CONSTRUCCION DE UNA GUIA PARA IMPLEMENTAR CONTROLES DE SEGURIDAD AL ALMACENAR DATOS SENSIBLES EN CLOUD DE EMPRESAS DE MENSAJERIA DE COLOMBIA

CESAR AUGUSTO CASTAÑEDA SANDOVAL

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2018

CONSTRUCCION DE UNA GUIA PARA IMPLEMENTAR CONTROLES DE SEGURIDAD AL ALMACENAR DATOS SENSIBLES EN CLOUD DE EMPRESAS DE MENSAJERIA DE COLOMBIA

CESAR AUGUSTO CASTAÑEDA SANDOVAL

Trabajo de grado para optar al título de

Magíster en Tecnologías de la Información y la Comunicación

Asesor

Hubert Demercado

Magister en Gerencia de Sistemas y Seguridad

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2018

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) _ Cesar A Castañeda S _____

Cesar Augusto Castañeda Sandoval

Firmado digitalmente por Cesar Augusto Castañeda Sandoval
Fecha: 2018.10.03 21:03:00 -05'00'

Medellín, Agosto de 2018

Tabla de contenido

GLOSARIO

Datos: Un dato es una representación simbólica de un atributo o variable cuantitativa o cualitativa.

Dato personal: información que permite identificar a una persona.

Dato Sensible: información que puede afectar la intimidad del titular

Privacidad: información que debe mantenerse confidencial y privada.

Integridad: la información debe permanecer exacta como fue ingresada.

disponibilidad: la información puede ser accedida por quien tenga los permisos.

Amenaza: posible ocurrencia de un hecho.

Vulnerabilidad: falla o deficiencia en seguridad que puede ser aprovechada.

Riesgo: Probabilidad de que ocurra un hecho.

SECaaS: Seguridad como servicio.

Firewall: Parte de un sistema que impide accesos no autorizados y permite comunicaciones autorizadas.

Responsable: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Encargado: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Cifrado: procedimiento que utiliza un algoritmo con una clave (clave de cifrado) para transformar un mensaje.

QoS: rendimiento promedio de la calidad del servicio de una red.

DDoS: ataque de denegación de servicio, causa que un servicio o recurso sea inaccesible a los usuarios.

SSL: Protocolo criptográfico que proporciona comunicaciones seguras

VPN: implementación de software o hardware en una red de computadoras para realizar una extensión segura de la red de área local sobre internet.

CCM: (Cloud Controls Matrix) matriz de controles de referencia para la seguridad Cloud, emitido por Cloud Security Alliance España, la cual busca la adopción de servicios cloud con seguridad efectiva.

RESUMEN

La protección de los datos (información) históricamente ha sido un reto para los especialistas de seguridad de la información y sigue intensificándose con la aparición de nuevas tecnologías, como el internet de las cosas (IOT) y servicios tecnológicos albergados en la nube. Colombia no escapa a los riesgos (privacidad y confidencialidad). En este sentido ya cuenta con la legislación que aborda dicha preocupación a través de La ley 1581 de 2012. Esta incluye aspectos relevantes en tópicos sobre la protección de información sensible, en algunos casos administrada por empresas de mensajería en territorio colombiano, las cuales se encuentran reglamentadas según la ley postal colombiana.(Colombia. Congreso de la República, 2009)

Esta propuesta consiste en crear una guía de aspectos relevantes a ser observados (diligencia debida) al momento de almacenar información sensible en proveedores de la nube de datos fuera del territorio nacional. Entre los enfoques que pensamos explorar se encuentran los siguientes: definición del conjunto de controles de seguridad mínimos, los cuales permitan mitigar las amenazas contra la disponibilidad, confidencialidad e integridad de dicha información, selección de al menos un proveedor en la nube que cuente con las medidas de seguridad definidas a través de este estudio y finalmente un pareo de requisitos contra los controles que permita evidenciar con el cumplimiento de la ley 1581 de 2012.

