FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

PROPUESTA METODOLÓGICA DE EVALUACIÓN PARA SEGURIDAD DE APLICACIONES EN EL CLOUD

AUTOR

Alexander David Caiza Caizaluisa

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROPUESTA METODOLÓGICA DE EVALUACIÓN PARA SEGURIDAD DE APLICACIONES EN EL CLOUD

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de

Ingeniero en Electrónica y Redes de la Información

Profesor Guía

Mg. Iván Patricio Ortiz Graces

Autor

Alexander David Caiza Caizaluisa

Año

2020

DECLARACIÓN DOCENTE GUÍA

"Declaro haber dirigido el trabajo, Propuesta metodológica de evaluación para seguridad de aplicaciones en el Cloud, a través de reuniones periódicas con el estudiante Alexander David Caiza Caizaluisa, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Iván Patricio Ortiz Graces

Magister en Redes de Comunicaciones

060235677-6

DECLARACIÓN DOCENTE CORRECTOR

"Declaro haber revisado este trabajo, Propuesta metodológica de evaluación para seguridad de aplicaciones en el cloud, del Alexander David Caiza Caizaluisa, en el semestre 202020, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

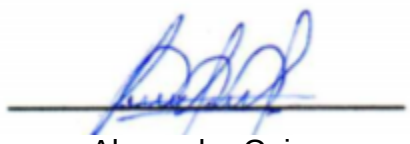
William Eduardo Villegas

Doctor en Filosofía

1715338263

DECLARACIÓN ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”



Alexander Caiza

172563248-1

AGRADECIMIENTOS

Ante mano a Dios por darme la salud y darme una familia que siempre estuvo ahí en los momento malos y buenos.

Agradezco a mis padres Carlos y Patricia por apoyarme en mis estudios ya que confiaron en mis capacidades y ya estoy cumpliendo una meta más de mi vida y decirle que los amo un montón.

También quiero agradecer a mi mamita Delia ya que fue el apoyo incondicional en todo momento y darme muchas fuerzas y decirme que si soy capaz de ir cumpliendo cada una de mis metas.

A mi hermano Roberto por ser el gran ejemplo a seguir y darme esos consejos que a veces uno recuerda con el tiempo, también quiero desearle lo mejor en su vida y que siga siendo la misma persona que nunca cambie.

A mi hermana Emelyn por ser la mejor hermana que dios me pudo dar ya que con sus ocurrencias me han sacado sonrisas en momento que uno no se imagina.

A todos mis familiares y amigos que siempre estuvieron apoyando en el trascurso de mi carrera dándome alientos para culminar mis estudios.

A mi niñito Rey de la Paz, aunque no sea
Una persona físicamente, sentí su apoyo
con las cosas que le pedí me cumplió por
eso te agradezco un montón y que
siempre estén protegiendo a todos los que
me rodean.

RESUMEN

El presente documento tiene como objetivo identificar el estado actual de las aplicaciones alojadas en la nube la misma que proporciona beneficios de almacenamiento, procesamiento de datos, recursos, fiabilidad, compatibilidad, disponibilidad, accesibilidad, seguridad y el cumplimiento de las necesidades del cliente o usuarios. La nube ha revolucionado al mundo permitiendo adoptar las nuevas tecnologías a un costo accesible, alcanzando mayor productividad y escalabilidad con el mínimo esfuerzo. A pesar de que existen algunas desventajas este servicio trata de brindar seguridad y confiabilidad al usuario ya que la responsabilidad no solo depende del proveedor sino también del cliente. Al momento de adquirir este tipo de servicio se debe considerar las necesidades de la organización o requerimientos del usuario para contratar el servicio.

El proyecto de titulación también se refiere sobre la seguridad de las aplicaciones que se encuentran en la nube considerando las normativas ISO 250010, 27001, 27018 y los protocolos de protección que siguen los proveedores para brindar un adecuado servicio. Así mismo, existen diversos métodos de protección para mantener la información segura, confiable y alojada en la nube la cual va a ser utilizada por usuarios actuales y futuros. Por ello, la concentración masiva de recursos e información en la nube se ha convertido un motivo para que los atacantes cibernéticos intenten adquirirla de cualquier manera la información.

Para finalizar se diseñará un modelo técnico de seguridad basándose en las normativas ISO para mantener la seguridad de la información que se aloja en la nube de manera segura y confiable. Además, que los clientes estén satisfechos y que las organizaciones progresen.

ABSTRACT

This document aims to identify the current status of cloud-hosted applications which provides benefits for storage, data processing, resources, reliability, compatibility, availability, accessibility, security and meeting the needs of the customer or users. The cloud has revolutionized the world by allowing new technologies to be adopted at an affordable cost, achieving greater productivity and scalability with minimal effort. Although there are some disadvantages this service tries to provide security and reliability to the user since the responsibility depends not only on the supplier but also on the customer. When purchasing this type of service, the needs of the organization or the user's requirements for contracting the service must be considered.

The titling project also addresses the security of cloud applications by considering ISO 250010, 27001, 27018 and the protection protocols that providers follow to provide an adequate service. In addition, there are various methods of protection to keep information secure, reliable and hosted in the cloud which will be used by current and future users. Therefore, the massive concentration of resources and information in the cloud has become a reason for cyber attackers to try to acquire it in any way information.

Finally, a technical security model will be designed based on ISO standards to maintain the security of information that is hosted in the cloud in a safe and reliable manner. In addition, clients are satisfied and organizations progress.

ÍNDICE

Índice de Figuras

Índice de Tablas

1. Introducción

Antecedentes

A la hora de trabajar con información en la nube, las empresas que prestan este servicio deben garantizar la integridad de los datos de sus usuarios. Para ello, existen las normas ISO 25010, 27001 y 27018, las que apuntan a fortalecer la ciberseguridad en servicios en la nube. En épocas anteriores los dispositivos se enfocaban solo en almacenamiento de datos y procesamiento en la unidad final, que eran los usuarios. Actualmente la computación en la nube permite sobrellevar estas limitaciones y mejorar el rendimiento de las aplicaciones. Con respecto a las normas, estas constituyen algunos de los principales estándares para resguardar la ciberseguridad y garantizar la integridad de la información alojada en la nube. Estos servicios son ofrecidos por empresas como:

Amazon Web Services (AWS), que ofrece servicios en línea para otros sitios web o aplicaciones del lado del cliente. La mayoría de estos servicios no están expuestos directamente a los usuarios finales, sino que ofrecen una funcionalidad que otros desarrolladores puedan utilizar en sus aplicaciones.

Google Cloud, que se refiere al espacio virtual a través del cual se puede realizar una serie de tareas que antes requerían de hardware o software y que ahora utilizan la nube de Google como única forma de acceso, almacenamiento y gestión de datos.

Microsoft Azure es un conjunto completo y en expansión constante de servicios en la nube que ayudan a su organización a afrontar sus desafíos. Azure le ofrece la flexibilidad de crear, administrar e implementar aplicaciones en una red mundial con las herramientas y las plataformas que se prefiera.

La computación en la nube es la tendencia en la que los recursos se proporcionan a un cliente local ha pedido, generalmente a través de Internet. Por tanto, Mobile cloud computing (MCC) ofrece numerosas ventajas. Por ende, los hackers también

están interesados en ella para cometer crímenes de diversa índole. Varios ataques tales como ingeniería social, ataques a las firmas, inyección de programa maligno, manipulación de datos, suplantación de cuentas, saturación del tráfico, y el ataque a la red de área local inalámbrica.

Alcance

El alcance del trabajo de investigación pretende elaborar un método para la evaluación de seguridad de aplicativos en el cloud. Mediante un estudio profundo sobre las normativas ISO 25010 que está enfocado en la calidad del producto, ISO 27001 que describe cómo gestionar la seguridad de la información en una organización y la ISO 27018 diseñado para proteger datos personales en la nube.

Analizar los servicios que brinda los proveedores principales del servicio en el Cloud, determinando sus características y ventajas, con el objetivo de brindar confianza los clientes. Además, contará con métodos para la evaluación de los aplicativos en la nube.

Justificación

Este proyecto de investigación es importante porque da una revisión teórica sobre los factores que permiten una mejor utilización de la nube. Se analizarán teorías sobre la nube, de igual manera se presentarán estudios sobre las normativas de organización internacional para la estandarización que le han permitido dar un sustento teórico de base a esta investigación.

Los problemas de seguridad siguen siendo la razón más común para evitar el uso de los servicios en la nube pública para las empresas, las cuales prefieren pagar el costo de oportunidad al no permitir el acceso y consiguiente uso de estas plataformas a sus empleados.

Otro beneficio de esta investigación es detectar si estos factores provocan un grado de utilización en el cloud y poder medir en que porcentajes deben estar presentes. También poder detectar en qué medida las empresas tienen una dependencia directa, que se tomaría con la nube al trabajar con estos tipos de normativas.

Objetivo General

Plantear una metodología para evaluar la seguridad de aplicaciones en el Cloud.

Objetivos Específicos

- Analizar el estado actual del manejo de seguridad de aplicaciones en el cloud.
- Investigar las diferentes normativas y procedimientos referentes a la seguridad sobre aplicaciones en el cloud.
- Diseñar el modelo basado en Normas ISO enfocadas en la seguridad.

2. Marco Teórico

En el presente capítulo se enfoca todo lo referente al cloud computing y como este ha evolucionado junto con las nuevas tecnologías que se han acoplado para brindar mayor eficiencia. Adicionalmente, se puntualizará sobre las normativas que intervienen en la seguridad de la información.

2.1 Cloud Computing

El Cloud Computing es una tecnología que nos permite acceso remoto, procesamiento de datos, almacenamiento de la información y poder tener acceso desde cualquier dispositivo electrónico. El Cloud computing o computación en la nube presta sus servicios mediante el internet para que los usuarios tenga fácil acceso de manera segura y rápida. Como lo puede ver en la siguiente figura 1.

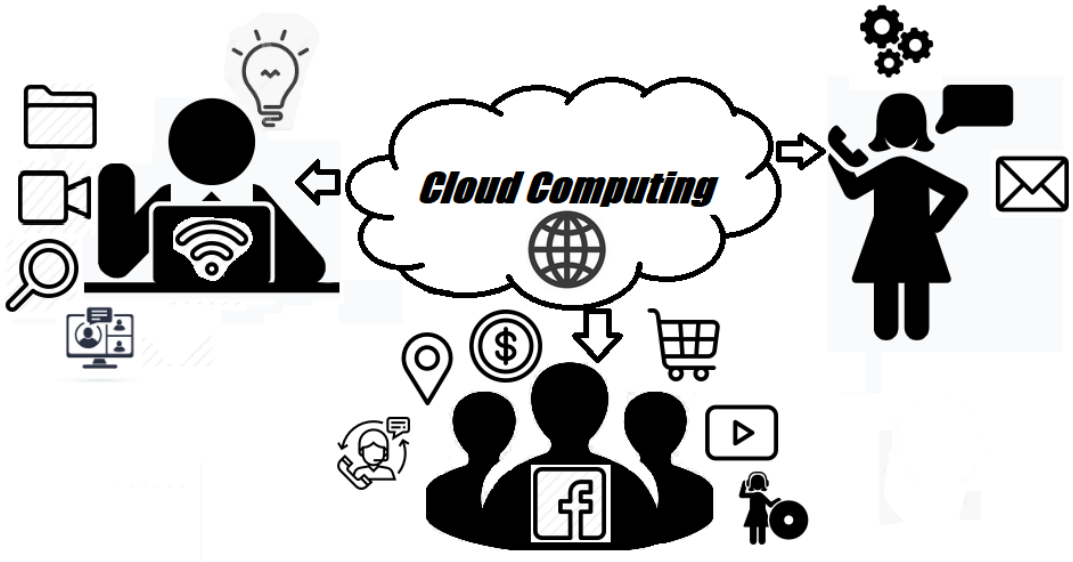


Figura 1. Cloud Computing.

2.2 Funciones del Cloud Computing

El Cloud Computing utiliza la red para conectar todos los dispositivos que utilizan los usuarios para realizar las diversas gestiones a su necesidad. También, brinda la confianza a sus usuarios mediante las empresas que ofrecen estos servicios las cuales dan soporte de mantenimiento a su infraestructura.

El almacenamiento es primordial, la nube cumple con las características como diferentes tipos de almacenamiento que varían dependiendo de la configuración de cada usuario. Por ende, disponen de bases de datos accesibles con la misma presentación que la instalada localmente.

2.3 Tipos de Servicios del Cloud Computing

Se puede agrupar los tipos de servicios que brinda el cloud Computing para ser implementados según los requerimientos del solicitante o de la empresa. A continuación, explicación de cada uno de ellos.

2.3.1 Servicio (IaaS)

Proporciona a sus clientes acceso a los recursos informáticos primarios, como la capacidad de procesamiento, la capacidad de almacenamiento de datos y la conexión en red, en el contexto de un centro de datos seguro.

2.3.2 Servicio (PaaS)

Orientadas a los equipos de desarrollo de software, las ofertas de PaaS proporcionan infraestructura informática, almacenamiento y también un nivel de plataforma de desarrollo, con componentes tales como servidores web, sistemas de gestión de bases de datos y kits de desarrollo de software (SDK) para varios lenguajes de programación.

2.3.3 Servicio (SaaS)

Los proveedores de SaaS ofrecen servicios de nivel de aplicación adaptados a una amplia variedad de necesidades empresariales, como la gestión de las relaciones con clientes, la automatización de marketing o el análisis empresarial.

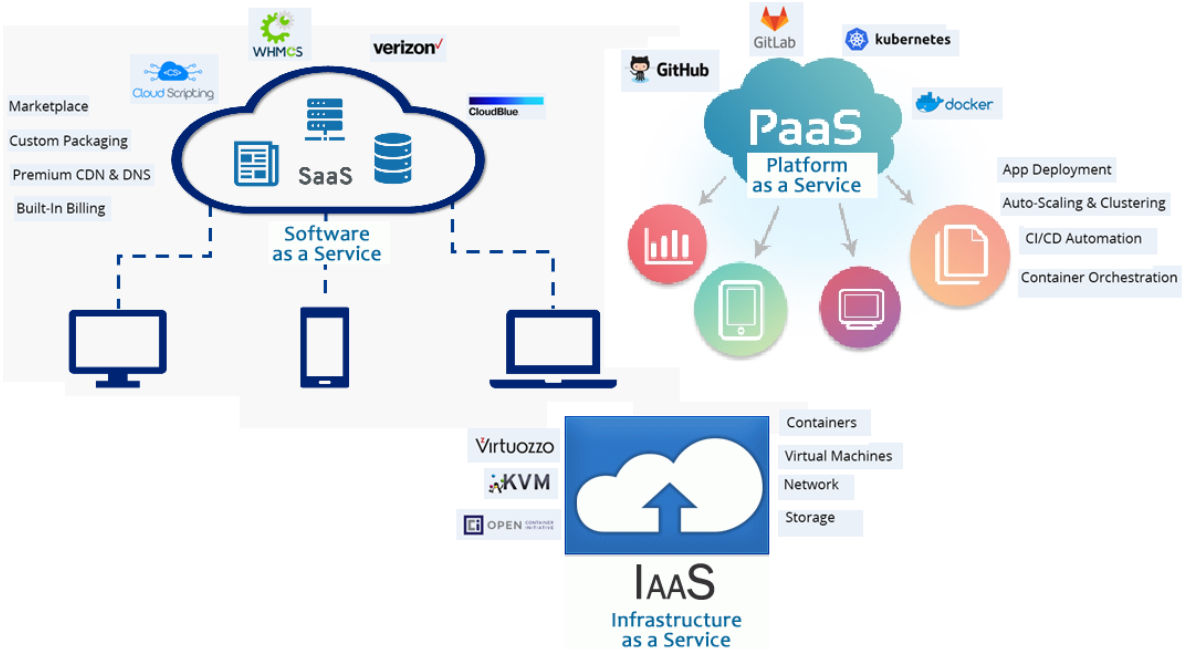


Figura 2. Tipos de servicio.

2.4 Tipos de Nubes

En el mundo existen diferentes tipos de nube en la cual los usuarios, empresas pueden alojar su información. De acuerdo con las necesidades de las organizaciones o usuarios, se adquiere el servicio y el tipo de nube. A continuación, podemos definir algunos tipos de nubes:

2.4.1 Nube Pública

La nube pública se define como servicios informáticos que ofrecen proveedores externos a través de la Internet pública y que están disponibles para todo aquel que desee utilizarlos o comprarlos. Pueden ser gratuitos o venderse a petición, lo que permite a los clientes pagar solo por el uso que hacen de ciclos de CPU, el almacenamiento o el ancho de banda que consumen. (Microsoft Azure, 2020)

Esto Quiere decir, que el proveedor dispone sus recursos de forma abierta o pagada a todos sus clientes, organizaciones por ejemplo Amazon, Azure de Microsoft o Google estos tipos de nubes brindan sus servicios de forma gratuita o pagada. Cómo se puede ver en la figura 3 la estructura de la nube pública.

2.4.2 Nube Privada

Las nubes privadas ofrecen un nivel más alto de seguridad y privacidad con firewalls de la compañía y hospedaje interno, con el fin de garantizar que las operaciones y los datos confidenciales no estén accesibles para proveedores externos. Un inconveniente es que el departamento de TI de la compañía es responsable de la administración de la nube privada y el costo que conlleva. Por tanto, las nubes privadas requieren el mismo gasto de personal, administración y mantenimiento que los centros de datos tradicionales en propiedad. (Microsoft Azure, 2020)

Otro aspecto importante de la nube privada es que brinda dos modelos de servicio. El primero Infraestructura como servicio (IaaS), que facilita a una organización utilizar recursos tales como red, almacenamiento, infraestructura como servicios. El segundo es plataforma como servicios (PaaS), que facilita a las organizaciones

obtener todos, como aplicaciones sencillas visualizadas en la nube hasta complejas. Cómo se puede ver en la figura 3, la estructura de la nube privada.

2.4.3 Nube Hibrida

La Nube hibrida está compuesta de la nube publica como de la privada dando parte de sus servicios e información de forma pública y el resto de manera privada. Por lo tanto, esta solución tiene potencial ya que ayuda al crecimiento del sistema contratando por las personas y entidades. Como se observa en la figura 3, se puede ver la estructura de la nube hibrida.

Una de las ventajas es que tiene mayor control de trabajo critico bajo infraestructura privada, flexibilidad ya que puede ser escalable gracias a los servicios que puede optar por la nube pública como privada y la sencillez dado que no todo está basado en la nube publica y su migración es gradual y controlada en las diferentes etapas que se presente o sean necesarias.

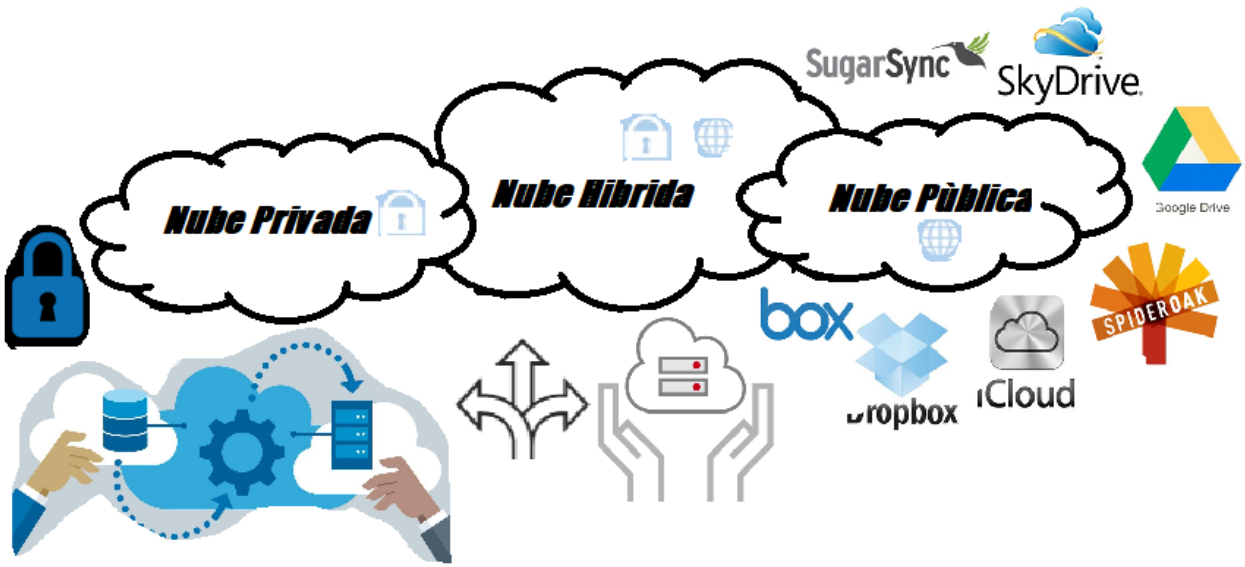


Figura 3. Nube publica, privada e hibrida.

