238:Computacion-en-la-nube, recuperado el 02 de 04 de 2020

[27]. Dennis Fisher, K., ¿Qué es un botnet?, https://www.kaspersky.es/blog/que-es-un-botnet/755/, recuperado el 24 de 06 de 2020.

[28]. EcuRed, Kernel, https://www.ecured.cu/Kernel, recuperado el 15 de 03 de 2020.

[29]. ESET Technology, ¿Qué es un 0-day? Explicando términos de seguridad, https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/, recuperado el 22 de 05 de 2020.

[30]. Fang Liu y NIST, Cloud Computing Reference Architecture - Special Pulication SP 500-292, https://www.nist.gov/publications/nist-cloud-computing-reference-architecture, Recuperado el 15 de 04 de 2020.

[31]. Filkins, B. and SANS, Security by Design: A Systems Road Map Approach. https://www.sans.org/reading-room/whitepapers/analyst/membership/39370, recuperado el 29 de 05 de 2020

[32]. Forum, T. O., Jericho Forum Cloud Cube Model - The Open Group Jericho Forum, https://publications.opengroup.org/w126?_ga=2.189252328.2744524997.1603249089-1708922885.1603249089, recuperado el 01 de 06 de 2020.

[33]. Gomez, J., . La Seguridad y la Confidencialidad de la Información es Obligación de Todos, https://www.merca20.com/la-seguridad-y-confidencialidad-de-la-informacion-es-obligacion-de-todos/, recuperado el 12 de Abril de 2020.

[34]. Google. Contenedores en Google, https://cloud.google.com/containers?hl=es, recuperado el 18 de 09 de 2020.

[35]. IBM, Inicio de sesión único de navegador web SAML 2.0., https://www.ibm.com/support/knowledgecenter/es/SSAW57_liberty/co

m.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_saml_web_sso.html, recuperado el 04 de 04 de 2020.

[36]. IBM Cloud Education, Multi-Tenant IBM, https://www.ibm.com/cloud/learn/multi-tenant, recuperado el 09 de 03 de 2020.

[37]. Karspersky Latam, ¿Qué son los ataques DDoS?, https://latam.kaspersky.com/resource-center/threats/ddos-attacks, recuperado el 29 de 05 de 2020.

[38]. Karspersky Latam, Qué es el spam y las estafas de phishing: definición, https://latam.kaspersky.com/resource-center/threats/spam-phishing, recuperado el 16 de 04 de 2020.

[39]. Microsoft, Azure - Servcio como un servcio, https://azure.microsoft.com/es-es/overview/what-is-saas/, Recuperado el 18 de 03 de 2020

[40]. Microsoft, Azure información general - ¿Qué es middleware?, https://azure.microsoft.com/es-es/overview/what-is-middleware/, recuperado el 30 de 03 de 2020.

[41]. Microsoft, Prevent Cross-Site Scripting (XSS) in ASP.NET Core, https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting?, recuperado el 01 de 04 de 2020.

[42]. NIST, Security and Privacy Controls for Federal Information Systems and Organizations - Special Pulication SP 800-53, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, recuperado el 08 de 06 de 2020.

[43]. Neoattack. Neowiki - ¿Qué es una API?, https://neoattack.com/neowiki/api/, recuperado el 10 de 03 de 2020.

[44]. NetSkope, ¿Qué es un Cloud Access Security Broker (CASB)?, https://www.netskope.com/es/about-casb, recuperado el 10 de 07 de 2020.

[45]. OECD, , Digital Security Risk Management for Economic and Social Prosperity Publishing. Paris, Francia, 2015.

[46]. Oracle, ¿Qué es big data?, https://www.oracle.com/ar/big-data/what-is-big-data.html, recuperado el 13 de 08 de 2020.

[47]. PowerData, Metadatos, definición y características, https://www.powerdata.es/metadatos, recuperado el 05 de 05 de 2020.

[48]. Red Hat, ¿Qué es el Internet de las cosas?, https://www.redhat.com/es/topics/internet-of-things/what-is-iot, recuperado el 10 de 09 de 2020.

[49]. Red Hat, Virtualización - ¿Qué es un hipervisor?, https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor, recuperado el 19 de 03 de 2020.

[50]. Rich, S., Data Security Lifecycle 2.0., https://securosis.com/blog/data-security-lifecycle-2.0, recuperado el 26 de 04 de 2020.

[51]. Rick Anderson, M. C., Prevent Cross-Site Scripting (XSS) in ASP.NET Core, https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting?view=aspnetcore-5.0, recuperado el 23 de 04 de 2020.

[52]. Rivero, M., ¿Qué son los Malwares? – InfoSpyware, https://www.infospyware.com/articulos/que-son-los-malwares/, recuperado el 31 de 03 de 2020.

[53]. Robert Cope, T. E., Cloud Computing Design Patterns, Prentice Hall Press. New Jersey, EE.UU., 2017.

[54]. Instituto Nacional de Ciberseguridad de España - Incibe, Cloud Computing – Una guía de aproximación para el empresario, https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf, recuperado el 03 de 04 de 2020.

[55]. Segu-Info, Noticias sobre la Seguridad de la Información - Phishing, https://segu-info.com.ar/malware/phishing, recuperado el 01 de 06 de 2020.

[56]. Segu-Info, Noticias sobre la Seguridad de la Información – Botnet, https://www.segu-info.com.ar/malware/botnet, recuperado el 16 de 04 de 2020.

[57]. NIST, Cloud Computing Standards Roadmap - Special Publication 500-291 V2., https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, recuperado el 30 de 05 de 2020.

[58]. NIST, Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, recuperado el 23 de 05 de 2020.

[59]. ENISA, Beneficios, riesgos y recomendaciones para la seguridad de la información, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file, recuperado el 20 de 04 de 2020.

[60]. Wayne Jansen, T. G. and NIST, Guidelines on Security and Privacy in Public Cloud Computing - Special Publication 800-144, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, recuperado el 10 de 04 de 2020.

[61]. Wikipedia, Dirección IP, https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP, recuperado el 03 de 06 de 2020.

[62]. Wikipedia, Token de seguridad, https://es.wikipedia.org/wiki/Token_de_seguridad#, recuperado el 10 de 09 de 2020.

[63] NIST, Marco para la Mejora de la Ciberseguridad en las Infraestructuras Críticas del NIST, 2014.

[64] Laotshi, Patrones de arquitectura de software vs Patrones de diseño, https://medium.com/@laotshi/patrones-de-arquitectura-de-software-vs-patrones-de-dise%C3%B1o-de-software-28ebd350ecbe, recuperado el 25 de 09 de 2020.

[65] Red Hat, ¿QUÉ ES DEVSECOPS? - DevSecOps y la seguridad de DevOps, https://www.redhat.com/es/topics/devops/what-is-devsecops#:~:text=DevSecOps%20significa%20integrar%20la%20seguridad,tambi%C3%A9n%20un%20enfoque%20organizativo%20distinto, recuperado el 11 de 05 de 2020.

[66] CISCO, TCP/IP Overview, https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html, recuperado el 25 de 08 de 2020.