PALABRAS CLAVE: Almacenamiento; Nube; Seguridad; SECaaS; datos personales

ABSTRACT

Data protection (information) has historically been a challenge for information security specialists and continues to intensify with the emergence of new technologies, such as the Internet of Things (IOT) and cloud-based technology services. Colombia does not escape the risks (privacy and confidentiality). In this sense already has the legislation that addresses such concern through Law 1581 of 2012. This includes relevant aspects in topics on the protection of sensitive information, in some cases managed by courier companies in Colombian territory, which are Regulated according to Colombian postal law (Colombia, Congress of the Republic, 2009)

This proposal consists of creating a guide of relevant aspects to be observed (due diligence) when storing sensitive information in suppliers of the data cloud outside the national territory. Among the approaches we intend to explore are the following: definition of the set of minimum security controls, which will mitigate threats against availability, confidentiality and integrity of such information, selection of at least one cloud provider that has the Security measures defined through this study and finally a pairing of requirements against the controls that allows evidence with compliance with law 1581 of 2012

KEY WORDS: Storage; cloud; security; SECaaS; personal data

1 INTRODUCCIÓN

El almacenamiento de información en la nube es un servicio que debe ser analizado desde diferentes puntos de vista, especialmente desde el tecnológico y el legal, enfocándose en principios tan fundamentales como la privacidad, la integridad y la disponibilidad, más aún cuando en Colombia existen leyes que reglamentan la manera como deben ser tratados los datos personales.

En esta guía se ofrecen herramientas que darán cubrimiento desde el ámbito tecnológico y legal para determinar con un poco más de certeza cual proveedor de servicios en la nube se encuentra mas alineado a la normatividad colombiana de protección de datos (Ley 1581 de 2012) en cuanto a sus implementaciones, responsabilidades y obligaciones.

Tomaran relevancia las responsabilidades del prestador de servicios en la nube como del tomador del servicio, a fin de encontrar la fórmula adecuada en cuanto a infraestructura, seguridad, procedimientos, contratos y certificaciones, para el funcionamiento seguro y adecuado que debe cumplir con los requerimientos de protección de datos vigentes en Colombia y en el mundo.

2 PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

El modelo actual de almacenamiento en la nube contiene una gran cantidad de terabytes que hacen difícil la labor de control y vigilancia, a su vez se intensifica dado que no se encuentra dentro de las premisas de la empresa proteger los datos sensibles allí almacenados. Quedando expuesto el problema de la privacidad y la estrategia que se empleara para mitigar ingresos no autorizados a esta.

Legislación vigente: La ley 1581 de 2012 de Colombia por medio de la cual se dictan medidas para la protección de datos personales y sensibles, complementa la regulación vigente en cuanto al habeas data y hace especial relación al tratamiento que deben tener los datos sensibles por parte de quienes realizan su captura y tratamiento en el sector servicios en Colombia.

A nivel mundial, alrededor de 60 países cuentan con reglamentación vigente para formalizar la protección de datos. (Agencia Española de Protección de Datos, n.d.)

"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales." (Colombia. Congreso de la República, 2012)

"Los riesgos pueden ser de dos tipos. El primero y principal es el que afecta a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Pero tampoco hay que descuidar los riesgos que puede afrontar una organización por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descuidada o errática, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces." (AEPD, 2014a)

Riesgos Identificados

"Entre estos riesgos podemos incluir los derivados de una percepción de falta de respeto a la privacidad o de cumplimiento de las expectativas de privacidad de las personas, lo que puede motivar una baja utilización de los productos o servicios ofertados; la aparición o el incremento de los costes de rediseño del sistema e, incluso, la retirada del mismo; la falta de apoyo de actores clave para la viabilidad del proyecto; la pérdida de reputación e imagen pública y, por supuesto, la posibilidad de acciones de investigación y, en su caso, sancionadoras por parte de la autoridad de protección de datos competente."(AEPD, 2014b)

2.2 Justificación

El almacenamiento de información personal o sensible captada en los establecimientos de comercio a los clientes en Colombia es reglamentado por la Ley 1581 de 2012. Las implementaciones de almacenamiento de la información deben cumplir con requerimientos que garanticen la privacidad de la misma por medio de procedimientos que impidan el acceso no autorizado y técnicas que disminuyan la posibilidad de pérdida, con fuertes acuerdos de servicio respaldados mediante contrato con el proveedor, demostrando que existe la voluntad de adherencia a la ley actual.(Susana Navas Navarro, 2015)