2.5 Características de Clouds Comerciales

Después de haber explicado sobre los tres tipos de nube que existen a continuación se verá algunas de sus características.

Tabla. 1

Características de los tipos de nubes

Publico	Privado	Híbrido
Contratación vía web/teléfono	Solución a medida en base a oferta	Soluciones a medida
Muy barato	Contrato personalizado	Tecnologías hibridas: Servicios de otros proveedores Nube Pública Nube Privada
Soporte básico	Aislamiento de hardware	VPS
Plataformas Compartidas	Mayor seguridad	Servicios Gestionados
Economías de escala	Servicios gestionados	Seguridad

Tomado de: (Gestiona software en linea 2414, SN)

2.6 Ventajas

La computación en la nube proporciona muchos beneficios y ventajas para los proveedores de cloud computing, operadores de redes móviles y consumidores tales como:

- Compartir información y aplicaciones sin necesidad de hardware.
- Reducir software complejos y costosos, ya que el procesamiento de datos se ejecuta en la nube.
- Diversas características y funcionalidades mejoradas dentro de los dispositivos con la ayuda del cloud.
- Fácil acceso a través de un navegador.
- Posibilidad de que las aplicaciones sean compartida y accedida por muchos usuarios de dispositivos.
- Mayor alcance y difusión de aplicaciones.
- Mejora de la capacidad de almacenamiento de datos y procesamiento.

- Mayor nivel de disponibilidad que el entorno Cloud Computing.
- Mayor fiabilidad, ya que los datos y las aplicaciones informáticas se almacenan y copian en varios ordenadores.
- Posibilidad de un sistema de aprendizaje a distancia en el entorno de la nube.

2.7 Seguridad de la Información en la Nube

La seguridad de los datos que son almacenados en la nube por los aplicativos es la manera que hoy en día la mayoría de las personas utilizan para poder acceder desde cualquier dispositivo a su información de manera segura.

Con referente a la ciberseguridad es más segura hoy en día, ya que deben cumplir la garantía en la integridad de la información de los usuarios y organizaciones que contraten el servicio.

Cabe resaltar también que la seguridad depende del usuario y organización que dispone del servicio. Por ejemplo, al momento de autenticarse debe tener una contraseña segura ya que esto impedirá a los atacantes no puedan acceder de manera fácil.

Para las organizaciones es importante la seguridad ya que debe determinar políticas de privacidad de su información y que las personas con permisos lo puedan acceder de manera segura, entre otras condiciones que cada empresa debe especificar en sus requerimientos.

2.8 Aplicaciones

En el mundo existen variedad de aplicaciones que brindan su servicio en la nube a continuación algunos ejemplos:

2.8.1 Plataforma Google

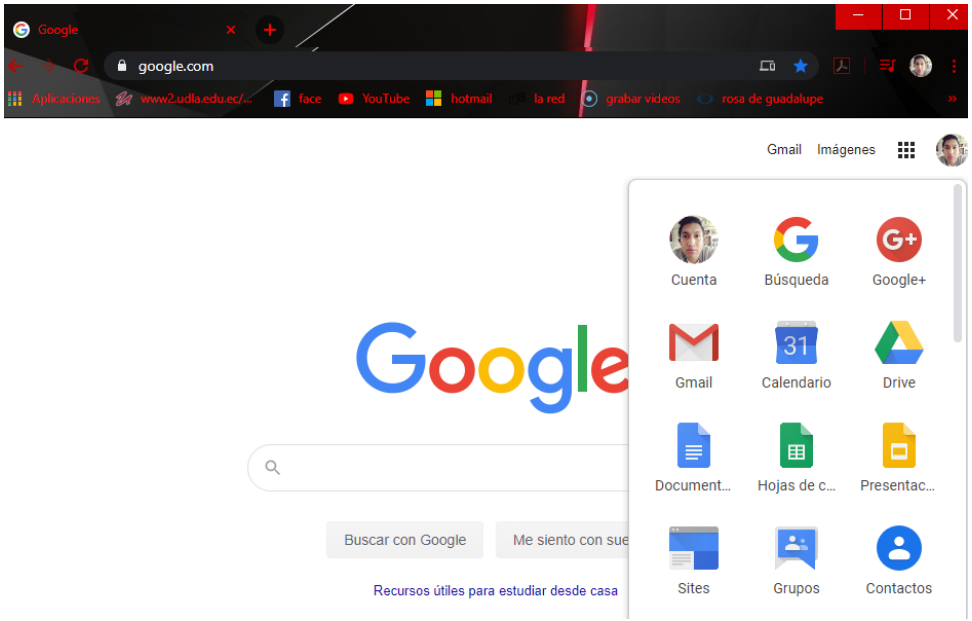


Figura 4. Plataforma de Google.

Tomado de: (Plataforma, 2020)

Como se observa en la figura 4, como primer ejemplo tenemos a la plataforma de Google https://www.google.com, que es el cliente que brinda el servicio de correo electrónico, almacenamiento entre otros servicios. Google es por esencia la plataforma cloud de servicios integrados más relevante de los últimos años, debido principalmente a la importante incursión de su buscador ya que es el día a día de las labores de millones de usuarios que lo realizan en computadoras y dispositivos que tengan conectividad al internet.

2.8.2 Office 365 (Microsoft)

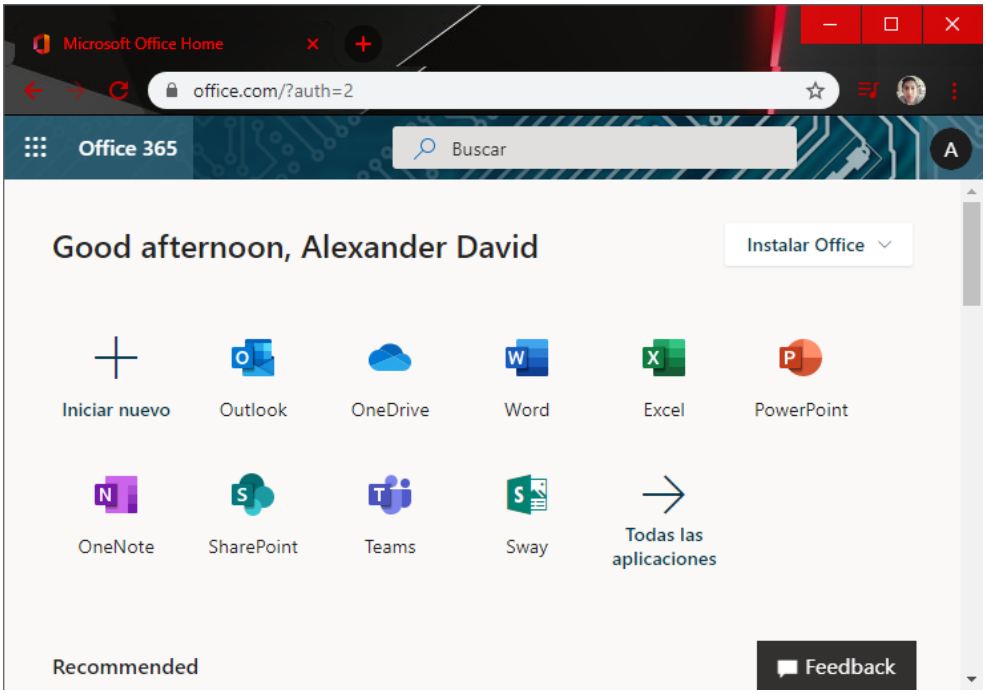


Figura 5. Plataforma de Microsoft Office 365.

Tomado de: (Plataforma, 2020)

Como se observa en la figura 5, otra aplicación bajo análisis será Office 365, que encierra un paquete de utilitarios de la empresa Microsoft, estos son: Word, Excel, PowerPoint, One Note, etc. Y que en esta versión brinda al usuario la posibilidad de utilizar estas aplicaciones desde dispositivos de escritorio, así como en dispositivos móviles.

2.8.3 Dropbox

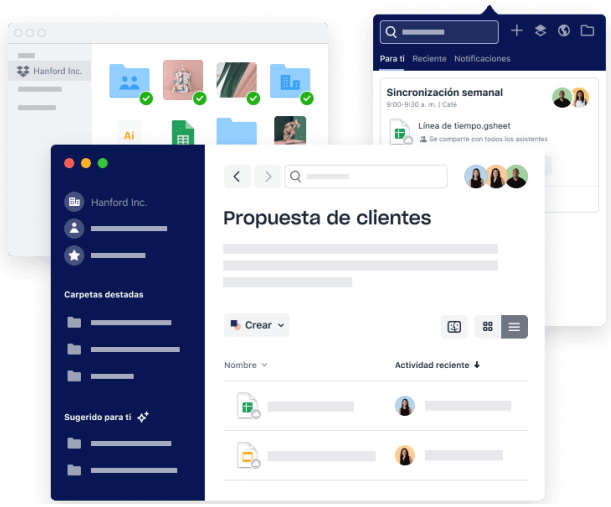


Figura 6. Plataforma de Dropbox.

Fuente: (Dropbox, SN)

Como se observa en la figura 6, Dropbox nos permite como usuarios almacenar y sincronizar toda la información en línea. Además, se puede compartir a los demás usuarios. Esta aplicación en la nube brinda su servicio de manera pagada o gratuita y sus versiones se puede encontrar para Android, Windows y iOS.

2.8.4 Spotify

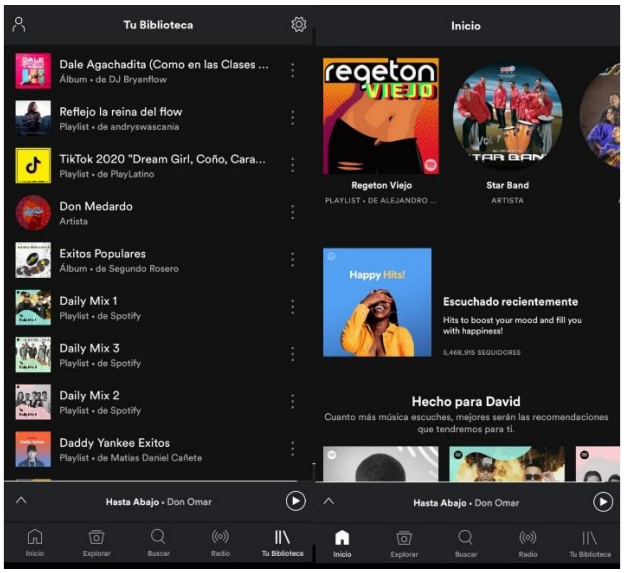


Figura 7. Plataforma de Spotify

Como se observa en la figura 7, Spotify es una aplicativo que brinda su servicio a sus usuarios de manera que puedan realizar sus actividades sin necesidad de estar cambiando de emisora ya que Spotify cuenta con gran variedad de música en línea esta aplicación da su servicio de forma pagada.

2.9 Ataques al Cloud Computing

Dentro de los ataques que tiene el cloud computing son los siguientes:

2.9.1 Abuso y mal uso del cloud computing

Principalmente afecta a los servicios PaaS y IaaS, se cuenta con un registro de acceso a las plataformas poco restrictivas. Por consiguiente, cualquiera persona con una tarjeta de crédito válida puede acceder al servicio.

2.9.2 Amenazas internas

Como en toda organización la amenaza se puede dar por los propios usuarios de la empresa dado que tiene acceso a la información y aplicaciones de la empresa.

2.9.3 Perdida de información

Esto se da cuando un usuario dentro de una organización no se siente conforme con el trato y tiene acceso a información importante puede borrarle o modificarle sin tener copia previa a la original.

2.9.4 Secuestro de sesión o servicio

Esto puede suceder si un usuario olvida cerrar sesión en un dispositivo que no es el suyo y el atacante de cualquier manera obtiene las credenciales del usuario puede realizar cualquier actividad, manipular datos, transacciones hasta redirigir a paginas maliciosas.

2.10 Normas ISO para la Seguridad en la Nube

Existen diversidades de normativas enfocadas a la seguridad la cual ayuda a que sus clientes mantengan su información de manera segura. A continuación, se detallará algunas de ellas:

2.10.1 ISO 25010

La norma ISO 25010 es un modelo que determina la calidad, funcionalidad, eficiencia, compatibilidad, usabilidad, fiabilidad, seguridad, mantenibilidad y portabilidad al momento de evaluar las propiedades de un producto determinado. Ya que el usuario debe quedarse satisfecho con la calidad del producto además la seguridad es importante para brindar confianza a sus usuarios.

2.10.1.1 Características

La norma ISO 25010 tiene subcaracterísticas las cuales se explicará a continuación:

Adecuada Funcionalidad, un producto debe tener un funcionamiento correcto ya que debe satisfacer las necesidades de los usuarios y sus requerimientos.

Eficiencia de desempeño, la eficiencia es el desempeño a la cantidad de recursos utilizados bajo determinadas situaciones.

Compatibilidad, con respecto a la compatibilidad es que un producto se pueda ejecutar en varios plataformas o componentes para interactuar la información y/o llevar a cabo sus funciones requeridas cuando comparten el mismo entorno hardware o software.

Usabilidad, capacidad del producto software para entenderse, aprenderse, ser usado y resultar atractivo para el usuario, cuando se usa bajo determinadas condiciones.

Fiabilidad, cuando el sistema desempeña funciones especificadas, cuando se usa bajo condiciones y tiempo determinado.

Seguridad, enfocados en la protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos.

Mantenibilidad, esta característica representa la capacidad del producto para modificarse con eficiencia y eficacia, debido a necesidades de actualizaciones, correcciones o sugerencias.

Portabilidad, Capacidad del producto o componente de transferirse de forma efectiva y eficiente de un entorno hardware, software, operacional o de utilización a otro.

Los beneficios del modelo buscan proporcionar una metodología para evaluar un producto de software con el objetivo de obtener la calidad esperada.

- Permite identificar los criterios que debe tener un producto software respecto a la calidad interna y externa que espera un usuario.
- Permite que las empresas o personas que están desarrollando un software evalúen su producto buscando llevar al usuario un producto de alta calidad.
- Mejora la calidad del producto.

2.10.2 ISO 27001

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y explicar cómo gestiona la seguridad de la información en una organización, se desarrolló en base a la norma británica BS 7799-2 que contiene la especificación para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora.

Esta norma ISO puede implementar en diferentes tipos de empresa públicas, privadas, pequeñas o grandes para la gestión de la seguridad. Además, permite que las empresas posean un certificado; esto significa que la empresa mantenga credibilidad al momento de proporcionar información verídica.

2.10.2.1 Características

La norma ISO 27001 permite el aseguramiento de la información gracias a las siguientes características:

Análisis de riesgo, la norma exige que la empresa haga un análisis de riesgos de seguridad periódicamente y siempre que se propongan o se establezcan cambios significativos.

Compromiso de alta dirección**,** la norma también exige el compromiso con el SGSI, además de ser esa parte de la empresa ella misma la responsable por la seguridad de la información. Los líderes son también responsables de asegurar que todos los recursos para la implantación del sistema estén disponibles y asignados correctamente, y además tienen la obligación de orientar a los colaboradores para que el sistema sea verdaderamente eficiente.

Definición de objetivos y estrategias, durante la planificación, la empresa necesita tener muy claro cuáles son sus objetivos de seguridad y cuáles serán las estrategias establecidas para alcanzar esos objetivos. Los objetivos, sin embargo, no pueden ser genéricos, deben ser mensurables y tener en cuenta los requisitos de seguridad.

Recursos y competencias, la organización también debe garantizar que todos los recursos necesarios no sólo para la implementación, sino que también para el mantenimiento del sistema estén disponibles.

Documentación de la información, la norma exige que toda la información sea documentada, con identificación, definición y formato.

Seguimiento de rendimiento, los objetivos definidos en pasos anteriores deben ser medidos y acompañados, a través de la aplicación de indicadores que posibiliten análisis de la eficiencia del sistema.

Mejora continua, una vez que se alcancen los objetivos en cuanto al sistema, es necesario que la empresa implemente y mantenga un sistema de mejora continua a fin de corregir cualquier tipo de no conformidad.

2.10.3 ISO 27018

La Norma ISO/IEC 27018:2019 es un Código de prácticas diseñado para proteger datos personales en la nube. Se basa en la norma ISO/IEC de seguridad de la información 27002 y proporciona pautas de implementación sobre los controles IEC/IEC 27002 aplicables a la información personalmente identificable (PII) en la nube pública. Además, proporciona un conjunto de controles adicionales y asesoramiento relacionado a fin de satisfacer los requisitos de protección de la información personalmente identificable en la nube no cubiertos por el conjunto de controles existentes de la norma ISO/IEC 27002. (Amazon Web Services, 2020).

El estándar ISO 27018 funciona de dos maneras:

- Se basa en los controles ISO 27002 existentes con artículos relativos a la privacidad en la nube.
- Proporciona controles de seguridad de los datos personales completamente nuevos.

2.10.3.1 Beneficios de la norma ISO/IEC 27018

Inspira confianza en su negocio, da una mayor seguridad a clientes y partes interesadas de que los datos y la información está protegida.

Reduce los riesgos, garantiza la identificación de los riesgos y la aplicación de controles para su gestión o posible reducción.

Ayuda a crecer a su negocio, proporciona una guía común en diferentes países por lo que es más fácil hacer negocios a nivel mundial y obtener acceso como un proveedor preferido.

3 Estado de la seguridad en aplicativos en el cloud y su protección

En este capítulo, se analizarán los diferentes modelos y mecanismos de seguridad para las aplicaciones en el Cloud. Además, los diferentes tipos de nube que existen y cuáles son sus características.

3.1 Análisis de los Tipos de Cloud

Dentro de la gran variedad de nubes que existe a continuación se mencionará algunas de ellas:

3.1.1 Nube de Amazon Web Services

Amazon Web Services es un tipo de nube que brinda más de 175 servicios integrados de centro de datos a nivel mundial. La mayoría de las organizaciones utilizan Amazon Web Services (AWS) para reducir los costos, crecer su agilidad, actualizar de forma rápida y segura. A continuación, en la figura 8 se puede ver algunos de los servicios que brinda AWS.

Figura 8. Nube de Amazon Web Services.

3.1.2 Nube de Google

La nube de Google brinda de igual manera diversos servicios donde puedes almacenar y compartir información. Puedes acceder mediante la creación de una cuenta de Google. A continuación, en la figura 9 se puede ver el logo y algunos servicios de la nube de Google.

Figura 9. Nube de Google.

3.1.3 Nube de Microsoft

La nube de Microsoft es un término que abarca un sistemas, herramientas y servicios en la nube. Dispone de varios servicios para almacenar, ejecutar y administrar la información como video, ofimática, correo o medios sociales. A continuación, en la figura 10 se puede ver algunos de los servicios que brinda la nube de Microsoft.

Figura 10. Nube de Microsoft.

3.1.4 Nube de Dropbox

La nube de Dropbox es un lugar donde puede alojar información y utilizar herramientas que contiene para organizar toda tu información y ordenar los datos de mayor importancia a menor. A continuación, en la figura 11 se puede ver lo que contiene la nube de Dropbox.

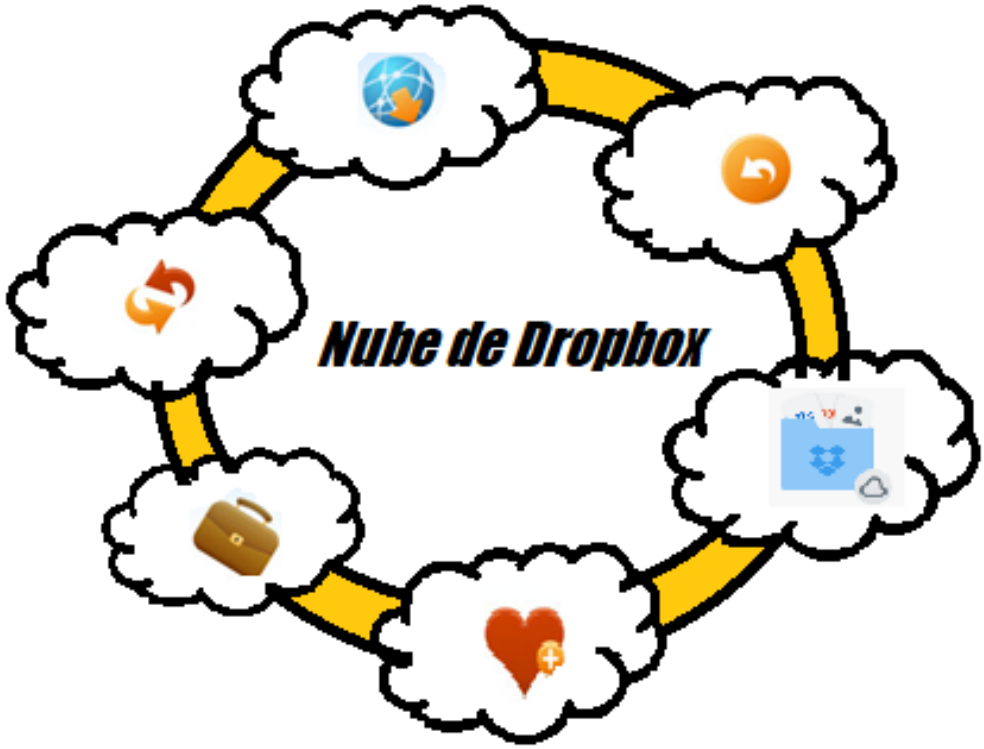


Figura 11. Nube de Dropbox.