El almacenamiento de información en entornos de nube (De La Hoz Freyle, Carrillo Rincón, & Gómez Flórez, 2014) requiere consideraciones en materia de seguridad y de privacidad de la información, ya que los datos allí contenidos deben conservar sus principios fundamentales. Es responsabilidad tanto del prestador de servicios en la nube como del administrador que los contrata, de brindar todos los mecanismos necesarios en cuanto a infraestructura, seguridad, procedimientos, contratos y certificaciones, para encontrar la fórmula para el funcionamiento seguro y adecuado a fin de llegar a un entorno que cumpla con los criterios requeridos para la protección de la información sensible allí almacenada.(Martínez Martínez, 2012)

"Desde el punto de vista de la innovación y la competitividad, la privacidad y la seguridad deben ser detonadores de aquéllas, generando la confianza necesaria. Se trata, por tanto, de que la regulación en materia de privacidad y la seguridad permitan el desarrollo de la tecnología, sin que la innovación y la competitividad supongan renunciar a derechos y, en particular, el derecho fundamental a la protección de datos personales." (Casasola Robles Mario, Maqueo Ramírez María Solange, Molina Rodríguez Marlon, Moreno González Jimena, & Recio Gayo Miguel, 2014)

En la misma medida que se vayan incorporando procedimientos y soluciones enfocadas en fortalecer la línea de defensa entre la nube, el exterior a esta y otros usuarios del mismo servicio, los usuarios serán beneficiados por los cambios e incrementen los niveles de confianza en sus proveedores.

El panorama de seguridad que se provee bajo los diferentes esquemas debe incluir al proveedor del servicio como a los administradores internos del cliente, en donde se evidencie un panorama de seguridad que provea controles eficientes y socios de negocios comprometidos con el valor de la información sensible que se está almacenando.

A raíz de los riesgos detectados en sistemas de almacenamiento en la nube (Areitio, 2011) y en general para todos sus servicios, se pueden encontrar diferentes opciones para proveer una apropiada solución de seguridad como servicio que varía dependiendo del proveedor de servicios en la nube, los cuales van desde llaves públicas y privadas, nubes hibridas, soluciones propias, contratada con el proveedor o seguridad como servicio, responsabilidades como encargados de tratamiento, acuerdos de niveles de servicio, combinación de certificaciones como CobIt, ISO 27018, PCI DSS, ISO 27001.

Para solucionar la situación planteada anteriormente (Tobergte & Curtis, 2013), se pretende analizar las implementaciones de SECaaS de tres proveedores pioneros en el mercado, y de esta forma poder seleccionar el proveedor más apto.

Este documento va dirigido a las personas encargadas y responsables del manejo y protección de los datos sensibles, quienes deben velar por la protección de estos y mantener la privacidad, confidencialidad e integridad.

3 OBJETIVOS Y ALCANCE

3.1 Objetivo General.

Diseñar una guía de implementación de seguridad como servicio en cloud para almacenamiento de datos sensibles de las empresas de mensajería, según el proveedor más adecuado de acuerdo con la normatividad colombiana de protección de datos.

3.2 Objetivos Específicos

1. Identificar las necesidades de seguridad para almacenamiento de información en la nube de las empresas de mensajería según la normatividad vigente en Colombia en el año 2018 y la exposición de riesgos inherentes a los servicios prestados.
2. Comparar los tres grandes proveedores a nivel mundial de SECaaS, disponibles en el mercado.
3. Seleccionar según los criterios de la normatividad colombiana de tratamientos de datos sensibles el proveedor de nube más adecuado.
4. Documentar la guía para una correcta ejecución de la seguridad como servicio en el proveedor más adecuado.

3.3 Alcance

Diseñar una guía para implementar controles de seguridad al almacenar datos sensibles en cloud de empresas de mensajería de Colombia, la cual permita determinar el proveedor más adecuado según los requerimientos de la ley de protección de datos 1581 de 2012 en Colombia.

4 MARCO REFERENCIAL

4.1 Marco contextual

Este proyecto pretende evaluar las implementaciones de seguridad como servicio de los tres grandes proveedores de tecnología en la nube a nivel mundial: Amazon, Azure y Google a fin de poder determinar cuál de estos se ajusta de mejor manera a la ley de protección de datos en Colombia.