3.1.5 Nube de Mega

La nube de mega tiene características similares a Google drive o Dropbox que facilita intercambiar o descargar archivos de cualquier tipo como: libros, películas, música, videojuegos, documentos e imagines de una forma segura. A continuación, en la figura 12 se puede observar la nube de Mega.

Figura 12. Nube de Mega.

3.2 Análisis del estado actual del uso de aplicaciones

En la actualidad la gestión de los sistemas en la nube emerge la necesidad de las organizaciones y usuarios acoplarse a un mundo hiperconectado debido a que las personas utilizan entre uno o más dispositivos para realizar el trabajo diario, esto provoca que la movilidad sea un pilar fundamental para las organizaciones y usuarios por lo cual la nube ayuda a cumplir este requisito de mantener la información segura.

Con la ayuda de la prueba de autoevaluación de Google se puede evidenciar un porcentaje de las personas que hoy en la actualidad utilizan este tipo de servicios y las aplicaciones que se encuentran alojadas en la nube, además, saber que tanto conocen sobre el cloud computing, como sus beneficios y desventajas. En la sección. Anexos, se encuentra la prueba de autoevaluación de Google.

Como se observa en la figura 13, un total de 50 personas respondieron sobre que tanto saben del cloud computing. Detallando así que un total de 20 personas

respondieron en un rango (10% - 30%) que saben sobre el cloud Computing, 15 personas respondieron entre (40%-60%) y 15 personas respondieron en un rango (70%-100%).

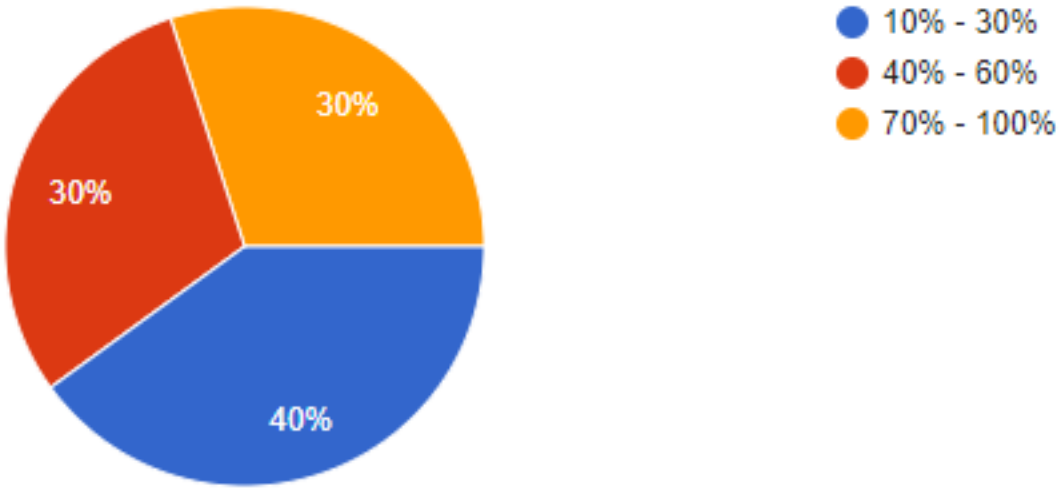


Figura 13. ¿Cuánto conoces del Cloud Computing?

Fuente: (Test de autoevaluación, 14)

Tabla. 2

Cuantas Personas conocen del Cloud Computing

	10% - 30%	**40% - 60%**	**70% - 100%**
¿Cuánto Conoces del Cloud Computing?	40% (20)	30% (15)	30% (15)

Como se observa en la figura 14, un total de 47 personas respondieron a la aplicación de Google que utilizan para almacenar su información y utilizar los recursos que este mismo proporciona. En segundo lugar, un total de 30 personas respondieron a la aplicación de Netflix a la cual utilizan sus servicios. En tercer lugar, un total de 19 personas respondieron que utilizan otras aplicaciones. En cuarto lugar, un total de 16 personas respondieron a las aplicaciones de Dropbox y Spotify para utilizar los recursos que proporciona.

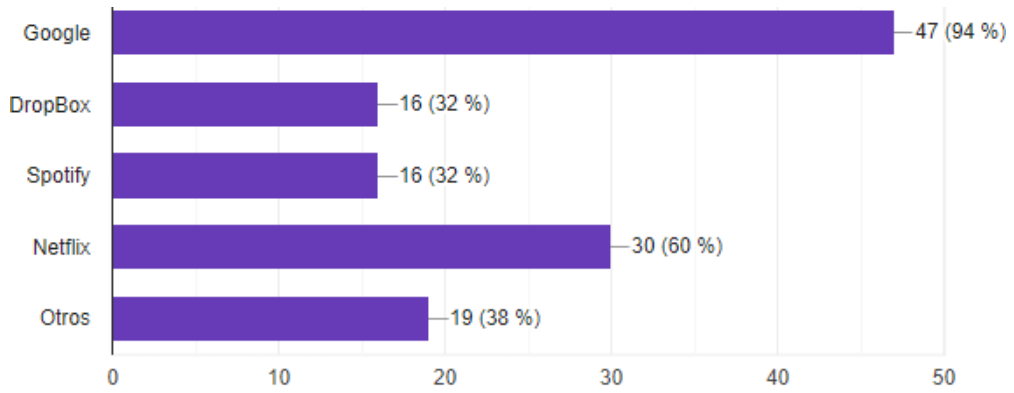


Figura 14. ¿De los siguientes aplicativos cual utilizas?

Fuente: (Test de autoevaluación, 14)

Tabla. 3

Aplicaciones que utilizan las personas

	Google	**Dropbox**	**Spotify**	**Netflix**	**Otros**
¿De los siguientes aplicativos cual utilizas?	94% (47)	32% (16)	32% (16)	60% (30)	38% (19)

Como se observa en la figura 15, un total de 39 personas respondieron que, si recomendasen un aplicativo que utilicen para sugerir a un amigo, familiar o conocido, un total de 2 personas dijeron que no recomendarían y un total de 9 personas dijeron tal vez.

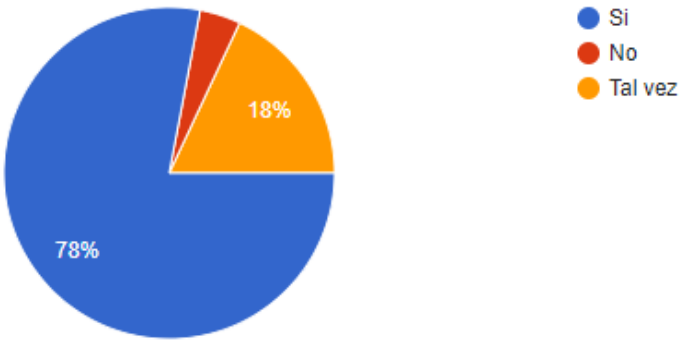


Figura 15. ¿Recomendarías un aplicativo que utilices a un amigo, familiar o conocido para que ellos utilicen y guarden su información en la nube?

Fuente: (Test de autoevaluación, 14)

Tabla. 4

¿Recomendarías un aplicativo que utilices a un amigo, familiar o conocido para que ellos utilicen y guarden su información en la nube?

	Si	No	Tal vez
¿Recomendarías un aplicativo que utilices a un amigo, familiar o conocido para que ellos utilicen y guarden su información en la nube?	78% (39)	4% (2)	18% (9)

Como se observa en la figura 16, un total de 47 personas respondieron que utilizan el servicio de correo para enviar información y un total de 3 personas respondieron que no utilizan el servicio de correo para enviar información.

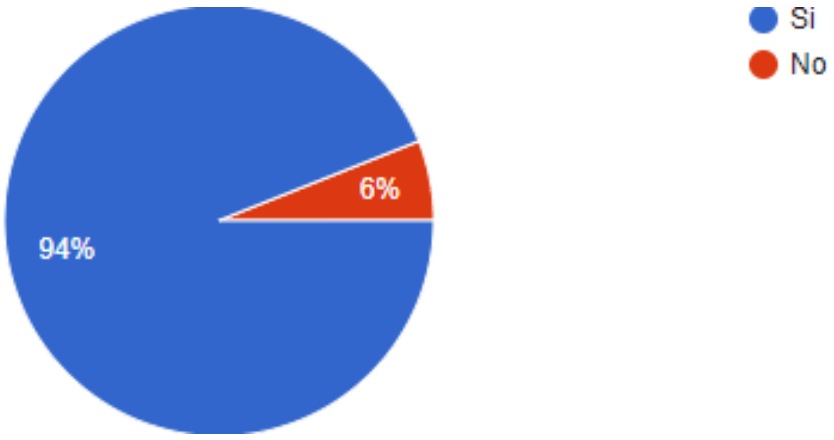


Figura 16. ¿Utilizas el servicio de correo para enviar tu información?

Fuente: (Test de autoevaluación, 14)

Tabla. 5

¿Utilizas el servicio de correo para enviar tu información?

	Si	No
¿Utilizas el servicio de correo para enviar tu información?	94% (47)	6% (3)

Como se observa en la figura 17, un total de 42 personas respondieron que utilizan entre uno o tres aplicaciones para guardar su información y un total de 8 personas respondieron que utilizan entre cuatro y seis aplicaciones para guardar su información.

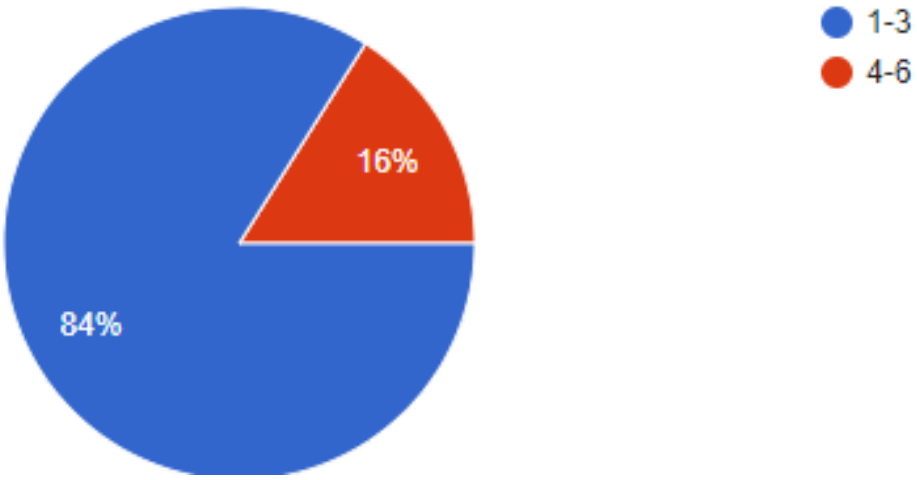


Figura 17. ¿Cuántas de tus aplicaciones utilizas para guardar tu información?
Fuente: (Test de autoevaluación, 14)

Tabla. 6

¿Cuántas de tus aplicaciones utilizas para guardar tu información?

	1 - 3	**4 - 6**
¿Cuántas de tus aplicaciones utilizas para guardar tu información?	84% (42)	16% (8)

Como se observa en la figura 18, un total de 49 personas respondieron que si les gustaría abrir desde cualquier tipo de dispositivo para abrir su información y un total de 1 persona dijo que no.

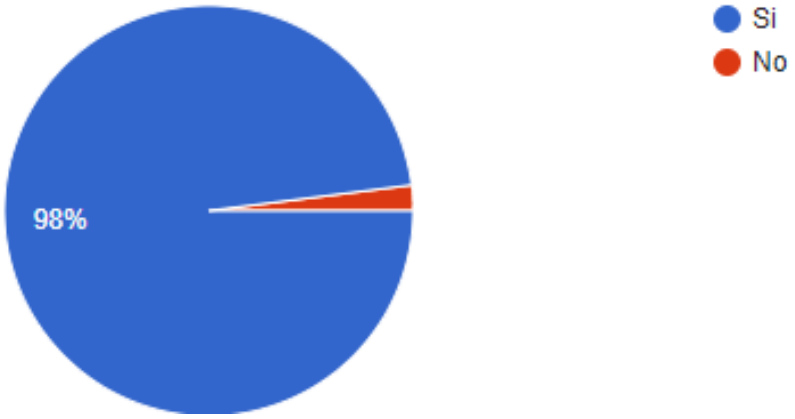


Figura 18. ¿Te gustaría abrir, compartir desde cualquier dispositivo tu información de forma segura?

(Test de autoevaluación, 14)

Tabla. 7

¿Te gustaría abrir, compartir desde cualquier dispositivo tu información de forma segura?

	Si	**No**
¿Te gustaría abrir, compartir desde cualquier dispositivo tu información de forma segura?	98% (49)	2% (1)

En conclusión, la encuesta de Google nos permitió saber que la mayoría de las personas utilizan aplicaciones para almacenar su información y utilizar sus recursos para mantener sus datos de manera confiable y segura. Por otro lado, la mayoría de las personas encuestadas dijeron que si les gustaría abrir desde cualquier dispositivo su información. Por ende, la seguridad es importante para que los usuarios confíen en utilizar los recursos que nos brinda la nube. Adicionalmente, se propone un modelo de seguridad por lo que se está realizando este tema de titulación para facilitar a los usuarios movilidad y este seguro su información en la nube.

3.3 Estado de la seguridad en la nube

En tiempos anteriores los resultados obtenidos referentes a la seguridad de la información de grandes, medianas y pequeñas empresas al enfrentar al traslado a la nube ha tenido algunas vulnerabilidades, pero en la actualidad se ha ido mejorando estos mecanismos ya que son uno de los factores principales para el crecimiento de la organización y poder simplificar los equipos de almacenamiento de datos, así acoplarse a las últimas tecnologías que van apareciendo

Por otro lado, el costo de estos servicios de seguridad sigue siendo el primer criterio al momento de contratar el servicio. Ya que los proveedores se enfocan en la satisfacción del cliente o usuario.

3.4 Servicio del Cloud Computing

Dentro de los servicios del cloud Computing existen 3 tipos a continuación se explicará cada uno de ellos:

3.4.1 Infrastructure as a Service (IaaS)

Es una manera de cloud computing que brinda recursos de manera virtual a través de la red o conocido internet. IaaS permiten a sus clientes consumir solo lo que se requiere mientras descargan su complemento. IaaS esta entre las tres principales de servicio de cloud computing, junto a SaaS y PaaS.

3.4.1.1 Arquitectura y como funciona

En un tipo de IaaS, un proveedor que brinda su servicio en la nube donde se alojan los elementos de infraestructura tradicional presente en un DataCenter local, adjuntando los servidores, hardware de red y almacenamiento. Así como, la capa de virtualización o hipervisor. Por tanto, el proveedor de IaaS brinda variedad de servicios para añadir a sus elementos de infraestructura. Por ello, puede incluir monitoreo, seguridad, facturación detallada, acceso al registro, respaldos, recuperación y equilibrio de carga, así como firmeza de almacenamiento. Como lo observa en la figura 19.

Estos servicios se basan en políticas lo que permite a los clientes de IaaS ejecutar mayor nivel de automatización para tareas de infraestructura. Por ejemplo, un usuario de una organización puede implementar políticas para mejorar el rendimiento, disponibilidad y equilibrio de carga de información de la aplicación.

Mientras que los clientes de IaaS pueden acceder a los recursos mediante el internet y utilizar los servicios del proveedor de la nube para complementar su requerimiento restante para el uso de las aplicaciones. También, los clientes pueden utilizar los servicios para monitorear, equilibrar el tráfico y dar soporte a aplicaciones y administrar la recuperación de información ante un desastre.

Figura 19. Arquitectura IaaS.
Fuente: (Microsoft Azure, 2020)

3.4.1.2 Como se maneja la seguridad en IaaS

El servicio IaaS se enfoca en la disponibilidad de capacidad de cómputo como el procesamiento, almacenamiento o red entre otros. Por ende, este servicio es el más cercano al hardware y a la tecnología de virtualización.

Por esta razón, la seguridad de estos servicios está enfocados en la virtualización. El Instituto Nacional de Estándares y Tecnología (NIST) identifica una serie de temas de seguridad basados a estos tipos de servicios que el proveedor brinda.

Por ello los proveedores de servicio IaaS tanto en la nube publica, privada o hibrida, se recomienda utilizar la Guía de seguridad para las tecnologías de virtualización dispuestas por el instituto nacional de estándares y tecnologías, la cual dispone de una serie de lineamientos que debe cumplir y seguir para prevenir cualquier tipo de riesgo en la seguridad.

3.4.1.3 Beneficios de IaaS

Entre los beneficios de IaaS existen los siguientes:

Mayor fiabilidad, permite facilitar las migraciones de carga de trabajo entre instancias de IaaS, asegurando todos los recursos estén ahí cuando se necesite.

Mayor seguridad**,** los proveedores de IaaS brindan seguridad a todo momento como elementos centrales de su modelo de negocio.

Soporte DevOps, los equipos de prueba, desarrollo y operaciones obtienen acceso inmediato a la infraestructura para acelerar en gran medida las operaciones de desarrollo y soporte

Enfoque comercial, debido a que sus servicios se encuentran en la nube, las empresas pueden destinar más tiempo y energía a sus modelos comerciales centrales.

3.4.1.4 Ventajas del servicio IaaS

Entre las ventajas del servicio IaaS son las siguientes:

Eliminación de gastos de capital y reduce los costos corrientes, permite evitar el primer gasto inicial, por lo que conforma una opción económica para organizaciones nuevas o que quieran adquirir nuevas ideas.

Mejora la continuidad empresarial y la recuperación ante desastres, el servicio brinda disponibilidad, continuidad y la recuperación de información ante cualquier desastre ya que requiere una cantidad de tecnología como personal para lograr dicha ventaja.

Innovar con rapidez**,** si la organización decide comercializar un producto nuevo o iniciativa, la infraestructura ayuda a cuestionar este requerimiento en horas o minutos, en lugar de días o semanas que tardaría una configuración interna.

Aumentar la estabilidad, la confiabilidad y la compatibilidad, con IaaS no hay necesidad de actualizar o realizar mantenimiento el software y hardware de manera periódica ya que el proveedor del servicio garantiza que la infraestructura sea confiable y cumpla con las necesidades del servicio contratado.

Mayor seguridad**,** con el contrato del servicio IaaS adecuado el proveedor brinda la seguridad de la información y de sus aplicaciones.

Hace llegar las aplicaciones nuevas a los usuarios con más rapidez**,** puesto que la organización localmente no tiene que configurar primero la infraestructura para desarrollar las aplicaciones y entregar a sus clientes.

3.4.2 Platform as a Service (PaaS)

El servicio de PaaS es un ambiente de desarrollo e implementación completo en el cloud, permitiendo entregar la mayoría de los recursos necesario desde una aplicación sencilla hasta una aplicación compleja. Al momento de contratar el servicio solo paga por los recursos que contrata los cuales accede de manera segura por internet. Al igual que el servicio de IaaS, PaaS incorpora infraestructura de almacenamiento, servidores y redes, pero también incluye middleware, herramienta de desarrollo, servicios, administración de base de datos. PaaS está diseñada soportar el ciclo de vida de cada una de las aplicaciones: pruebas, compilaciones, implementación, actualización y administración.

PaaS permite eludir el gasto y complejidad que supone la administración y compra de las licencias de software. Usted administra cada una de las aplicaciones y los servicios que desarrolla y, normalmente, el proveedor de servicios en la nube administra todo lo demás.

3.4.2.1 Arquitectura y cómo funciona el servicio PaaS

El servicio de PaaS no reemplaza con totalidad la infraestructura de una organización, sino que tiende a agregar varios componentes de infraestructura de nube subyacentes como servidores, sistemas operativos, base de datos, equipos de red, middleware y servicios de almacenamiento todas de estas funciones son dominio del proveedor las cuales tienen que configurarlas, operarlas y dar mantenimiento. PaaS dispone también de recursos adicionales tales como: lenguajes de programación, herramientas de desarrollo, bibliotecas y sistemas de gestión de base de datos.

Un proveedor de servicio PaaS proporciona y crea un ambiente optimizado y resistente en los que cada uno de los usuarios puedan instalar aplicativos y conjunto de datos. Esto permite que los usuarios puedes enfocarse en crear y ejecutar sus aplicativos en lugar de construir y mantener la infraestructura de la organización y los servicios subyacentes.