La seguridad de la nuble depende de varios actores que intervienen de forma activa para proporcionar la mejor experiencia a los usuarios, para lograr esto se deben adoptar medidas de prevención al tener información sensible para proteger, es determinante considerar seriamente el componente de seguridad ofrecido por los proveedores y los componentes de este, asegurándose de obtener siempre el mejor beneficio, enfocado en la minimización de los riesgos. (Casasola Robles Mario et al., 2014)

"Recomiendo que se negocie para que el contrato incluya una cláusula que obligue al servicio a cumplir ciertas normas específicas de seguridad internacionales, y/o las normas de seguridad propias del cliente. El contrato debe explicitar la responsabilidad (y sus límites) del proveedor de servicios en caso de pérdida de datos o de un fallo de seguridad. Los clientes deben negarse a firmar un contrato que exima al servicio de la nube de toda responsabilidad por pérdida de datos o violación de la seguridad." (Oppenheim, 2012)

El desarrollo de este proyecto está enfocado en el sector de empresas de mensajería de Colombia, teniendo en cuenta la normatividad vigente al año 2018 sobre el tratamiento de información sensible, la cual se encuentra reglamentada en la ley 1581 de 2012.

La matriz de controles en cloud (CCM de Cloud Security Alliance) proporciona los principios de seguridad fundamentales para orientar a los proveedores de la nube y para ayudar a los usuarios de la nube a evaluar el riesgo general de seguridad de un proveedor de la nube, presentando un marco de control que permite una comprensión detallada de los conceptos y principios de seguridad mediante 13 dominios. Los fundamentos de la matriz se apoyan con otros estándares de seguridad, regulaciones y marcos de control como ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum y NERC CIP. Brindando herramientas a las organizaciones para entender la estructura, los detalles y la claridad necesaria en relación con la seguridad de la información adaptada a la nube. Su objetivo es fortalecer los entornos existentes de controles de seguridad de la información, reducir e identificar amenazas de seguridad y vulnerabilidades en la nube y proporcionar seguridad y administración de riesgo operacional.

4.2 Marco conceptual

"La computación en nube ha sido definido por el NIST como un modelo que permite un cómodo acceso, en demanda de la red a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo de rapidez esfuerzo de gestión o interacción proveedor de la nube. La computación en nube puede ser considerado como un nuevo paradigma de computación en la medida que permite la utilización de una infraestructura de computación en uno o más niveles de abstracción, como un servicio bajo demanda a su disposición a través de Internet u otra red informática. Debido a las implicaciones para una mayor flexibilidad y disponibilidad a un costo menor, la computación en nube es un tema que ha estado recibiendo una gran cantidad de atención." (Jansen & Grance, 2011)

Los modelos de despliegue hacen referencia al tipo de nube que se van a usar para desplegar los servicios, los cuales pueden ser PRIVADA en donde los recursos proporcionados son exclusivamente para uso de quien los contrata, PUBLICA donde los recursos utilizados son propiedad de un gran distribuidor y la información se coloca allí con acuerdos públicos, en la nube COMUNITARIA los recursos se comparten con comunidades que por lo general buscan el mismo fin, HIBRIDA es un conjunto seleccionado de los modelos anteriores definido por necesidades o fines específicos. (Areitio, 2011)

Por otro lado, los modelos de servicio tienen que ver con el tipo de infraestructura o plataforma en donde deseamos implementar los servicios, así que podemos encontrar:

SaaS: Software como Servicio, consiste en proveer al usuario final una sencilla plataforma para que use los servicios alojados en el proveedor.

PaaS: Plataforma como Servicio, proporciona al consumidor recursos con capacidad para desplegar en los servicios que prestara y de las cuales tiene el control.

IaaS: Infraestructura como Servicio, el consumidor cuenta con recursos de procesamiento, almacenamiento y puede proveer más recursos para poder configurar múltiples plataformas de servicios.

Los servicios de almacenamiento los podremos encontrar con la opción de SECaaS, la cual es un modelo de servicios de seguridad en la nube que se provee por suscripción y se integra a la infraestructura, sin que se requieran elementos de hardware.

La normatividad colombiana conceptualiza y da claridad respecto a los términos de la norma de protección de datos que están inmersos en este proyecto. (Colombia. Congreso de la República, 2012)

La transaccionalidad de los datos es una cuestión de suma importancia para las relaciones entre los diferentes países en el contexto de la economía digital global, que lleva inmersa la recolección de los datos, uso y borrado, y se hacen necesarios acuerdos entre países que permitan que los acuerdos pactados de confidencialidad permanezcan siempre intactos. Estados Unidos y la Unión Europea han adelantado un acuerdo llamado “Escudo de la Privacidad” el cual busca cumplir con este fin.(Europea, n.d.)