Como se dijo anteriormente no reemplaza toda la infraestructura de una organización para el desarrollo del software. Se basa a través de la infraestructura hospedada de un proveedor de servicios en el cloud. PaaS se puede entregar a través de nubes públicas, privadas e híbridas para brindar servicios como alojamiento de aplicaciones y desarrollo en Java. a continuación, en la figura 20, se puede ver la arquitectura de PaaS.

Figura 20. Arquitectura de PaaS.

Fuente: (Microsoft Azure, 2020)

3.4.2.2 Como se maneja la seguridad en el servicio PaaS

El servicio PaaS maneja su seguridad en base de reglas de seguridad de la red, acceso y aplicaciones. También, el servicio PaaS para organizaciones dispone de herramientas integrales coherentes para auditorias y registros. Por otro lado, fortalece, simplifica la seguridad y apresura la respuesta a nuevas amenazas en distintos componentes. PaaS perfecciona la resistencia empresarial y minimiza el tiempo de inactividad al tiempo que evita perdida de información y busca la mejor manera de recuperación.

3.4.2.3 Tipos de Servicios PaaS

Existen varios tipos de servicios PaaS que actualmente se encuentran disponibles para los desarrolladores:

PaaS Público, es la mejor opción para empresas pequeñas y medias que requieran el uso de la nube pública. Un servicio PaaS publico permite a los usuarios contralar la implementación del software, de esa manera, el proveedor del servicio en la nube administra el resto de los componentes importantes para el alojamiento de los aplicativos incluyendo base de datos, servidores, sistemas operativos y de almacenamiento.

PaaS Privado, tiene como objetivo brindar la agilidad de PaaS público al tiempo que sustenta la seguridad, cumplimiento y beneficios. Un PaaS privado se entrega como un dispositivo o software dentro del firewall al usuario, que se encuentra frecuentemente en el centro de datos localmente de la empresa. PaaS privado brinda mejor uso del servicio a los desarrolladores mejorando el uso de recursos. Dicho de otro modo, permite que sus desarrolladores puedan implementar y administrar sus aplicativos al mismo tiempo que se cumple los requisitos de privacidad y seguridad.

PaaS Híbrido**,** es la combinación entre PaaS público y Privado para facilitar a las organizaciones la flexibilidad de la capacidad infinita suministrada por un PaaS

público y la eficiencia de los costos de adquirir una infraestructura interna en PaaS privado.

PaaS Comunicación, es el servicio en la nube que facilita a los desarrolladores agregar comunicaciones en tiempo real de sus aplicaciones. Normalmente, este tipo de comunicaciones son creadas con el fin de que sus usuarios mantengas la comunicación. Por ejemplo, WhatsApp, Skype, Microsoft Teams y la telefonía tradicional. Los proveedores de este tipo de comunicación proporcionan soporte y documentación del producto.

PaaS Mobile, es un servicio de entorno de desarrollo de pago para las aplicaciones móviles sean configuradas. Este tipo de servicio se entrega desde un navegador web lo cual le hace compatible con la nube publica, privada y almacenamiento local. También, proporciona una interfaz de arrastrar y soltar (orientada a objetos) permitiendo a los usuarios simplificar su desarrollo. Por otro lado, es compatible con diversos sistemas operativos.

PaaS Open, es una plataforma de código abierto y se diseñó para permitir a los usuarios implementar rápidamente nuevas aplicaciones con el objetivo de desarrollar una tecnología PaaS que esté comprometida con las aplicaciones de colaboración empresarial, específicamente aquellas implementadas en nubes híbridas.

3.4.2.4 Beneficios de PaaS

A continuación, algunos beneficios específicos que su organización puede obtener al utilizar PaaS:

Adopción más rápida, fácil y menos riesgosa de una gama más amplia de recursos, proporciona variedad de acceso de opciones en la pila de desarrollo de cada aplicación como: base de datos, sistemas operativos, middleware, bibliotecas de código y componentes. Por otro lado, permite adoptar nuevos sistemas, herramientas, idiomas sin tener que colocar la infraestructura necesaria para efectuarlo.

Escalabilidad fácil y rentable, es escalable ya que se puede adquirirlo la cantidad necesario de recursos al momento de querer aumentar sus requerimientos por ende su rentabilidad.

Menores costos, debido a que no hay infraestructura para construir, sus costos son económicos. Por ende, los proveedores de PaaS cobran a los clientes en función de uso.

3.4.2.5 Ventajas de PaaS

Entre las ventajas que brinda el servicio de PaaS son las siguientes:

Reducir el tiempo de programación, las herramientas de PaaS reducen el tiempo ya que brinda su servicio con aplicaciones ya creadas en su plataforma con esto ayuda el fluido de trabajo, servicios, seguridad, características, búsqueda, etc.

Desarrollar para varias plataformas (teléfonos móviles) con mayor facilidad**,** estos proveedores brindan sus servicios en diferentes tipos de plataforma sea como teléfonos, PC, navegadores lo que permite agilitar y facilitar el desempeño de las aplicaciones multiplataformas.

Usar herramientas sofisticadas a un precio accesible**,** este modelo brinda este tipo de servicio de pago por uso, los clientes u empresas pueden hacer uso del software de desarrollo y herramientas.

Colaboración en equipos de desarrollo distribuido, **l**os trabajadores dentro de la organización pueden aportar para el desarrollo de una aplicación que sean afines al tema.

Administrar el ciclo de vida de las aplicaciones con eficiencia, el servicio PaaS brinda todas estas características para mantener el ciclo de vida de cada una de las aplicaciones como: pruebas, administración, compilación, actualización e implementación, dentro del mismo entorno.

3.4.3 Software as a Service (SaaS)

El servicio SaaS está enfocada a brindar sus servicios de sus aplicaciones mediante el internet. Por ejemplo, Microsoft Office, Netflix, calendarios entre otros aplicativos, por ende, es un modelo de pago por uso. Esto quiere decir, que un usuario a través del internet contrata uno de estos servicios para su empresa o uso personal y lo utilice normalmente con un explorador web. En referente a su infraestructura subyacente, el software, middleware y la información de las aplicaciones en encuentran alojadas en la base de datos del proveedor.

El proveedor de SaaS es el encargado de administrar el software, hardware, el servicio contratado con esto debe garantizar la seguridad, disponibilidad, confiabilidad y la información que se encuentre a su disposición. SaaS al igual que el servicio PaaS permite que las empresas comiencen ejecutando sus aplicaciones con un costo inicial mínimo.

3.4.3.1 Arquitectura y cómo funciona el servicio de SaaS

Este tipo de arquitectura utiliza una versión única de un aplicativo, con una configuración para los clientes. Como se puede ver su arquitectura en la figura 21. Todas las aplicaciones se instalan en diferentes máquinas para el crecimiento de escalabilidad denominada (escala horizontal). En ciertos casos, se configura en segundo plano la versión de la aplicación para realizar pruebas a un grupo selecto. Existen dos tipos de servicios SaaS:

SaaS Vertical**,** es un software garantiza las necesidades de una organización especifica. Por ejemplo, software de organizaciones de finanzas, Bienes raíces, la industria de la salud.

SaaS Horizontal, los servicios SaaS horizontal se centran en una categoría de software como puede ser: ventas, recursos humanos, marketing, herramientas de desarrollo los cuales son independientes de la organización.

Funcionalidad, el servicio de SaaS brinda su servicio a través del internet de manera centralizada. Los clientes crear sus respectivas cuentas y la forma de pago se factura de manera mensual o anual. Referente a sus aplicaciones se ejecutan de manera online no es necesidad que el usuario tenga instalado la aplicación en su dispositivo. Por ende, el proveedor es responsable de: la disposición, la actualización, el mantenimiento. Mientras que los clientes se limitan a acceder al software mediante un navegador. El acceso se puede dar desde cualquier dispositivo que mantenga conexión a internet ya que lo único necesario es iniciar sesión con las credenciales correspondientes del cliente.

Figura 21. Arquitectura SaaS.

Fuente: (Microsoft Azure, 2020)

3.4.3.2 Como se maneja la seguridad en el servicio SaaS

El servicio de SaaS está involucrado en los firewalls, configuración de DNS, detención de intrusos, utilización de puertos. También, el servicio SaaS se enfoca en la seguridad del canal de transmisión de la información de la empresa o usuario, esto significa altos niveles de autenticación SSL y TSL (protocolos criptográficos), para prevenir que los atacantes no pudieran entrar y romper las reglas de seguridad, aunque los datos estén cifrados están expuesta.

3.4.3.3 Beneficios y ventajas del modelo SaaS

Con la información anterior sobre el SaaS (Software As a Services), se detallaras algunas de sus ventajas y beneficios:

Menor costo de utilización, con el servicio de SaaS no se requiere adquirir el software, equipo especifico, licencia y menos gastar en su mantenimiento y su actualización. Por ende, su costo es menor.

No necesita máquinas para alojar el software, el software está alojado en el cloud, sin la obligación de un ordenador específico para mantenerlo en actividad. Esto permite mayor usabilidad, agilidad.

Acceso en cualquier lugar**,** lo único que toca tener es un dispositivo conectado a internet. Esto facilita que utilices un programa de la organización desde tu hogar o cualquier localidad que te encuentres y con el avance de la disponibilidad de tener acceso a internet, el área de cobertura genera posibilidades de uso.

Opción adaptable a las necesidades del cliente, si el servicio no satisface la necesidad que se requiere el cliente, es posible añadir paquetes adicionales o a su vez personalizar el servicio y así aumentar la eficiencia del servicio contratado.

Actualizaciones de forma automática, a comparación con un software común se invierte en las actualizaciones pagando distinto con el software como servicio eso no es necesario ya que las actualizaciones se realizan de manera automática por lo que esta alojada en la nube.

Integración con otros sistemas de forma fácil, entre las ventajas del servicio SaaS tiene la posibilidad de la integración con otros sistemas, por ello ya vienen diseñadas para su integración de manera rápida y simple.

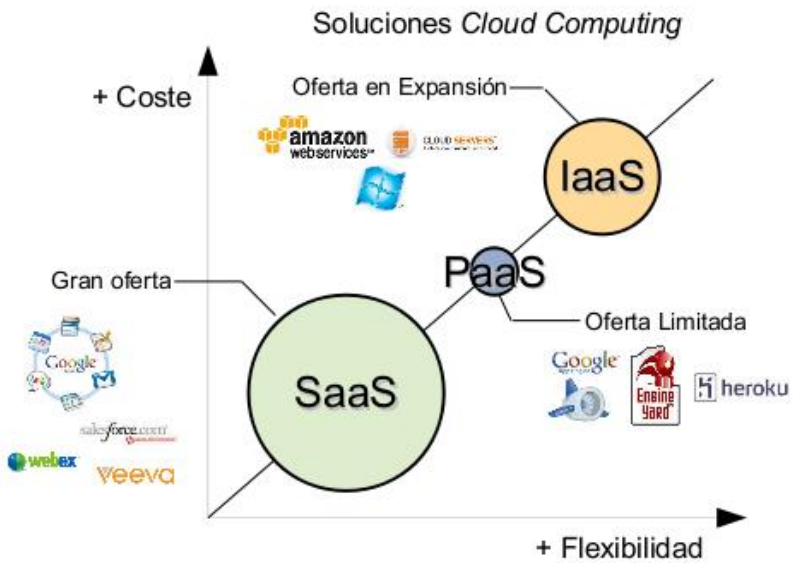


Figura 22. IaaS, PaaS y SaaS.

Fuente: (Arquitecturas de TI, 2014)

3.5 Mecanismo de protección en el cloud

Gracias a las soluciones que brinda el cloud computing enfocadas en la seguridad en gran medida depende de los proveedores del servicio ya que ellos son los responsables de gestionar que el servicio sea adecuado y seguro. Para explicar de mejor manera definamos quienes son los involucrados en los modelos del cloud computing.

3.5.1 Proveedor de servicio

Es la organización que dispone de la infraestructura necesaria para alojar los programas, aplicaciones entre otras características la cual brinda sus servicios a sus respectivos clientes.

3.5.2 Clientes

Como su nombre lo dice es aquel que contrata el servicio en la nube (empresas, personas) para favorecerse de los servicios por los cuales paga.

3.5.3 Usuario

Es la persona o grupos de involucrados cuales utilizan los servicios acordes a la empresa los requiera. No es necesario que el cliente sea el que utilice el servicio.

Por ejemplo, dentro de una organización los usuarios finales son los encargados de utilizar dichos servicios o soluciones que contrata la empresa. Como se puede ver en la figura 23, los involucrados al momento de adquirir estos servicios.

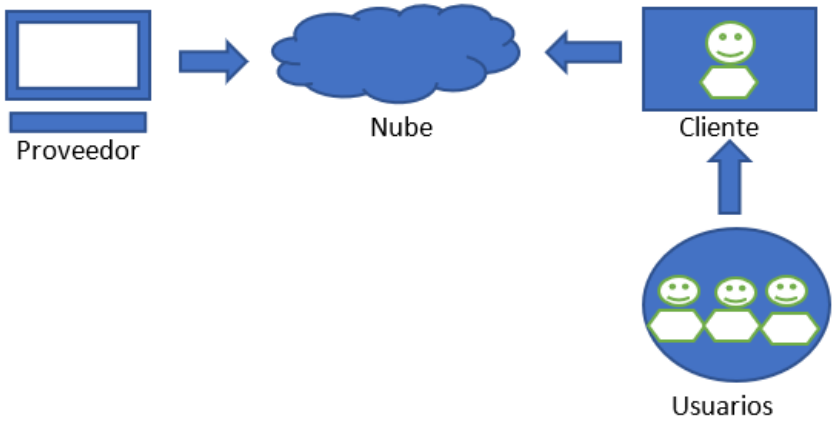


Figura 23. Involucrados en el cloud computing.
Fuente: (Ecuador Patente nº 1, 2020)

3.5.4 Medidas de seguridad que deben cumplir los proveedores del cloud computing

La medida que debe cumplir los proveedores de servicio en el cloud es impedir que terceras personas no autorizadas puedan obtener la información de sus clientes. También, es importante mantener actualizados las últimas versiones de su software para tener mejor protección ante un posible ataque en la red. Por otro lado, reforzar la seguridad, implementar la virtualización y segmentar la información.

3.5.5 ¿Y los clientes?

También los clientes toman un papel importante al momento de mantener el sistema actualizado y ver mejoras de seguridad que vayan mostrándose el transcurso que la tecnología va avanzado. Por otro lado, es necesario sustentar políticas de seguridad: revisión del software para verificar que no haya vulnerabilidades, eliminar cuentas que ya no estén en funcionamiento, el control de usuarios entre otras políticas.

3.5.6 Prevención frente a perdidas

Entre la mayoría de los riesgos que presenta una organización al momento de adquirir el servicio de cloud computing es la perdida de datos, ya dependa de que el usuario borre información accidentalmente, fallo de dispositivos o realizan un ataque de manera brusca. Por otro lado, perder información valiosa de una empresa no solo significa que toca comenzar de nuevo sino pérdidas económicas. La solución a este problema se puede dar de dos maneras.

En primer lugar, el uso correcto de políticas de seguridad limitando la información a sus usuarios de manera jerárquica, protección de los equipos a utilizar dentro y fuera de la organización para que los atacantes no puedan acceder a la información de la empresa. El proveedor de servicio es el encargado de brinda la solución o soluciones adecuadas con los elementos necesarios electrónicos. Por ejemplo, si detectan algún fallo dentro de la organización inmediatamente deberá asilar el proceso y los procesos restantes deberán de alguna manera migrar y dar seguimiento al problema para solucionarlo. El proceso deberá durar al menos unos minutos sin necesidad de interrumpir los demás servicios, dando disponibilidad el trabajo del resto.

En segundo lugar, realizar el uso correcto de las políticas de copia de seguridad permitiendo la recuperación de la información, aunque todos los mecanismos de seguridad hayan fallado o un desastre ambiental. Todos los proveedores del cloud computing ofrecen este servicio de copia de seguridad de manera transparente para el cliente. Para esto, solo es necesario seleccionar los dispositivos que requiera realizar el proceso y dar prioridad de acuerdo con la necesidad que se requiera hacer la copia. La recuperación frente a un atacante puede ser sencilla como la restauración de snapshot (copia instantánea de volumen) anterior de la máquina virtual.

Las características detalladas anteriormente permiten alinear un sistema robusto con capacidad de recuperación ante cualquier desastre natural o ataque

informático, permitiendo a la organización avance con el negocio. Por último, hay variedades de ventajas extras que son los dispositivos portátiles ya que las organizaciones permiten a sus empleados utilicen para realizar su trabajo. Por ello, estos dispositivos pueden extraerse o ser robados y exhibiendo la información a personas que no pertenezca a la organización. Por esto, al utilizar estos sistemas de prevención en el cloud, ya que, si se pierde un dispositivo o es robado, los datos de la organización permanezcan inaccesible para personas que no sean parte de la organización.

3.5.7 Cifrado de la información

Otro método para mantener segura la información de la empresa es el cifrado o conocido como encriptación, es un proceso el cual incrementa la seguridad y permite ocultar la información legal de la empresa (documentos, mensajes, etc.) por lo tanto, la codificación de la información por medio de un algoritmo permite invisible los datos a terceras personas y visible al destinatario.

Esto se realiza para mejorar la protección de los datos tanto para la organización como para sus clientes. Por ejemplos, al momento de realizar un pedido sea de comida, víveres, etc. la información de la transición como es datos personales suele cifrase con el propósito de mantener a salvo dicha información.

Para las empresas proveedoras de servicios TI manejen adecuadamente los datos de sus clientes y no tenga perdida de información, lo primero en realizar, es el cifran la información por ende para que la otra parte lo desea ver tiene que haber un descifrado. Lo que permite un nivel de complejidad para terceras personas puedan acceder y los proveedores tiene a ganar a más clientes por su prestigio y confianza.

3.5.7.1 Tipos de cifrados

Existen variedades de tipos de cifrado a continuación se explicará algunos:

Simétrico, el emisor con el receptor realiza la misma clave para realizar el cifrado como descifrado de la información permitiendo así complejidad para terceros.

Algunos ejemplos tenemos como: Blowfish (es un codificador de bloques simétricos), IDEA, DES. El mecanismo lo puede ver en la figura 24.

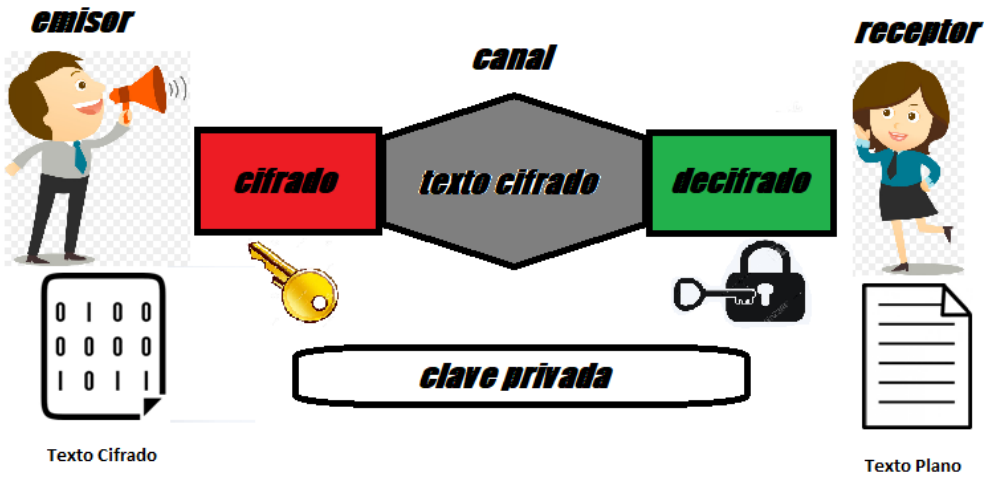


Figura 24. Cifrado simétrico.

Asimétrico, este tipo de cifrado es utilizado para servicio de correo, es para asegurar la confidencialidad y autenticar cualquier firma digital. Existen claves públicas como privadas. Poe ejemplo, DSA, RSA, Diffie-Hellman. Como puede ver en la figura 25 el cifrado Asimétrico.

Figura 25. Cifrado asimétrico.

Cifrado Hibrido, es la combinación del cifrado simétrico como asimétrico ya que aprovecha la fortaleza del uno y ligereza del otro por lo que garantiza la conexión segura. Algunos de los métodos de cifrado:

Secure Socket Layer (SSL), Es un protocolo de cifrado que permite comunicación segura en la red esto permite autenticar los servidores de comunicación e

intercambio de claves de forma segura entre proveedor y cliente, cifrando los datos simétricamente. Este tipo de seguridad se aplica en diferentes ámbitos:

- HTTPS: protocolo seguro.
- FTP: protocolo de cambios de ficheros (SSL utiliza para seguridad).
- SMTP: protocolo de correo (SSL utiliza para seguridad).