4.3 Marco legal

La Ley 1581 de 201 reglamentada mediante el decreto 1377 de 2013, reglamenta:

"Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente Ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control, del lavado de activos y el financiamiento del terrorismo.

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales.

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008. f) A las bases de datos y archivos regulados por la Ley 79 de 1993." (Colombia. Congreso de la República, 2012)

4.4 Estado del arte

Al desarrollarse diferentes tecnologías para optimizar el uso de los recursos disponibles, avanzan los sistemas de administración de ambientes virtualizados, viéndose impactado en gran medida el tratamiento del dato sensible y la seguridad que se provee para tratar de garantizar la privacidad deseada en los datos almacenados en ambientes de nube (Wang, Wang, Ren, & Lou, 2009), es allí donde empieza a tener valor la estrategia que se utilice para disminuir el impacto negativo sobre el negocio, que puede causar el uso inadecuado y no autorizado de la información, ya que en ambientes virtualizados de nube es compleja la definición de las fronteras físicas que anteriormente existían en los data center propietarios.

Se deben considerar las medidas que implementa la NIST SP 800-144,(Jansen & Grance, 2011) como parte fundamental de la estrategia, complementado con un acuerdo de servicios (ANS) y fortaleza en el contrato establecido desde el punto de vista jurídico y penal que corresponda en cada país, tanto donde se utiliza el servicio como donde se almacenan los datos, teniendo en cuenta los servicios de alta disponibilidad que se encuentran distribuidos en diferentes partes del mundo.

En el mercado de servicios de almacenamiento en la nube, se encontrarán proveedores con un sinnúmero de servicios con características atractivas desde el punto de vista de servicio, sin embargo, el punto realmente importante confluye en elegir un proveedor que ayude a garantizar el cumplimiento de la normatividad vigente en temas de protección de datos en Colombia.

No se debe olvidar de las obligaciones que se adquieren al ser responsable de la información captada y que de igual manera se debe establecer una relación de iguales dimensiones con quien será el prestador del servicio.(David López Jiménez, 2013)

Es importante considerar aspectos como:

- Inclusión del principio de privacidad de la información desde manera temprana.
- Cláusula de confidencialidad.
- Certificaciones que puedan impactar el negocio de manera positiva.
- Establecer acuerdos de niveles de servicio adecuados para mi negocio.
- El servicio contratado debe cumplir con todas mis necesidades como empresa, y a su vez debe cumplir con los requerimientos de ley.
- Al ser un contrato de servicios se debe buscar equilibrio en las responsabilidades de tratamiento de información sensible, ya que deben estar soportados adecuadamente los perfiles de responsable y encargado según lo dicta la ley.(Casasola Robles Mario et al., 2014)

"En los últimos años se ha hecho popular el concepto de evaluación del impacto de la privacidad (PIA), una evaluación independiente de los riesgos para la privacidad de un determinado servicio o sistema, junto con consejos sobre cómo solucionar las cosas si es necesario. Pocos contratos de nube incluyen referencias a los PIA. Asimismo, no permiten comprobar el cumplimiento de la privacidad a sus clientes." (Oppenheim, 2012)

La evaluación del impacto en la privacidad de los datos lleva una creciente maduración en países con legislaciones comprometidas con la protección de datos, esta es en sí un análisis de riesgos que buscan eliminarlos o mitigarlos y a tratarlos entre los interesados, convirtiéndose en un ejercicio de retroalimentación entre los tratantes.(AEPD, 2014b)(AEPD, 2014a)

Se deben establecer acuerdos que permitan realizar mediciones del servicio en términos del cumplimiento de los acuerdos del contrato a fin de poder planificar el aprovisionamiento.

No se puede dejar de un lado la importancia que tiene incluir en el contrato, la terminación de la relación comercial con el proveedor, la cual debe incluir la eliminación de datos.(Bradshaw, Millard, & Walden, 2011)

Amazon inicia como pionero del servicio de cloud en el año 2006, seguido de Azure en el año 2010 y un año más tarde presenta sus servicios el gigante Google. Rápidamente comienzan a incursionar con servicios independientes que daban inicios a un conjunto de herramientas encargadas de mitigar la exposición de la información y los constantes ataques a los que estaban expuestos los sitios publicados en la nube. Actualmente la seguridad como servicio es un componente fundamental que no puede ser opcional al momento de elegir la estrategia de nube.