Firma Digital, Es una forma de autenticación de personas o dispositivos a un archivo como autor para que la información sea segura e incorporar las firmas digitales, se mide los datos de las firmas, que se logra con algoritmos matemáticos. El receptor del archivo deberá extraer la cifra cifrada para que el archivo sea descifrado a través de mecanismo tecnológicos necesarios.

Los beneficios de cifrado, la protección de los datos confidenciales de una empresa esto se puede dar por la encriptación de los datos para proteger la información delicada de la empresa como: datos de los colaboradores, políticas internas, procedimientos, entre otros. Por otro lado, la comunicación se da a través de los canales que brindan el internet y son susceptibles a ser extraídos por eso la información debe ir cifrada.

Entre otros beneficios que tiene el cifrado de la información es la protección de los dispositivos móviles ya que si son sustraídos la información sigue estando segura por el cifrado.

3.5.8 Evaluar los tratamientos y riesgos de protección de la información

Los usuarios también deben estar al tanto con un estudio a detalle de los tratamientos que se realiza al momento de transferirse a los servicios de la nube, no solo considerando los beneficios, sino los posibles riesgos que se puede implicar al momento de adquirirlo deben tener previo conocimiento.

3.5.9 Contraseñas seguras

Es un mecanismo básico que todos los clientes que contratar el servicio de la nube debe cumplir, pero pocos clientes cumplen. Por ello, una clave segura es una

combinación de letras minúsculas, mayúsculas, números, caracteres y un rango aceptable para que las personas no pertenecientes a la organización no puedan acceder de manera fácil. También, es sugerible que se cambien la contraseña con frecuencia.

3.5.10 Responsabilidades y términos de uso

Dentro de la empresa debe tener un acuerdo entre el proveedor del servicio y el cliente mediante un contrato. Este contrato debe ser claro y conciso con referente a la prestación del servicio para brindar confiablidad, disponibilidad y las obligaciones que el proveedor va a dar a sus clientes. Los términos de uso deben cumplir técnicas relacionadas con la entrega y calidad del servicio. Dentro del contrato el cliente debe centrarse su atención en las siguientes partes:

Acuerdos de Nivel de Servicio**,** como sus correspondientes informes periódicos, Confidencialidad, al momento de traslado de la información y almacenamiento en sus servidores. Disponibilidad, que los proveedores mantiene el servicio activo y sin interrupciones. Rendimiento**,** asegura el potencial que tiene al momento del almacenamiento y ancho de banda.

La Seguridad es un componente primordial al momento de contratar el servicio ya que debe ser lo más seguro para que el cliente tenga confianza al momento de adquirirlo, los Pagos dependen de los clientes ya ellos deben tener al día para que su servicio sea de igual manera ya que deben incluir fechas, días exactos del servicio y el pago acorde con el proveedor. La Suspensión del Servicio está relacionado que la organización o cliente debe tener un proveedor, el Servicio de Soporte compromete al proveedor dar las 24 horas de atención a cualquier petición del cliente.

4 Normativas y Procedimientos de Seguridad para el Cloud.

En este capítulo, se detallará más a fondo sobre las normativas y procedimientos de seguridad de la información que se encuentra en la nube y como utilizarlo para mantener la información segura.

4.1 ISO 25010

El modelo ISO 25010 además que se basa en la calidad del producto también presenta una característica enfocada a la seguridad entre otras características que abarca para dar soporte a un producto. A continuación, se explicará las características que presenta este modelo:

4.1.1 Adecuada Funcionalidad

Es la capacidad del producto para dar un servicio adecuado y satisfaga la necesidad del cliente. A su vez debe cumplir subcaracterísticas:

Completitud Funcional, abarca todas las funcionalidades que debe cumplir las tareas y objetivos del cliente especifico.

Corrección Funcional, disponibilidad del sistema o producto para obtener resultados correctos a las necesidades requeridas.

Pertinencia Funcional, enfocada a proporcionar un conjunto de herramientas, funcionalidades para realizar las tareas que debe realizar los usuarios.

4.1.2 Eficiencia de desempeño

Representa el desempeño del producto a la cantidad de recursos que va a utilizar bajo condiciones que la organización disponga. A su vez debe cumplir subcaracterísticas:

Comportamiento temporal, el tiempo que demora el procesamiento y las respuestas al cumplir las funciones bajo condiciones de la organización con lo que es referentes a pruebas predeterminadas.

Utilización de recursos, es la porción de recursos que va a utilizar el software en determinadas funciones específicas.

Capacidad, disponibilidad máxima de un producto o sistema para cumplir los requisitos de la organización.

4.1.3 Compatibilidad

Posible acoplamiento a diversos sistemas para procesar la información y llevar a cabo las funciones requeridas al compartir el mismo entorno de software o hardware. A su vez debe cumplir subcaracterísticas:

Coexistencia, suficiencia del producto para ser compatible con otros softwares en entornos similares, compartiendo sus recursos.

Interoperabilidad, suficiencia de dos o más componentes o sistemas para trocar información y manejar la información o datos intercambiados.

4.1.4 Usabilidad

Aprendizaje del producto o sistema para ser entendido, usado por los usuarios bajo demanda de la empresa. A su vez debe cumplir subcaracterísticas:

Capacidad para reconocer su adecuación, permitir al usuario entender el producto o software para sus necesidades.

Capacidad de aprendizaje, explicación al usuario para que aprenda a utilizar el producto o software.
Capacidad para usarse, posibilidad que el usuario pueda controlarlo y operarlo con facilidad.

Protección contra errores de usuario, protección ante errores para que el usuario no tengas inconvenientes al utilizar el producto o software.

Estética de la interfaz de usuario, la interfaz sea agradable y satisfaga la interacción con cada uno de los usuarios.

Accesibilidad, permitir que el software o producto sea utilizado por usuarios específicos.

4.1.5 Fiabilidad

Disponibilidad del producto o componentes para el desempeño de las funciones determinadas cuando se utiliza bajo demanda y periodo de tiempo. A su vez debe cumplir con las subcaracterísticas:
Madurez, disponibilidad del producto para satisfacer las necesidades en condiciones normales.

Disponibilidad, el producto o software debe estar disponible a cualquier momento, mantenga sus operaciones y sea accesible.

Tolerancia a fallos, disponibilidad del software o producto para tener operación ante presencia de fallos de software como de hardware.

Capacidad de recuperación, capacidad del software para recuperar la información afectada y restablecerlo al estado deseado en caso de algún fallo o interrupción.

4.1.6 Seguridad

Capacidad de protección de los datos para que las personas no pertenecientes a la organización no tengan accesibilidad o puedan modificarlas. A su vez debe cumplir estas subcaracterísticas:

Confidencialidad, que la información tenga un mecanismo de protección para no permitir acceso o ser modificada por personas no autorizadas.

Integridad, prevenir a las personas no perteneciente a la organización el acceso no autorizada para modificar la información.

No repudio, demostrar los eventos o acciones que han tenido lugar para rechazar cualquier acceso no autorizado.

Responsabilidad, Capacidad de examinar de forma adecuada las acciones de una organización.

Autenticidad, disponibilidad del producto o software para demostrar la identificación del usuario o recurso.

4.1.7 Mantenibilidad

El producto puede modificarse de manera eficiente y efectiva, debido a necesidades de actualización de este, como también puede ser correcciones o perfectivas. A su vez debe cumplir con las subcaracterísticas:

Modularidad, disponibilidad del sistema o programa para permitir que un recurso o elemento tenga un impacto mínimo al resto de lo demás elementos.

Reusabilidad, reutilizar un activo para utilizar en más de un sistema o en la construcción de otros activos.

Analizable, disponibilidad para evaluar un cambio realizado en el producto o software, ver las causas y deficiencias, o identificar las partes a modificar.

Capacidad para modificarse, accesibilidad del producto para recibir cambio de forma efectiva y eficiente sin interrumpir a los demás procesos.

Capacidad para probarse, disponibilidad para realizar pruebas bajo criterios de la organización para un componente o sistema y que cumplan dichos criterios.

4.1.8 Portabilidad

Facilidad del sistema o producto para transferirse de manera eficiente y efectiva en un entorno de software, operacional, hardware o de utilización a otro. A su vez debe cumplir con las subcaracterísticas:

Adaptabilidad, el producto pueda acoplarse a cualquier sistema de forma eficiente y efectiva. Además, en diferentes entornos como software, hardware o uso.

Capacidad para instalarse, eficiencia de la instalación o desinstalación de forma exitosa en el entorno.

Capacidad para reemplazarse, capacidad del producto o software para utilizarse en otros entornos similares o tengan el mismo propósito.

4.2 ISO 27001

Después de haber mencionado algunos aspectos de la normativa ISO 27001 a continuación se va a profundizar con respecto a la seguridad que va a brindar a la información de organizaciones y usuarios.

4.2.1 Seguridad de la información

La protección de la información es muy amplia, por lo que no solo depende de una cuestión técnica, sino que es importante la responsabilidad de la organización como sus directivos. También, toca considerar los procesos, funciones, sujetos, además de la seguridad de los recursos/activos de la organización y beneficiarse de la seguridad de sus datos, dentro de los requisitos de responsabilidad de la empresa. Además, toca considerar los riesgos técnicos de TIC que son riesgos operacionales, organizacionales y físicos.

El riesgo operacional es aquel que puede ser provocado debido a errores del ser humano, fallos del sistema, procesos internos defectuosos o inadecuados y como consecuencia de acontecimientos externos en lo referente a la seguridad de los datos. Lo que permite:

Logra obtener un diagnóstico por entrevistas.

Análisis exhaustivo de todos los riesgos que se puedan presentar. Crear un plan de acción acorde a las necesidades puntuales de la empresa.

Diseño de procedimientos, Comprender todos los requerimientos de seguridad de los datos de una empresa y establecer objetivos y políticas para operar los riesgos de seguridad y puedan implementarse. Además, revisar el desempeño,

monitorización y la efectividad del sistema de gestión de seguridad de la información.

4.2.2 Importancia de la ISO 27001

Hoy en la actualidad las empresas se enfrentan a que sus datos sufran de tipo de hackeos, espionaje, fraude o mal uso por parte de sus trabajadores. Por ello, se requiere contratar herramientas o mecanismos que eviten que suceda estos sucesos.

Disponer de un sistema de seguridad de los datos permite cumplir todos los requerimientos legales de la organización y la normativa ISO 27001 ofrece una metodología que lo cumple. Ya que obtener un certificado permite dar un valor agregado frente a su competencia y brindar confianza a sus clientes actuales y futuros. Por otro lado, brinda la posibilidad que no ocurra incidente o perdida de información, es así como evita consecuencias perjudiciales y ahorro de dinero.

4.2.3 Estructura de la norma ISO 27001

A continuación, en la figura 26 se muestra la estructura que tiene la normativa ISO 27001

Figura 26. Estructura de la norma ISO.

Tomado de: (riesgoscero, SN)

Objeto y campo de la aplicación: dispone de las herramientas y uso, que beneficios trae y el método de aplicación.

Referencias normativas: son archivos que toca tener en cuenta al momento de aplicar las recomendaciones de la norma.

Términos y definiciones: Es un vocabulario que permite captar todas las palabras claves descritas allí.

Contexto de la organización: son los requisitos de la normativa, donde se busca entender el contexto de la organización y determinar sus necesidades para comprobar su alcance del sistema de seguridad.

Liderazgo: es importante originar una cultura dentro de la empresa, por ello, todos los que conforman la organización deben entender los planes de acción que se ejecutan o se llevan a cabo y de qué forma contribuyen al cumplimiento de este, es así como los líderes deben nombrar responsables y dar a conocer las políticas establecidas.

Planificación: se detalla los objetivos y como se va a realizar, como será su funcionamiento del sistema de seguridad teniendo en cuenta los riesgos ya identificados.

Soporte: disponibilidad de los recursos que sean competentes, buena comunicación y documentar la información para cada caso.

Operación: contiene la eficacia para implementar, monitorear, planificar y controlar cada proceso, crear soluciones y valorar cada riesgo.

Evaluación de desempeño: el análisis, medición y seguimiento de la evaluación del sistema o aplicación con verificar que cumpla lo establecido.

Mejora: identificar cada uno de los aspectos no funcionen para corregirlos y que cumplan el objetivo.

4.2.4 Protocolos de seguridad de la información

Es primordial comprender cuando se navega en el internet se está intercambiando información con las diferentes páginas. Para proteger estos datos se debe utilizar

protocolos de seguridad que garantice la confiabilidad y que cumplan las reglas establecidas. Por ello, se diseña para prevenir que personas no autorizadas o no pertenecientes puedan tener acceso a la información y están compuestos por:

Cifrado de datos: esto ayuda que la información viaje sobre el canal de una manera segura y llegue al receptor.

Lógica: debe cumplir un orden al momento de enviar el mensaje como los datos del mensaje, significado y a qué momento se envía.

Autenticación: esto permite que solo personal autorizado está manipulando los datos y no permite que cambia o tenga intervención por personas externas. v

4.3 ISO 27018

La normativa ISO 27018 se enfoca en las buenas prácticas para la protección de la información que se aloja en la nube. Esta normativa se complementa con las normas ISO 27001 e ISO 27002 en lo que se refiere a la protección de los datos y que va orientado específicamente a los proveedores de servicio.

4.3.1 Requisitos para la protección de los datos

El estándar ISO 27018 suministra orientación destinada a asegurar que los proveedores de servicio en la nube puedan presentar controles de seguridad de datos adecuados con la finalidad de mantener la privacidad de los clientes. A continuación, algunas medidas de innovación de la norma:

El proveedor de servicio dispone de las herramientas necesarias.

El proveedor de servicio debe vigilar el cumplimiento del tratamiento de seguridad a sus clientes.

Dispone de una prohibición establecida por la ley, se refiere si los datos personales son divulgados por las autorizaciones administrativas estos serán notificados sin demora.

El cliente debe conocer ante la subcontratación sobre la normativa antes de utilizarla.

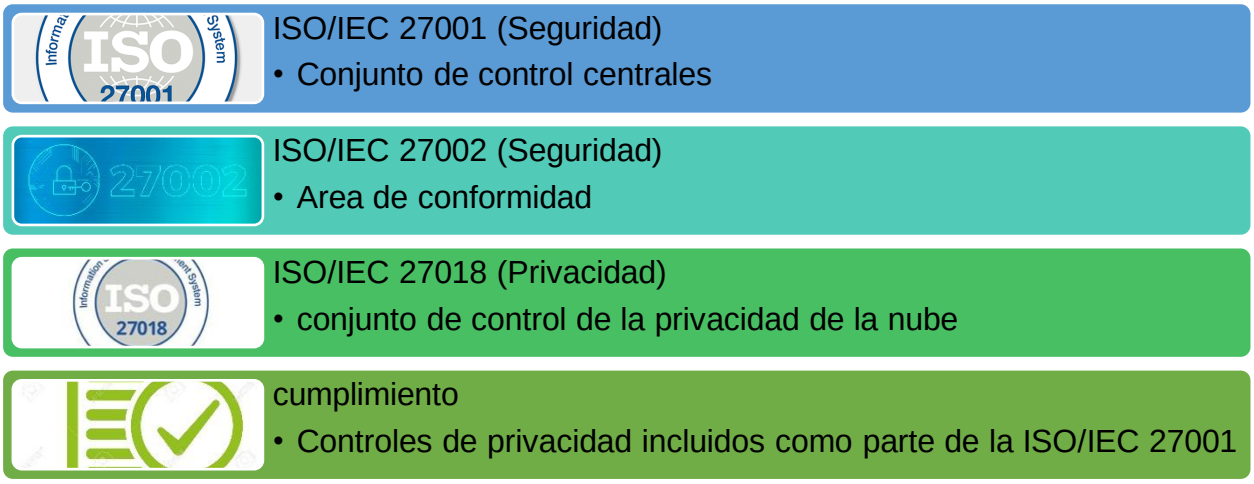
El proveedor de servicio notificara en seguida al cliente cualquier tipo de violación de la información como alteración, perdida, divulgación, destrucción o acceso no autorizado, con el fin de mantener la información segura y que los clientes estén satisfechos.

El servicio debe tener políticas de traslado que se enfoca en la transferencia, restitución o cancelación de sus datos en dominio del proveedor que acordaron en el contrato.

Las medidas de seguridad de los datos deben mantenerse en un acuerdo de confidencialidad entre el proveedor y cliente.

4.3.2 Ámbitos de aplicación y objetivo

La norma ISO 27018 ayuda a fortalecer la gobernanza de seguridad de los datos de una empresa a continuación algunas normas que se enfocan en la seguridad de la información.



4.3.3 Aportaciones

Es una norma que se alinea de modo directo con el modelo europeo de protección de la información personal y brinda confianza al mercado para los proveedores que

lo ponen en marcha. Además, la normativa ISO 27018 aprecia con transparencia la identidad de los objetivos vigentes de la norma y con los objetivos incorporarse la propuesta de reglamento general de protección de la información. Por otro lado, el crecimiento del estándar ISO 27018 incluye no solo la revisión de realizar buenas prácticas en materia de los datos en el cloud sino un instrumento útil que brinda la confianza al mercado por cumplimiento de normas del proveedor de servicio.

4.4 Procedimientos de Seguridad en el cloud

La protección de los datos es importante para la era digital y el uso seguro de los servicios que brinda la nube. Por ello, los servicios y la encriptación son puntos importantes tener en cuenta al momento de elegir una aplicación para su almacenamiento en la nube. A continuación, algunos de procesos que toca tener en cuenta.

Cloud Access Security Broker, esta es una de las soluciones disponibles para utilizar los servicios de la nube de forma segura. Es un software diseñado para proteger y controlar el acceso a la nube. Además, tiene diversas funciones que sirven como la gestión dentro de la nube, monitorización, estableciendo acciones en caso de que exista una alerta de seguridad.

Como protege Google la información e impide el acceso no autorizado**,** google utiliza una infraestructura incomparable de agilidad que dispone a sus clientes sus ventajas en el ámbito de seguridad. Google diseño G Suite cumpliendo uno de los estándares muy estrictos de privacidad y seguridad. En el siguiente enlace explica un poco más sobre como protege la información, https://www.sistel.es/seguridad-gsuite-como-protege-google-mis-datos.

Como protege la información Microsoft, protege la información de cada usuario y lo clasifica confidencialmente. También, aplica directivas de protección integral de los datos de forma manual o automática. Configura acciones de seguridad de los datos como lo es el cifrado. Por otro lado, supervisa y corrige la información confidencial en riesgos, esto quiere decir que ayuda a optimizar las directivas y obtener un

equilibrio entre la productividad y la seguridad. En el siguiente enlace profundiza sobre la protección de la información, https://www.microsoft.com/es-es/security/business/information-protection.

Realizar backup: Es una manera de tener una copia de toda la información de un usuario u organización para posibles restauraciones o recuperaciones. Las copias de seguridad cumplen con la necesidad:

Copias para recuperación ante desastres: es importante tener una copia cada determinado tiempo en caso de que suceda un desastre para no tener tanta perdida de información.

Copias operacionales: este tipo de copias es para disponer de forma instantánea de los datos en determinado momento.

La importancia de utilizar estrategias para la seguridad

Es primordial tener estrategias de seguridad que proteja la información en tres fases como: en la nube, el medio de transmisión que es la red y por ultimo los dispositivos a donde va a llegar la información.

4.5 Características de calidad y seguridad de las normativas ISO

Se puede determinar que la normativa ISO 25010 se enfoca en la usabilidad para determinar las características de calidad y seguridad, en cambio la normativa ISO 27001 ayuda al aseguramiento, integridad y confidencialidad de la información y la normativa 27018 garantiza que los proveedores de servicio en la nube ofrezcan excelentes servicios de seguridad de los datos. Por ello, presentan ciertas características para la protección de la información que se encuentra en la nube. a continuación, se destaca algunas de las características principales de cada una de las normativas explicadas en la tabla 8.

Tabla. 8

Cumplimento de las normativas ISO de seguridad.

Características de calidad/seguridad	**ISO 25010**	**ISO 27001**	**ISO 27018**
Adecuada funcionalidad	X		
Planificación		X	X
Privacidad			X
Políticas de seguridad		X	X
Cifrado		X	X
Mantenibilidad	X		
Autenticación		X	X
Facilidad de pruebas			X
Análisis de riesgo			X
Copias de seguridad		X	X
compatibilidad	X		X
conformidad		X	
Seguridad física y ambiental			X
usabilidad	X		
Evaluación de desempeño	X	X	X
soporte		X	X
Separación de desarrollo			X
Fiabilidad	X		
Seguimiento de rendimiento			X
Mejora continua		X	X
Portabilidad	X		X
Fiabilidad	X		

5 Modelo de seguridad para aplicaciones en la nube enfocadas en las normas ISO

En este capítulo, se explicará sobre el modelo de seguridad basado en las normativas que paso toca seguir para evaluar una aplicación como su monitorización, actualización, seguridad. A continuación, se detallará los pasos:

5.1 Modelo de seguridad

A continuación, se detallará cada uno de los pasos a seguir del modelo de seguridad.

5.1.1 Selección de la aplicación o sistema a evaluar

En primer lugar, ante de comenzar un procedimiento se debe seleccionar la aplicación la cual va a evaluarse. Por ejemplos, aplicaciones como se ve en la figura 27.

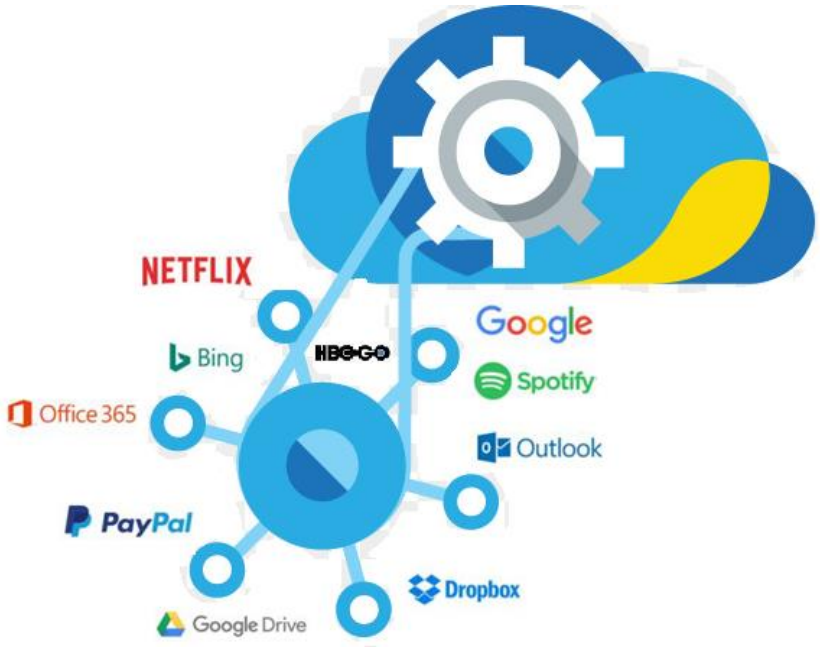


Figura 27. Ejemplo de algunas aplicaciones

5.1.2 Especificación de los requisitos de la evaluación

En este paso se identifica y se menciona los requerimientos que debe cumplir previo al diseño de la evaluación de seguridad del producto o software. A continuación, en la figura 28 se detalla los procesos y salidas que debe cumplir esta etapa.

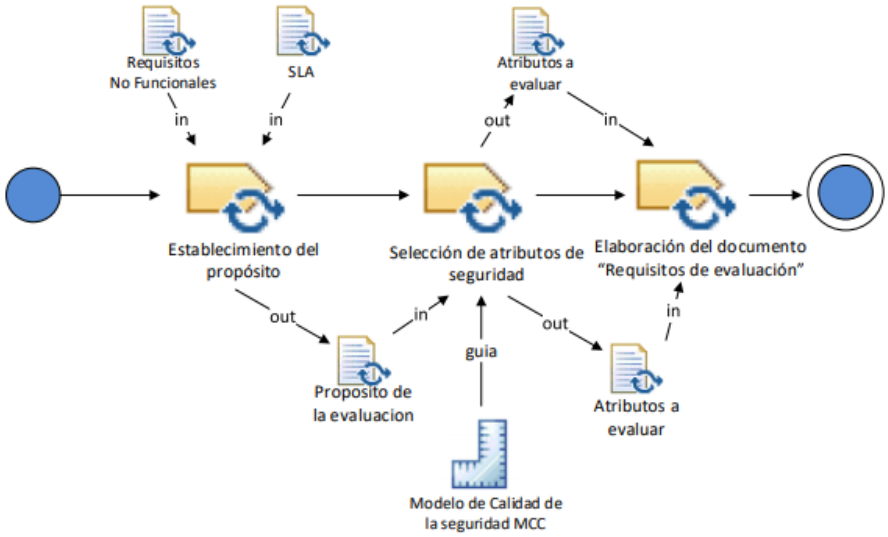


Figura 28. Especificación de los requisitos para evaluar el producto.

Fuente: (Juárez, 2017)

5.1.2.1 Establecer el propósito de evaluación

En este paso consiste en decidir que la evaluación se efectuará al cliente final en cual va a utilizar el producto es decir si va a utilizar la aplicación en SaaS, PaaS, IaaS. Por ende, es necesario seleccionar la aplicación a ser evaluada y obtener un SLA para la revisión al finalizar del proceso a ver si se cumplió todo lo requerido.

5.1.2.2 Selección de los atributos de seguridad

En este paso se especifica los requerimientos de evaluación que debe cumplir el producto, así como también quien lo solicita.

El analizador debe consolidar que los clientes involucrados del producto deben identificarse. Por eso, se necesita la información necesaria para llevar a cabo este proceso ya sea para una organización o persona y que pueda estar en todo el proceso de la evaluación. Uno es el proveedor como desarrollador, otro es el cliente aquel que necesita la evaluación, la información sobre la calidad y seguridad del producto por eso al finalizar el proceso requiere un reporte de la evaluación.

Por eso es importante tener un modelo de seguridad desarrollado por partes para facilitar sus respectivas mejoras o modificaciones. A continuación, en la tabla 9, se muestran las métricas para evaluar la seguridad.

Tabla. 9

Parámetros para evaluar la Seguridad.

	Atributos por Evaluar
1	Administración de los datos
2	Control de acceso y gestión de identificación
3	Seguridad en SLA
4	Calidad de encriptación
5	Evaluación de seguridad
6	Manipulación de la información del usuario
7	Prevención de ataques
8	Seguridad complementaria
9	Notificación y respuesta de incidentes de seguridad
10	Gestión y control de cuentas
11	Gestión de contenido antispam
12	Políticas de contraseñas seguras
13	Contexto de uso

5.1.2.3 Elaboración del Documento de Requisitos de Evaluación

Después de haber recogido toda la información se comenzará a la elaboración de un documento donde estén especificados todos los requisitos para la evaluación. Se puede utilizar plantillas para contener toda la información referente al proceso y tener previo a cualquier ataque. En el tema de definición de la plantilla para el informe de seguridad se podrá ver una plantilla de requerimientos.

5.1.3 Especificación de la evaluación

En este punto se detalla la evaluación que se realizara, que puntos se van a evaluar, que medidas se va a tomar y de qué forma, para que los resultados obtenidos se puedan ver y reportar algún fallo si se lo requiere.

5.1.3.1 Selección de Atributos Por Evaluar

En este paso se elige los componentes a ser evaluados. Por ello, nos referiremos a los modelos de calidad dichos en capítulos anteriores. Esto nos permite que para posteriores podrán verificarse con dicho informe. Los mecanismos de evaluación son documentados, teniendo en cuenta cada acción a ser ejecutada para determinar la evaluación.

5.1.3.2 Selección de Métricas Por Emplear

Después de tener los componentes de seguridad para evaluar, el modelo de calidad a elegir nos permitirá establecer métricas para cada uno de los componentes. Cabe determinar que la métrica se enfoca en la elaboración de buenas prácticas de seguridad a manera de un checklist, cuya información será evaluada por el cumplimiento de los requerimientos de la organización y construir la métrica para los componentes correspondientes. A continuación, en la tabla 10, se especifica la métrica.

Tabla. 10

Tabla de la métrica por implementar en la evaluación.

Atributos	métrica	Umbral
Administración de datos	(Componentes MDM implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Control de acceso y gestión de identificación	(Controles implementados) (# total de controles)	1 = Ideal 0 = Mejorable -1 Deficiente

Seguridad en SLA	(Seguridades implementadas en el SLA) (# total de seguridades SLA)	1 = Ideal 0 = Mejorable -1 Deficiente
Calidad de encriptación	(Características implementadas) (# total de características)	1 = Ideal 0 = Mejorable -1 Deficiente
Test de seguridad	(Componentes de prueba implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Manipulación de la información del usuario	(Seguridades de datos disponibles) (# total de Seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Prevención de ataques	(Seguridades-prevenciones implementadas) (# total de seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Seguridad complementaria	(Seguridades complementarias disponibles) (# total de seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Notificación y respuesta de incidentes de seguridad	(Acciones implementadas) (# total de acciones a implementar)	1 = Ideal 0 = Mejorable -1 Deficiente
Gestión y control de cuentas	(Controles implementados) (# total de controles disponibles)	1 = Ideal 0 = Mejorable -1 Deficiente
Gestión de contenido antispam	(Componentes implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente

Políticas de contraseñas seguras	(Políticas implementadas) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Contexto de uso	(Componentes implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente

5.1.3.3 Definición del Criterio de Decisión para los procesos

El criterio se establece para cada uno de los procesos elegidos. También, son usados para enfocarse el nivel de confianza de las aplicaciones analizadas. Como prevención el tema de seguridad es realizada para evitar cualquier tipo de incidente, sin embargo, se intenta abarcar las precauciones para reducir los riesgos y mejor su seguridad.

5.1.3.4 Definición de la Plantilla para el Informe de Seguridad

En este paso se va a diseñar un documento donde abarca todos los problemas de seguridad para ir buscando un método de seguridad y tomar una buena decisión. En la tabla 11, se encuentra los elementos que debe contener:

Tabla. 11

Plantilla de para el informe de seguridad.

ID del proceso	Número de proceso para identificarse
Nombre del proceso	Nombre del proceso a analizar
Propósito del proceso	Explicación o heurística del atributo evaluado con las diferentes métricas y controles relacionados a cada uno.
Perspectiva MCC	Se indica la perspectiva desde la que se está evaluando
Tipo de nube	Se puede seleccionar si es MCC: Público, Hibrido o Privado.

Modelos de Servicio	Servicio MCC Opciones de servicio a ser evaluado: IaaS, PaaS o SaaS.
Escala	Unidades de medida (ej. porcentaje)
Nivel para el cumplimiento	Objetivo con el que el indicador o atributo es considerado como aceptable.
Medición	Registro de los valores obtenidos de acuerdo con el cumplimiento de cada uno de los controles verificados en cada elemento.
Nivel de cumplimiento	Valoración numérica obtenida como resultado de la medición planteada.

5.1.4 Diseño de la evaluación

Después de haber seleccionado la aplicación o software a evaluar y especificar los requerimientos necesarios se procede a diseñar el modelo de evaluación, como se mira en la figura 29.

Figura 29. Diseño de la evaluación

Fuente: (Juárez, 2017)

Elaboración del plan de evaluación, en los fundamentos recompilados en el proceso anterior. En este paso se comienza a la elaboración del plan de evaluación

de seguridad el cual no va a contener tareas duplicadas y va a estar enfocada en la decisión del proceso como el cuándo y porque el motivo de la evaluación. Esto nos va a permitir disminuir el riesgo de errores y minimizar el esfuerzo de la evaluación a futuro.

5.1.5 Ejecución de la evaluación e Informe de seguridad

En este punto se obtiene el plan de evaluación y las especificaciones de los elementos y métricas observadas que serán evaluadas y por consecuencia la elaboración del informe de resultados respectos a la seguridad. A continuación, en la figura 30, se muestra el proceso de ejecución de la evaluación.

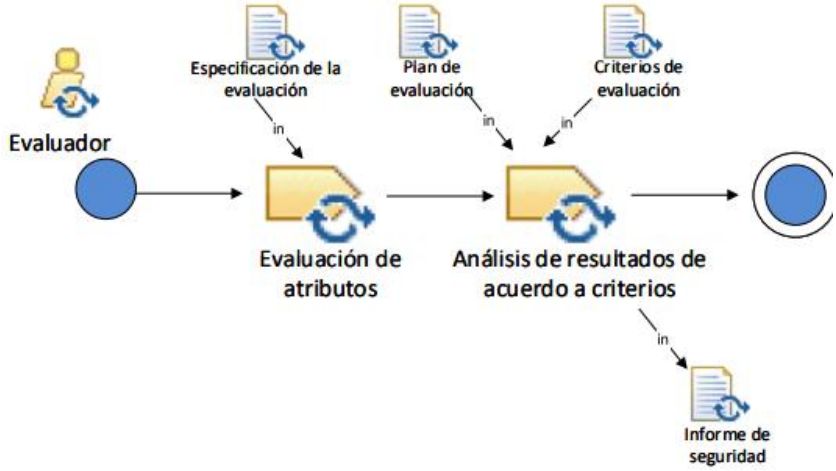


Figura 30. Proceso de Ejecución de la evaluación

Fuente: (Juárez, 2017)

5.1.5.1 Evaluación por atributo

En este punto se valida todos los ítems de seguridad sobre la aplicación o producto alojado en la nube. El cual el checklist evaluado cumple o no con los requerimientos.

5.1.5.2 Análisis de resultado de acuerdo con el criterio

En este punto toda la información recompilada se analizará cada uno de los atributos respecto a los requerimientos y criterios de evaluación expuesto en los anteriores pasos, después se entrega un informe final sobre la seguridad del

aplicativo o producto. A continuación, algunos aspectos que deberá contener el informe:

Indicar un apropiado grado de confianza al cliente o usuario sobre su aplicación o producto y que cumpla con los requerimientos de seguridad.

Proponer la oportunidad de escalabilidad del producto o aplicativo, así como posibles necesidades de evaluación adicional.

Identificar riesgos o vulnerabilidades en la plataforma que se brinda.

Tener documentación adicional para posible renovación de la evaluación.

5.1.5.3 Elaboración de informe de seguridad

Para este punto debe contener la plantilla de seguridad con todos los parámetros analizados y los criterios de evaluación que son las tareas en esta fase.

5.1.6 Finalización de la evaluación

Después de haber cumplido todos los pasos de la evaluación de la aplicación o sistema se procede a una revisión final con los involucrados como se observa en la figura 31.

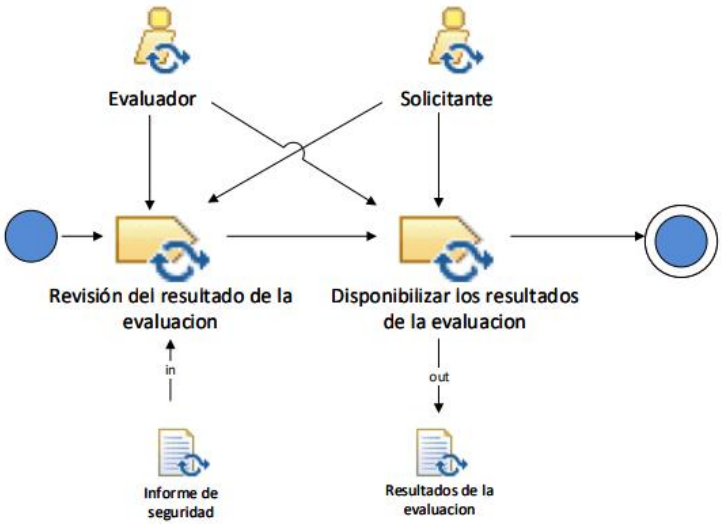


Figura 31. Proceso de evaluación

Fuente: (Juárez, 2017)

5.1.6.1 Revisar el resultado de la evaluación

El proveedor y el cliente deben llevar una revisión conjunta de los procesos ejecutados en la evaluación. Además, todos los reportes de la evaluación deben estar colocados en el informe final de la evaluación.

5.1.6.2 Disponer los datos de la evaluación

Al finalizar la evaluación, la información y los literales de evaluación deben ser concordados con los datos requeridos por el cliente o usuario. A continuación, se encuentra una evaluación del modelo plantado en este capítulo enfocado en la seguridad.

5.2 Procedimiento de seguridad en la plataforma de Google

A continuación, se comenzará a seguir cada uno de los pasos mencionados en el capítulo 4 sección 4.4 sobre el proceso de seguridad de las aplicaciones descritas en el capítulo de marco teórico en la sección 2.8.

5.2.1 Selección de la aplicación a evaluar

Como primer ejemplo de seguridad se realizará en la aplicación de Google. La plataforma de Google es unas de las aplicaciones más utilizadas por los usuarios por el buscador, ya que se realiza diariamente consultas, investigación de algo en específico, etc. Pero la plataforma de Google tiene una gran variedad de servicios con diferentes funcionalidades y características. Como se observa en la figura 32, la plataforma de Google.

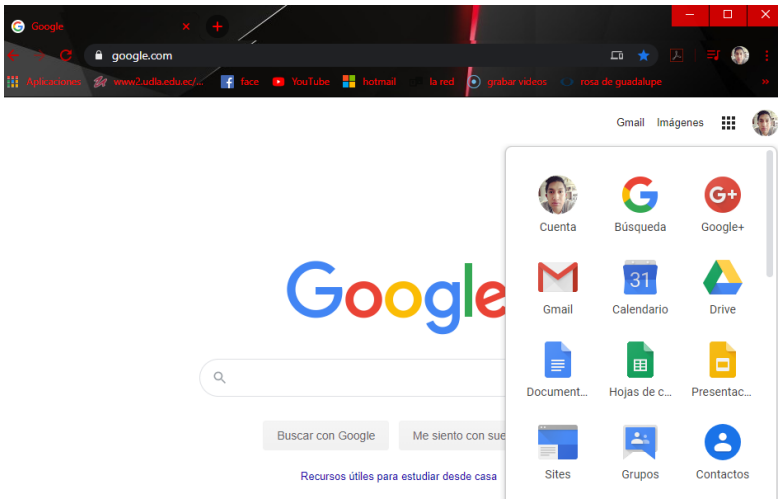


Figura 32. Plataforma de Google

5.2.2 Especificación de los requisitos de evaluación

Después de haber seleccionado la aplicación a ser evaluada se procede a establecer los requisitos para la evaluación de seguridad y detallar cada uno de los procesos que se explicó en el modelo de seguridad.

5.2.2.1 Establecer el propósito de evaluación

El propósito de la evaluación es identificar que contenga la mayor seguridad para que los clientes confíen en utilizar sus recursos. Por ello, es compatible para la versión de Android y iOS.

La plataforma de Google sobre la seguridad dice *"*La seguridad de nuestra infraestructura en la nube no depende de una sola tecnología en particular. En nuestra pila, la seguridad se establece en capas progresivas que conforman un auténtico sistema exhaustivo de defensa.*"* (Google Cloud, 2020)

Google utiliza el servicio de SaaS (Software como servicio) para desarrollo, escalabilidad y modernizar a la organización con una tecnología diferenciada que transciende la infraestructura. En el siguiente enlace podrá entrar más afondo sobre qué servicios y como opera la seguridad la plataforma de Google, https://cloud.google.com/security/infrastructure

La plataforma de Google está certificada de conformidad con ISO 27001. También, algunas normativas que están relacionadas son las ISO 27017 (Control de la seguridad de la información en la nube) y ISO 27018 (Protección de los datos personales) en el siguiente enlace encontrar algunos de los servicios de Google en el ámbito de la ISO 27001, https://cloud.google.com/security/compliance/iso-27001?hl=es

5.2.2.2 Selección de los atributos de seguridad

Los requisitos de seguridad que debe cumplir la aplicación por parte del proveedor como el cliente final se encuentran detallado en la siguiente tabla 12.

Tabla 12

Atributo para la evaluación de Seguridad.

Atributos por Evaluar	
1	Administración de los datos
2	Control de acceso y gestión de identificación
3	Seguridad en SLA
4	Calidad de encriptación
5	Evaluación de seguridad
6	Manipulación de la información del usuario
7	Prevención de ataques
8	Seguridad complementaria
9	Notificación y respuesta de incidentes de seguridad
10	Gestión y control de cuentas
11	Gestión de contenido antispam
12	Políticas de contraseñas seguras
13	Contexto de uso

5.2.2.3 Elaboración del documento de requisitos de evaluación

Se realizará un informe que refleje cada uno de los requisitos de la evaluación de seguridad de la aplicación. Por ello, se elaborará una plantilla que incluirá la información de cada uno de los atributos a evaluar.

5.2.3 Especificación de la evaluación

A continuación, se desplegará cada uno de los atributos para la evaluación de la aplicación. Que métricas se aplicara, de qué manera y como se obtiene el resultado.

5.2.3.1 Selección de atributos por evaluar

Una vez de haber especificado los atributos de evaluación se especificará una métrica para su evaluación. Por ello, se colocarán en el informe para posterior comprobación.

5.2.3.2 Selección de métrica por emplear

A continuación, se establecen los atributos de seguridad para ser evaluados. Cabe determinar que estas métricas se elaboraron basadas en una serie de buenas prácticas de seguridad a manera de checklist.

Tabla. 13

Tabla de métrica para evaluar la aplicación.

Atributos	métrica	Umbral
Administración de datos	(Componentes MDM implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Control de acceso y gestión de identificación	(Controles implementados) (# total de controles)	1 = Ideal 0 = Mejorable -1 Deficiente
Seguridad en SLA	(Seguridades implementadas en el SLA)	1 = Ideal 0 = Mejorable

	(# total de seguridades SLA)	-1 Deficiente
Calidad de encriptación	(Características implementadas) (# total de características)	1 = Ideal 0 = Mejorable -1 Deficiente
Test de seguridad	(Componentes de prueba implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Manipulación de la información del usuario	(Seguridades de datos disponibles) (# total de Seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Prevención de ataques	(Seguridades-prevenciones implementadas) (# total de seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Seguridad complementaria	(Seguridades complementarias disponibles) (# total de seguridades)	1 = Ideal 0 = Mejorable -1 Deficiente
Notificación y respuesta de incidentes de seguridad	(Acciones implementadas) (# total de acciones a implementar)	1 = Ideal 0 = Mejorable -1 Deficiente
Gestión y control de cuentas	(Controles implementados) (# total de controles disponibles)	1 = Ideal 0 = Mejorable -1 Deficiente
Gestión de contenido antispam	(Componentes implementados) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Políticas de contraseñas seguras	(Políticas implementadas) (# total de componentes)	1 = Ideal 0 = Mejorable -1 Deficiente
Contexto de uso	(Componentes implementados)	1 = Ideal

	(# total de componentes)	0 = Mejorable -1 Deficiente

5.2.3.3 Definición del Criterio de Decisión para las Métricas

Los parámetros de decisión lo veremos en la tabla 13, establecida en el anterior paso para la evaluación de seguridad.

5.2.3.4 Definición de la Plantilla para el Informe de Seguridad

Para la presentación de problemas de usabilidad se usa una plantilla propuesta en el capítulo que especifica el método de evaluación.

Tabla. 14

Plantilla de Seguridad para la aplicación.

ID del proceso	Número de proceso para identificarse
Nombre del proceso	Nombre del proceso a analiza
Propósito del proceso	Explicación o heurística del atributo evaluado con las diferentes métricas y controles relacionados a cada uno.
Perspectiva MCC	Se indica la perspectiva desde la que se está evaluando
Tipo de nube	Se puede seleccionar si es MCC: Público, Hibrido o Privado.
Modelos de Servicio	Opciones de servicio a ser evaluado: IaaS, PaaS o SaaS.
Escala	Unidades de medida (ej. porcentaje)
Nivel para el cumplimiento	Objetivo con el que el indicador o atributo es considerado como aceptable.

Medición	Registro de los valores obtenidos de acuerdo con el cumplimiento de cada uno de los controles verificados en cada elemento.
Nivel de cumplimiento	Valoración numérica obtenida como resultado de la medición planteada.

5.2.4 Diseño de la evaluación

En este paso, se debe marcar que restricciones se afronta al momento de la evaluación de la aplicación.

Plan de evaluación**,** en el plan de evaluación se aplica el modelo de seguridad para la aplicación valorando el control, proceso o política de cumplimiento o no, por cada uno de los atributos.

5.2.5 Ejecución de la evaluación e informe de seguridad

Después de haber especificados todos los parámetros, requisitos y métricas se comenzará la evaluación de seguridad de la aplicación.

5.2.5.1 Evaluar por atributo

A continuación, se procede a la evaluación por atributo con la ayuda de la plantilla de seguridad de la tabla 13.

Administración de los datos, analizar cada control importante para un correcto programa de MDM (gestión de datos maestros). A continuación, en la tabla 15, se encuentran los controles.

Tabla. 15

Controles de evaluación de la aplicación.

N.º	control	medición	resultado
1	Se puede ejecutar en los diferentes sistemas operativos.	Si = 1, No = 0	1

2	Cuenta con bloqueo remoto.	Si = 1, No = 0	1
3	Tiene opción de borrado.	Si = 1, No = 0	1
4	Previene la transferencia de información no autorizada.	Si = 1, No = 0	0
5	Proporciona desactivación de módulos de comunicación remota.	Si = 1, No = 0	0
6	Inicio de sesión único.	Si = 1, No = 0	1
7	Informa el intento de instalación no autorizada.	Si = 1, No = 0	0*

Después de validar los controles de evaluación de la aplicación se pudo observar que el parámetro de administración de datos no está protegido por lo cual en la siguiente tabla 16, se especificará el nivel que cumple.

Tabla. 16

Evaluación de la administración de datos.

ID del proceso	**001**
Nombre del proceso	Administración de los datos
Propósito del proceso	Se estima el servicio de administración de los dispositivos implementados por el sistema en la nube.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	0

Control de acceso y gestión de identidades, en este paso se intenta tener una buena práctica de control de acceso y actividades. A continuación, en la tabla 17, se observa los controles planteados.

Tabla. 17

Controles de evaluación de la aplicación.

N.º	control	medición	resultado
1	Cuenta con inventarios de dispositivos.	Si = 1, No = 0	1
2	Alerta notificaciones de dispositivos nuevos.	Si = 1, No = 0	1
3	Revisa y deshabilita las cuentas no autorizadas.	Si = 1, No = 0	1
4	Revocación automática del acceso a la nube.	Si = 1, No = 0	0
5	Supervisa cuentas desactivadas en un periodo.	Si = 1, No = 0	1
6	Maneja un perfil por usuario.	Si = 1, No = 0	1
7	Monitoriza cambios en configuraciones o actividades.	Si = 1, No = 0	0
8	Monitoriza las sesiones	Si = 1, No = 0	1
9	Valida configuraciones de los dispositivos	Si = 1, No = 0	1

Como se pudo evidenciar en los controles de acceso y gestión de identidades tiene un gran cumplimiento de parámetros para mantener la seguridad de la información por lo cual en la siguiente tabla 18, se especificará el nivel que cumple.

Tabla. 18

Evaluación del control de acceso y gestión de identidades.

ID del proceso	**002**
Nombre del proceso	Control de acceso y gestión de identidades
Propósito del proceso	Estimación de las características de control de accesos y la actividad de cada cuenta de los usuarios.

Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	1

Seguridad en SLA (Service Level Agreement), se considera las características importantes y que debe acordar un SLA (Es un contrato que describe el nivel de servicio que un cliente espera de su proveedor), para el Cloud computing. A continuación, en la tabla 19, se observa los controles planteados.

Tabla. 19

Controles de seguridad en SLA.

N.º	control	medición	resultado
1	Permite auditorias y certificados de seguridad	Si = 1, No = 0	1
2	La normativa está acorde a la legislación del país del suscriptor del servicio.	Si = 1, No = 0	1
3	Provee información sobre seguridad periódicamente.	Si = 1, No = 0	1
4	Informa acerca del tratamiento de la información del cliente.	Si = 1, No = 0	1
5	Ofrece opciones disponibilidad para dispositivos móviles.	Si = 1, No = 0	1
6	Garantiza la encriptación de la información.	Si = 1, No = 0	1*
7	Informa acerca del uso de los canales de transmisión.	Si = 1, No = 0	1
8	Tiene políticas de seguridad	Si = 1, No = 0	1

Como se puede evidenciar el proceso de seguridad en SLA cumple con la mayoría de los requerimientos planteados por lo cual en la siguiente tabla 20, se especificará el nivel que cumple.

Tabla. 20

Evaluación de la seguridad SLA.

ID del proceso	**003**
Nombre del proceso	Seguridad en SLA
Propósito del proceso	Estimación de las características de los controles de seguridad en SLA
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	8
Nivel de cumplimiento	1

Calidad de encriptación **,** opciones ideales de modos de encriptación en ambiente de la nube, en el siguiente enlace el modo de encriptado que utiliza Google https://cloud.google.com/security/encryption-at-rest/default-encryption?hl=es. A continuación, en la tabla 21, se observa los controles planteados.

Tabla. 21

Controles de encriptación.

N.º	**control**	**medición**	**resultado**
1	Dispone de técnicas de cifrado	Si = 1, No = 0	1
2	Usa controles de claves como KEK90 (Clave de Cifrado de Claves).	Si = 1, No = 0	0

3	Evita utilizar estándares de encriptación antiguas.	Si = 1, No = 0	1
4	Utiliza Secure Sockets Layer.	Si = 1, No = 0	1

Como se puede evidenciar la calidad de encriptación cumple con la mayoría de los controles planteados en la tabla 21, por lo cual en la siguiente tabla 22, se especificará el nivel que cumple.

Tabla. 22

Evaluación de la calidad encriptación.

ID del proceso	**004**
Nombre del proceso	Calidad de encriptación
Propósito del proceso	Se calcula las opciones ideales en cuanto a la encriptación en ambientes.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	3
Nivel de cumplimiento	1

Test de seguridad, se testea las pruebas recomendables que debe realizarse en la aplicación. A continuación, en la tabla 23, se observa los controles planteados.

Tabla. 23

Evaluación de la prueba de Seguridad.

N.º	**control**	**medición**	**resultado**
1	Test de intrusión internos y externo.	Si = 1, No = 0	1

2	Realizan pruebas a terminales móviles.	Si = 1, No = 0	1
3	Verificación periódica de acceso.	Si = 1, No = 0	1
4	Vulnerabilidad en el sistema del cloud	Si = 1, No = 0	1

Como se evidencia en la tabla 23, los procesos de control la mayoría cumple, aunque existen más variedades de verificación de evaluación de pruebas de seguridad por lo cual en la siguiente tabla 24, se especificará el nivel que cumple.

Tabla. 24

Evaluación de la prueba de seguridad.

ID del proceso	**005**
Nombre del proceso	Test de seguridad
Propósito del proceso	Se comprueban las pruebas mínimas que corresponden al ambiente.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	1

Manipulación de los datos del cliente, Además de realizar una prueba de seguridad también toca enfocarse como la información de cada uno de los usuarios son manipulados, modificados, eliminados. A continuación, en la tabla 25, se observa los controles planteados.

Tabla. 25

Controles de manipulación de los datos del cliente.

N.º	control	medición	resultado
1	Tiene herramientas para etiquetar y clasificar la información.	Si = 1, No = 0	1
2	Tiene portabilidad de los datos a otros sistemas.	Si = 1, No = 0	1
3	Asegura que la información no se pueda recuperar después de haberla eliminado.	Si = 1, No = 0	1
4	Dispone de políticas y procedimientos para la eliminación de la información.	Si = 1, No = 0	1

Como se puede evidenciar en la tabla 25, cumple con la mayoría de los controles de la manipulación de los dalos del cliente por lo cual en la siguiente tabla 26, se especificará el nivel que cumple.

Tabla. 26

Evaluación sobre la manipulación de los datos del cliente.

ID del proceso	006
Nombre del proceso	Manipulación de los datos del cliente
Propósito del proceso	Se realiza una ratificación de los controles que se someten a los datos de los usuarios/cliente.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	1

Prevención de ataques, otro punto para mantener la información segura es la prevención ante ataques y se recomendaría que el servicio debe tener en la tabla 27, algunos de los controles.

Tabla. 27

Controles para la prevención ante ataques.

N.º	control	medición	resultado
1	Presenta un certificado de seguridad conocida.	Si = 1, No = 0	1
2	Soporta controles técnicos (registro de dispositivos finales).	Si = 1, No = 0	1
3	Aviso al usuario sobre actividades en tiempo real.	Si = 1, No = 0	1
4	Restringe tráfico no autorizado	Si = 1, No = 0	0
5	Configuración de seguridad para la autenticación.	Si = 1, No = 0	1
6	Previene y denuncia ataques de suplantación de identidad.	Si = 1, No = 0	0
7	Dispone de defensa en profundidad como análisis de la información.	Si = 1, No = 0	0

Como se puede evidenciar en la tabla 27, la prevención de los ataques cumple casi con la mayoría de los controles ya que no siempre la seguridad va a ser un 100% siempre, por eso va a ver métodos para poder acceder a la información por lo cual en la siguiente tabla 28, se especificará el nivel que cumple.

Tabla. 28

Evaluación de la prevención ante ataques.

ID del proceso	007
Nombre del proceso	Prevención de ataques

Propósito del proceso	Se establece las seguridades con las que debe tener un servicio para prevenir ataques.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	0

Seguridad complementaria, la seguridad complementaria se refiere a la protección de la información de manera física. A continuación, en la tabla 29, se observa los controles planteados.

Tabla. 29

Controles de seguridad complementaria.

N.º	control	medición	resultado
1	Autenticación Biométrica (verificación de identidad del usuario).	Si = 1, No = 0	0
2	Métodos de verificación.	Si = 1, No = 0	1
3	Actualizaciones de permisos de acceso.	Si = 1, No = 0	1
4	Sistema de identificación.	Si = 1, No = 0	1

Como se puede evidenciar en la tabla 29, la seguridad implementaría es muy necesaria ya que no solo depende del proveedor sino también del cliente para mantener la información segura. A continuación, en la tabla 30, se ve el nivel de cumplimiento.

Tabla. 30

Evaluación de seguridad complementaria.

ID del proceso	008
Nombre del proceso	Seguridad complementaria
Propósito del proceso	Se consulta sobre seguridades adicionales primordiales respecto a las instalaciones físicas.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	3
Nivel de cumplimiento	1

Notificación y respuesta de incidentes de seguridad, se cuantifica la capacidad del servicio a lo que se refiere el tiempo de respuesta y la notificación de algún incidente. A continuación, en la tabla 31, se observa los controles planteados.

Tabla. 31

Controles de notificación y respuesta de seguridad.

N.º	control	medición	resultado
1	Cuenta con un plan de seguridad.	Si = 1, No = 0	1
2	Dispone de firewall.	Si = 1, No = 0	1
3	Notificación en todos los dispositivos vinculados con el mismo correo.	Si = 1, No = 0	1
4	Cuenta con herramientas de registro de incidentes de aplicaciones.	Si = 1, No = 0	1
5	Tiene plan de recuperación de la información.	Si = 1, No = 0	1
6	Cuenta con una copia de seguridad en la nube.	Si = 1, No = 0	1

7	Brinda respuesta de incidentes automatizadas.	Si = 1, No = 0	1

Como se evidencia en la tabla 31, cumple con la mayoría de los controles para la notificación y respuesta de incidentes para la seguridad de la información por lo cual en la tabla 32, se evalúa el nivel de cumplimiento.

Tabla. 32

Evaluación de la notificación y respuesta a un incidente de seguridad.

ID del proceso	**009**
Nombre del proceso	Notificación y respuesta de incidentes de seguridad
Propósito del proceso	Se valida la precaución que el proveedor puede tomar para evitar ataques a la integridad de los usuarios.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	1

Gestión y control de cuentas de usuario, la gestión y control de cuentas también dependen de los usuarios por ello toca ver que dispositivos utilizan para la utilización de la aplicación. A continuación, en la tabla 33, se observa los controles planteados. En el siguiente enlace se podrá centrar más afondo sobre la activación o desactivación de cuentas, https://support.google.com/a/answer/57919?hl=es

Tabla. 33

Gestión y control de cuentas de usuarios.

N.º	control	medición	resultado
1	Existen un listado de cuentas en los dispositivos.	Si = 1, No = 0	1
2	Maneja un porcentaje de cuentas sin actividad (G Suite Enterprise, obtener el servicio(activar)).	Si = 1, No = 0	1
3	Posee cuentas de servicio para pruebas.	Si = 1, No = 0	0
4	Dispone de autenticación y control de acceso para el administrador.	Si = 1, No = 0	1
5	Dispone de políticas y control de usuarios con privilegios.	Si = 1, No = 0	1
6	Emplea herramientas como SAPM (Gestión de Contraseñas de Cuentas Compartidas).	Si = 1, No = 0	1

Como se evidencia en la tabla 33, el cumplimiento de la gestión y control de cuentas de usuarios cumple con la mayoría de los controles planteados por lo cual a continuación en la tabla 34, se evalúa el nivel de cumplimiento.

Tabla. 34

Evaluación de la gestión y control de cuentas de usuarios.

ID del proceso	010
Nombre del proceso	Gestión y control de cuentas de usuario
Propósito del proceso	Se afirman las medidas de seguridad en cuanto a la revisión de los usuarios y las cuentas de acuerdo con sus perfiles.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público

Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	5
Nivel de cumplimiento	1

Gestión de contenido antispam, es importante evaluar la gestión de contenido antispam ya que la aplicación es fundamental para la gestión de envío y recepción de correo. A continuación, en la tabla 35, se observa los controles planteados. El siguiente enlace se podrá profundizar sobre el control de correo, https://support.google.com/accounts/answer/162744?hl=es-419

Tabla. 35

Control de gestión de contenido antispam.

N.º	control	medición	resultado
1	Monitoreo de los correos electrónicos procesados.	Si = 1, No = 0	1*
2	Realiza un control de correo rechazados.	Si = 1, No = 0	0
3	Envió de información no inapropiada entre correos vinculados de la aplicación.	Si = 1, No = 0	0
4	Controla un porcentaje de falsas identificaciones de spam.	Si = 1, No = 0	1

Como se puede evidenciar en la tabla 35, la gestión de contenido antispam es u punto donde tocaría fortalecer la seguridad de la información de los usuarios ya que hoy en día los atacantes utilizan enlaces enviados al correo electrónico para obtener información por lo cual a continuación en la tabla 36, se evalúa el nivel de cumplimiento sobre la gestión de contenidos antispam.

Tabla. 36

Evaluación de la gestión antispam.

ID del proceso	011
Nombre del proceso	Gestión de contenido antispam
Propósito del proceso	Se admiten las acciones a tomar a razón de la incidencia de contenidos spams de la aplicación utilizada por el usuario.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	2
Nivel de cumplimiento	0

Políticas de contraseña, las políticas de contraseña son importantes para mantener la información segura por lo cual en la tabla 37, se establece controles de evaluación enfocada en la seguridad. En el siguiente enlace se profundiza sobre las políticas, https://support.google.com/a/answer/139399?hl=es

Tabla. 37

Control de políticas de contraseñas.

N.º	control	medición	resultado
1	Políticas de caducidad de contraseñas.	Si = 1, No = 0	1
2	Longitud de contraseñas	Si = 1, No = 0	1
3	Políticas de autenticación en dos pasos	Si = 1, No = 0	1
4	Disponen de documentos sobre todos los requisitos y nivel de confianza para el acceso.	Si = 1, No = 0	1

Como se puede evidenciar en la tabla 37, cumple con todos los controles planteados sobre las políticas de seguridad por lo cual en la tabla 38, se ve el nivel de cumplimiento.

Tabla. 38

Evaluación de políticas de contraseñas.

ID del proceso	**012**
Nombre del proceso	Políticas de contraseña
Propósito del proceso	Se verifica contraseñas seguras para los usuarios para el cumplimiento de las condiciones y ajustarse la seguridad.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	1

Contexto de uso, el contexto de uso nos permite ver si los usuarios detectan al momento de abrir la aplicación en dispositivos diferentes por lo cual en la tabla 39, se establece controles de validación.

Tabla. 39

Controles de contexto de uso.

N.º	**control**	**medición**	**resultado**
1	Detección de biometría para verificación del usuario.	Si = 1, No = 0	0
2	Detecta cambios de direcciones IP.	Si = 1, No = 0	0
3	Tiene avisos de emergencia.	Si = 1, No = 0	0*

Como se puede evidenciar en la tabla 39, el contexto de uso no cumple con los controles establecidos por lo cual se tendrá que mejorar sus vulnerabilidades ya que es importante reforzar estos parámetros por lo cual en la tabla 40, se valida su cumplimiento.

Tabla. 40

Evaluación del contexto de uso.

ID del proceso	**013**
Nombre del proceso	Contexto de uso
Propósito del proceso	Se observa posibles vulnerabilidades en los dispositivos de cada usuario.
Perspectiva MCC	Enfocado al usuario
Tipo de nube	Público
Modelos de Servicio	SaaS
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0

Análisis de resultados de acuerdo con el criterio, después de haber evaluado por atributo cada elemento para mantener la información segura se detalla cómo se podría mejorar la calidad de seguridad de la aplicación. A continuación, en la tabla 41 se detalla todos los atributos evaluados.

Tabla. 41

Resumen de los atributos evaluados.

Atributos	**métrica**	**Umbral**
Administración de datos	(Componentes MDM implementados) (# total de componentes)	0

Control de acceso y gestión de identificación	(Controles implementados) (# total de controles)	1
Seguridad en SLA	(Seguridades implementadas en el SLA) (# total de seguridades SLA)	1
Calidad de encriptación	(Características implementadas) (# total de características)	1
Test de seguridad	(Componentes de prueba implementados) (# total de componentes)	1
Manipulación de la información del usuario	(Seguridades de datos disponibles) (# total de Seguridades)	1
Prevención de ataques	(Seguridades-prevenciones implementadas) (# total de seguridades)	0
Seguridad complementaria	(Seguridades complementarias disponibles) (# total de seguridades)	1
Notificación y respuesta de incidentes de seguridad	(Acciones implementadas) (# total de acciones a implementar)	1
Gestión y control de cuentas	(Controles implementados) (# total de controles disponibles)	1
Gestión de contenido antispam	(Componentes implementados) (# total de componentes)	0
Políticas de contraseñas seguras	(Políticas implementadas) (# total de componentes)	1
Contexto de uso	(Componentes implementados) (# total de componentes)	0

Después de haber evaluado cada uno de los atributos se considera como poder mejorar el método de protección de cada uno de ellos.

El primer lugar, la administración de los datos necesita mejorar en el punto de prevenir en la transferencia de información no autorizada para ello se recomienda

que debe validar el contenido que se está tratando de enviar. Otro punto, es la desactivación de módulos de comunicación remota en este punto se puede optar por verificación de del correo electrónico al momento de desactivar un medio de comunicación ya puede ser como video llamada. También en el intento de instalación de aplicaciones no autorizadas se puede mejorar con verificación de un código pin.

En segundo lugar, el control de acceso y gestión de identificación, en el punto de revocación automática de acceso a la nube en este punto para mejorar su rendimiento se podría poner un límite se acceso a los datos alojado en la nube o permitir que lo descarguen en un tiempo determinado y así mantener la información segura. Otro punto, es el monitoreo de cambio de configuración o actividad para mejorar este punto se podría hacer que cada vez que se cambie una configure se verifique por medio de correo electrónico detallando que cambios se realizó o que actividades hizo.

En tercer lugar, la seguridad en SLA en este punto cumplió con todos los controles detallados, aunque también toca recalcar que no solo depende de los proveedores y los usuarios, sino que le medio de comunicación sea segura.

En cuarto lugar, la calidad de encriptación en el transcurso de los años se ha ido mejorando, pero nunca se podrá proteger la información a un nivel del 100% ya que siempre hay mecanismo para accederla, pero toca complicarle para la obtención.

En quinto lugar, la prueba de seguridad cumple con los controles planteados, pero hay que mejorarles para mantener segura la información.

En sexto lugar, la manipulación de los datos del cliente cumple con los controles planteados, pero siempre tienen que estar en actualizaciones de mejora.

En séptimo lugar, la prevención de ataques, en el punto de restricción de tráfico no autorizado depende de todos los involucrados por lo cual eso sería la mejor manera de prevenir un ataque. Por otro lado, la denuncia y defensa de suplantación de

identidad es siempre estar en constante verificaciones de la información para mantener un adecuado análisis de la información.

En octavo lugar, la seguridad complementaria se refiere que hay mecanismo que depende de manera física mas no de tecnología informática por lo cual una autenticación biométrica ayudaría a reducir un nivel aceptable de ataque a la información.

En noveno lugar, la notificación y respuesta de incidentes de seguridad para mantener los datos de manera segura tendría que haber notificaciones de cada cosa que se realice de forma periódica.

En décimo lugar, la gestión y control de cuentas de usuarios en este punto se tendría que prevenir que se creen cuentas diferentes para el mismo usuario o que tenga un límite de creación.

En undécimo lugar, la gestión de contenido antispam este punto se refiere a que los usuarios son los únicos responsables para abrir cualquier tipo de enlace que se le envié por correo.

En duodécimo lugar, las políticas de contraseñas sean ido fortaleciendo en el transcurso que la aplicación a realiza sus actualizaciones por ello se recomienda a cada usuario actualizar en determinado tiempo sus contraseñas.

En decimotercero lugar, el contexto de uso, en este punto solo depende de las personas que utilizar la aplicación de forma adecuada.

6 Conclusiones

Las aplicaciones alojadas en la nube han permitido que las personas y organizaciones puedan utilizar los recursos que disponen para tener mejora en el rendimiento en cuestión de almacenamiento, procesamiento y modificación de sus datos por lo que es primordial realizar los procesos adecuados de seguridad para mantener de forma segura y confiable los datos.

Existen variedades de métodos para mantener segura la información por la razón que los usuarios y organizaciones almacenan bastante información en sus dispositivos. Por ello, surge la necesidad de usar aplicaciones que se alojan en la nube. Además, las normativas ISO establecen variedades de mecanismos de seguridad para mantener segura la información de los usuarios y organizaciones.

Hoy en la actualidad las aplicaciones que se encuentra en la nube con respecto al estado de seguridad se pueden decir que la mayoría de las aplicaciones cuentas con un mecanismo de seguridad, pero esto no quiere decir que están 100% segura. Ya que todos los involucrados en la manipulación de la información tienen un papel importante en su uso. Por ejemplo, los usuarios son los responsables de que información suben a la nube por medio de las aplicaciones y por parte del proveedor tiene que enfocarse en mantener segura y que la información no sea extraída. Finalmente, se podría también profundizar en los medios de transmisión por donde se transmite la información.

Dentro del análisis de la encuesta de google se puede observar que la mayoría de las personas optarían por utilizar estas aplicaciones que se alojan en la nube ya que les permite almacenar variedad de información. Por ello, la seguridad debe ser robusta para que brinde confianza a los usuarios y organizaciones.

Con la aplicación del modelo de seguridad en el aplicativo elegido se evidencia que existe una seguridad robusta, pero en ciertos puntos evaluados tiene vulnerabilidades las cuales podrían mejorar ya que, la tecnología ha evolucionado

extraordinariamente. Por ello, los usuario y organizaciones deben cumplir con las normativas de los proveedores para tener un excelente servicio.

Las normativas ISO nos proporciona información de cómo debemos proteger los datos y como crear modelos de seguridad permitiendo así reducir costo antes que se implemente. Por otro lado, permiten que los proveedores estén siempre en constante actualizaciones en lo que se refiere a mejorar los mecanismos de seguridad y así brindar un excelente servicio, brindando confianza a sus usuarios y organizaciones que optan por utilizar estos servicios.

7 Recomendaciones

Para finalizar, se recomienda a todos los usuarios y organizaciones que no solo depende de los proveedores de servicio de la seguridad de la información, sino que todos son los involucrados en la seguridad de los datos y así prevenir la sustracción. Por tal motivo, los controles y métricas de seguridad deben implementarse según lo requerido ya que si hay seguridad robusta esto permite que los atacantes no puedan adquirir la información fácilmente.

En base a los resultados de la encuesta de google y aporte bibliográfico de esta tesis, se recomienda el uso de las aplicaciones en la nube con debida responsabilidad ya que cada uno es responsable de lo que se sube, porque el uso de las aplicaciones nos permite un mejor rendimiento de los dispositivos y ahorro de almacenamiento.

De esta forma, al momento de adquirir el servicio de los proveedores los usuarios y organizaciones deben tener los requisitos que necesitan para que los proveedores puedan tener la facilidad al momento de proponer una solución adecuada. Por otro lado, los usuarios y organizaciones son parte de la responsabilidad de mantener segura la información.

En cuestión de costos se recomienda a los usuarios y organizaciones faciliten a los proveedores con las plantillas de los elementos que quieren asegurar para evitar gastos innecesarios y ver que normativa ISO le favorece.

La medida de protección de los proveedores también es asegurar el canal de transmisión por el cual se transfiere la información como usar protocolos seguros y así tener una seguridad robusta.

Se recomienda a las demás personas profundicen en el tema de seguridad en lo que se refiere a la protección de los dispositivos ya que si existe mayor protección en los dispositivos ayudaría que los datos no se puedan sustraer fácilmente.

8 Referencias

¿Cómo puede proteger sus datos en la nube? – Revista IT NOW. (2019, mayo 9). Recuperado de https://revistaitnow.com/como-puede-proteger-sus-datos-en-la-nube/

¿Cómo protege Google mi información? (s. f.). Recuperado 20 de mayo de 2020, de https://www.sistel.es/seguridad-gsuite-como-protege-google-mis-datos

¿Qué es SaaS? Software como servicio. (s. f.). Recuperado 24 de abril de 2020, de https://azure.microsoft.com/es-es/overview/what-is-saas/

1&1 IONOS España S.L.U. (2020, abril 20). Qué es SaaS. Recuperado de https://www.ionos.es/digitalguide/servidores/know-how/que-es-saas/

10 procedimientos para mantener la seguridad de IoT en la nube. (s. f.). Recuperado 20 de mayo de 2020, de https://ausum.cloud/es/blog/iot/2019/10-procedimientos-para-mantener-la-seguridad-de-iot-en-la-nube

Activar o desactivar Gmail en cuentas de usuario - Ayuda de Administrador de G Suite. (s. f.). Recuperado 16 de mayo de 2020, de https://support.google.com/a/answer/57919?hl=es

Alexander. (2020). Ecuador Patente N.º 1.

Algoritmo de Cifrado. (11 de 06 de 2015). Obtenido de Algoritmo de Cifrado: http://media.espora.org/mgoblin_media/media_entries/1661/presentacion.pdf

Álvarez vañó, j. M. (2018). Modelo comparativo de plataformas cloud y evaluación de microsoft azure, google app engine y amazonec2 (doctoral dissertation).

Amazon web services. (2020). Conformidad con iso/iec 27018:2019. Obtenido de aws: https://aws.amazon.com/es/compliance/iso-27018-faqs/

Androidsis. (12 de 11 de 2013). Obtenido de Androidsis: https://www.androidsis.com/consigue-50gb-de-espacio-de-almacenamiento-en-la-nube-gratis-con-mega/

Arcila Bonfante, L. E. (2019). Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información.

Arquitecturas de TI. (19 de 06 de 2014). Obtenido de Arquitecturas de TI: http://arquiticarlosaraujo.blogspot.com/2014/06/servicios-los-servicios-se-constituyen.html

Bautista Grisales, V., & Robayo Bautista, E. C. (2019). Modelo ISO/IEC 25010 en el proceso de evaluación de la calidad del software en la empresa obras civiles de Bogotá en el área de tecnología de la información y comunicación.

Blanquer, M. A. (2020, abril 14). Tipos de Cloud Computing. Recuperado de https://openwebinars.net/blog/tipos-de-cloud-computing/

Byte Ti, R. (2019, diciembre 19). El estado de la nube: cinco tendencias de la seguridad empresarial en 2019. Recuperado de https://revistabyte.es/tendencias-byte-ti/el-estado-de-la-nube-seguridad/

Cómo obtener un resumen de los datos de tu Cuenta de Google - Ayuda de Cuenta de Google. (s. f.). Recuperado 16 de mayo de 2020, de https://support.google.com/accounts/answer/162744?hl=es-419

Condori, J. J. M. (2012). Ventajas y desventajas de cloud computing. *Revista de información, tecnología y sociedad*, *7*.

Consejos de seguridad para soluciones en la nube. (2018, marzo 14). Recuperado de https://www.tecon.es/consejos-de-seguridad-para-soluciones-en-la-nube/

Content, R. R. (2019, octubre 29). SaaS: qué es y cómo funciona el software como servicio ¡Ingresa! Recuperado de https://rockcontent.com/es/blog/saas/

Cumplimiento del ISO 27001 |. (s. f.). Recuperado 16 de mayo de 2020, de https://cloud.google.com/security/compliance/iso-27001?hl=es

Cloud Computing Services |. (s. f.). Recuperado 16 de mayo de 2020, de https://cloud.google.com/?&utm_source=google&utm_medium=cpc&utm_campaign=latam-LATAM-all-es-dr-bkws-all-all-trial-e-dr-1008075-LUAC0010197&utm_content=text-ad-none-none-DEV_c-CRE_382263535346-ADGP_BKWS+%7C+Multi+%7E+Google+Cloud+Platform-KWID_43700047166266662-kwd-301173107504-userloc_9069516&utm_term=KW_google%20cloud%20platform-ST_Google+Cloud+Platform&gclid=Cj0KCQjw2PP1BRCiARIsAEqv-pSnkzTxHDNH-cNanhs0a-hCWRS4D0Iy5FjjEXPTwBIT_c1_UYOy9sEaAtxhEALw_wcB&gclsrc=aw.ds

de Parga, D. C. J. (2011). *Cloud computing: retos y oportunidades*. Fundación Ideas.

Diferencias entre PaaS pública y privada. (s. f.). Recuperado 22 de abril de 2020, de https://bbvaopen4u.com/es/actualidad/diferencias-entre-paas-publica-y-privada

Dropbox. (SN de SN de SN). Obtenido de Dropbox: https://www.dropbox.com/es/

EditorR. (2017, marzo 24). ISO 27018 La primera normativa para la privacidad en la nube. Recuperado de https://www.isotools.org/2017/03/23/iso-27018-la-primera-normativa-la-privacidad-la-nube/

editorE. (2015, abril 10). ISO 27001: Seguridad informática y seguridad de la información. Recuperado de https://www.isotools.org/2015/01/05/iso-27001-seguridad-informatica-seguridad-informacion/

Encriptado en reposo en Google Cloud Platform | Documentación. (s. f.). Recuperado 16 de mayo de 2020, de https://cloud.google.com/security/encryption-at-rest/default-encryption?hl=es

E&N Estrategia y Negocio. (15 de 06 de 2019). Obtenido de E&N Estrategia y Negocio: https://www.estrategiaynegocios.net/lasclavesdeldia/1293634-330/google-apuesta-us2600-millones-por-la-nube

Gestionar la configuración de las contraseñas de los usuarios - Ayuda de Administrador de G Suite. (s. f.). Recuperado 16 de mayo de 2020, de https://support.google.com/a/answer/139399?hl=es

Gestiona software en línea 2414. (SN de SN de SN). Obtenido de Gestiona software en línea 2414: https://sites.google.com/site/gestionasoftwareenlinea2414/conclusion-de-ivan/tipos-de-nube

GlobalLogic Latinoamérica. (2013, febrero 22). Seguridad en el modelo IaaS | GlobalLogic Latinoamérica. Recuperado de https://www.globallogic.com/latam/blog/seguridad-en-el-modelo-iaas/

Guerrero Alemán, A. C., Mena Maldonado, E. K., & Bernal Carrillo, I. (2010). Implementación de un prototipo de Cloud Computing de modelo privado para ofrecer Infraestructura como Servicio (IaaS).

Habilitar cookies y SSL en el navegador - Ayuda de AdSense. (s. f.). Recuperado 16 de mayo de 2020, de https://support.google.com/adsense/answer/35730?hl=es

Iso, N. (2017, noviembre 24). ISO / IEC 27018 2014 Requisitos para la protección de la información de identificación personal. Recuperado de https://www.normas-iso.com/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal/amp/

Iso, N. (2019, noviembre 22). ISO 27001 Seguridad de la Información. Recuperado de https://www.normas-iso.com/iso-27001/amp/

HERNÁNDEZ, L. E. G. (2019). Optimización multiobjetivo de un sistema de almacenamiento de datos en la multi-nube con un esquema de compartición de secretos basado en RRNS.

IESOFT technologics. (SN de SN de SN). Obtenido de IESOFT technologics: https://iesoftfzc.com/services/enterprise/cloud-based-applications/

José María Gonzáles Blog de Virtualización & Cloud Computing en español. (24 de 04 de 2018). Obtenido de José María Gonzáles Blog de Virtualización & Cloud Computing en español: https://www.josemariagonzalez.es/amazon-web-services-aws/la-plataforma-de-computacion-en-la-nube-de-amazon-aws.html

La Vanguardia. (11 de 04 de 2017). Obtenido de La Vanguardia: https://www.lavanguardia.com/muyfan/20170411/421621106380/lista-spotify-novio-romper.html

MC PRO. (12 de 07 de 2018). Obtenido de MC PRO: https://www.muycomputerpro.com/2018/07/12/que-es-nube-hibrida

MCPRO. (14 de 11 de 2012). Obtenido de MCPRO: https://www.muycomputerpro.com/2012/11/14/dropbox-supera-100-millones-usuarios

Microsoft Azure. (s. f.). Recuperado 22 de abril de 2020, de https://azure.microsoft.com/es-es/overview/what-is-paas/

Microsoft Azure. (SN de SN de 2020). Obtenido de Microsoft Azure: https://azure.microsoft.com/es-es/overview/what-is-iaas/

Moreira Zambrano, C. A. (2015). Mecanismo de alta disponibilidad y virtualización con soluciones de bajo costo usando el modelo infraestructura como servicio (IaaS). Caso de estudio ESPAM MFL.

P. (s. f.). Manual para implementar la seguridad de la información, según la ISO 27001. Recuperado 7 de mayo de 2020, de https://www.riesgoscero.com/academia/especiales/manual-para-implementar-la-seguridad-de-la-informacion-segun-la-iso-27001

PaaS (Platform-as-a-Service). (2020, marzo 9). Recuperado de https://www.ibm.com/cloud/learn/paas

Plataforma como servicio. (s. f.). Recuperado 22 de abril de 2020, de https://www.ticportal.es/paas-plataforma-servicio

Plataforma. (17 de 03 de 2020). Captura de pantalla del navegador. Conocoto, Pichincha, Ecuador.

PowerData, G. (s. f.). MDM (Máster Data Management). ¿Qué es y cómo debes implementarlo en tu empresa? Recuperado 16 de mayo de 2020, de https://www.powerdata.es/mdm

Protección de la información de Microsoft – Seguridad de Microsoft. (s. f.). Recuperado 20 de mayo de 2020, de https://www.microsoft.com/es-es/security/business/information-protection#office-SecondaryMessaging-fw5353f

ONCLOUD soluciones en la nube. (03 de 03 de 2019). Obtenido de ONCLOUD soluciones en la nube: https://on-cloud.blog/2019/03/03/on-cloud-servicios-en-la-nube/

OSI Oficina de Seguridad de Internauta. (10 de 07 de 2019). Obtenido de OSI Oficina de Seguridad de Internauta: https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad

Ramos Ali, J. R. (2012). Infraestructura como Servicio (IaaS). *Revista de Información, Tecnología y Sociedad*, 106.

Ramos Palacios, D. E. (2016). *Diseño de un modelo de evaluación de la calidad de productos de software, basado en métricas externas y usabilidad aplicado a un caso de estudio* (Master's thesis, Quito, 2016.).

Revista Gerencia - Seguridad en la nube: El próximo desafío del cloud computing. (2020, abril 26). Recuperado de http://emb.cl/gerencia/articulo.mvc?xid=597

Redondo, D. G. (2015, noviembre 30). ISO 27018: Cloud Computing. Recuperado de https://blogs.deusto.es/master-informatica/iso-27018-cloud-computing/

Rgpd, C. (2020, febrero 26). ¿Cómo puedes proteger tus datos en la nube? Recuperado de https://clickdatos.es/como-puedes-proteger-tus-datos-en-la-nube/

Rguez, I. H. (2017, mayo 16). El Cifrado de Seguridad en la Cloud Computing. Recuperado de http://www.nube.villanett.com/2016/01/14/cifrado-en-la-cloud-computing/

Rouse, M. (2019, November 27). Platform as a Service (PaaS). Recuperado de https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

Seguridad en la nube: desafíos y soluciones. (2020, mayo 15). Recuperado de https://www.ionos.es/digitalguide/servidores/seguridad/seguridad-en-la-nube-desafios-y-soluciones/

Seguridad y privacidad del Cloud Computing. (2019, mayo 9). Recuperado de https://www.programacionintegral.es/actualidad/nos-interesa/item/737-seguridad-y-privacidad-del-cloud-computing

Tozzi, C. (2019, noviembre 25). Opciones de IaaS vs. PaaS en AWS, Azure y Google Cloud Platform. Recuperado de https://searchdatacenter.techtarget.com/es/consejo/Opciones-de-IaaS-vs-PaaS-en-AWS-Azure-y-Google-Cloud-Platform

Trusted Cloud Infrastructure (IaaS) |. (s. f.). Recuperado 16 de mayo de 2020, de https://cloud.google.com/security/infrastructure

tic. PORTAL. (03 de 03 de 2020). Obtenido de tic. PORTAL: https://www.ticportal.es/temas/cloud-computing/microsoft-cloud

ANEXOS

Test de Autoevaluación de Google

Que tanto sabes de los aplicativos que utilizas

Dirección de correo electrónico*

Tu dirección de correo electrónico

¿Cuánto Conoces del Cloud Computing?

- ◯ 10% - 30%
- ◯ 40% - 60%
- ◯ 70% - 100%

¿De los siguientes aplicativos cual utilizas?

- ☐ Google
- ☐ Dropbox
- ☐ Spotify
- ☐ Netflix
- ☐ Otros

¿Recomendarías un aplicativo que utilices a un amigo, familiar o conocido para que ellos utilicen y guardar su información en la nube?

- ◯ Si
- ◯ No
- ◯ Tal vez

¿Utilizas el servicio de correo para enviar tu información?

◯ Si

◯ No

¿Cuántas de tus aplicaciones utilizas para guardar tu información?

◯ 1 – 3

◯ 4 – 6

Te gustaría abrir, ver, ¿compartir desde cualquier dispositivo tu información de forma segura?

◯ Si

◯ No