La seguridad como servicio ofrece a los administradores tener un mayor control de la infraestructura que tenga alojada en la nube(Hussain & Abdulsalam, 2011), así como de las medidas de seguridad implementadas para proteger la misma, dotados de herramientas de gestión operativa y prácticas de mitigación de amenazas que son esenciales para la protección fuerte de servicios y datos.

Se puede llegar a concluir como lo afirma el autor(Van Niekerk & Jacobs, 2013), en una solución de infraestructura hibrida, la cual combine tecnologías de seguridad basadas en la nube, apoyada con soluciones de infraestructura propietaria, el objeto de esta guía es escoger la mejor implementación de seguridad basada en la nube, por lo que se propone y se deja planteado un próximo estudio referente a la implementación.

El responsable por parte del cliente debe desplegar toda su confianza en el proveedor de servicios, previamente diseñado un contrato y unos acuerdos de servicios, para resguardar los

datos sensibles y buscar la garantía inquebrantable de que los utilizara específica y explícitamente para resguardarlos y mantenerlos disponibles.(Susana Navas Navarro, 2015)

Teniendo claro el significado de SECaaS y su papel dentro de una implementación de almacenamiento basado en la nube, analizaremos los tres principales proveedores de servicios en la nube a nivel mundial(Services, Azure, & Platform, n.d.) y su implementación SECaaS, para posteriormente realizar un cuadro comparativo de servicios. (Mahendiran, Saravanan, & Sairam, 2012)

Amazon Web Services

(AmazonWeb Services, n.d.)

- Proporciona diferentes opciones en cuanto a capacidad y servicios de seguridad para mejorar la privacidad y control el acceso de redes.
- Los firewalls de red integrados en Amazon y sus capacidades para aplicaciones web permiten crear redes privadas y controlar el acceso a las instancias y aplicaciones.
- Cifrado con TLS, opciones de conectividad que permiten conexiones privadas o dedicadas desde la oficina o entorno on-premise.
- Los servicios que se diseñan con una respuesta automática a los ataques
- DDoS, Amazon CloudFront y Amazon Route 53.
- Características de cifrado escalables y eficientes disponibles en los servicios de base de datos y almacenamiento de AWS, como EBS, S3, Glacier, Oracle RDS, SQL Server RDS y Redshift.
- Opciones de administración de claves, como AWS Key Management Service.
- Almacenamiento de claves criptográficas dedicado y basado en hardware que utiliza AWS CloudHSM.
- API para integrar el cifrado y la protección de los datos con cualquiera de los servicios que desarrolle o implemente en un entorno de AWS.
- Servicio de evaluación de la seguridad, Amazon Inspector.
- Herramientas de implementación para administrar la creación y la desactivación de los recursos de AWS conforme a los estándares de la organización.
- Herramientas de administración de inventario y configuración.
- Herramientas de definición y administración de plantillas, como AWS CloudFormation.
- AWS proporciona herramientas y características que permiten ver exactamente lo que sucede en su entorno de AWS
- Gran visibilidad en las llamadas de la API a través de AWS CloudTrail,

- Opciones de agregación de logs que simplifican las investigaciones y los informes de conformidad.
- Notificaciones de alerta a través de Amazon CloudWatch.
- Herramientas y características para identificar problemas antes de que afecten a la empresa
- Capacidades para definir, hacer cumplir y gestionar las políticas de acceso de los usuarios en los servicios de AWS
- AWS Identity and Access Management (IAM) permite definir cuentas de usuarios individuales
- AWS Multi-Factor Authentication para cuentas con privilegios
- AWS Directory Service permite integrarse y federarse con directorios corporativos
- AWS ofrece integración nativa con Identity and Access Management
- Pruebas de intrusión

Microsoft Azure (Đorđević, Jovanović, & Timčenko, 2014)

(Microsoft, n.d.)

- Gestión de identidad y acceso (Azure Active Directory)
- Estrategia de seguridad en la infraestructura y operaciones
- Seguridad en las redes, Firewall, VPN
- ExpressRoute, Forced Tunnleing
- Netwotk security groups
- IP Management
- Protección antimalware, manejo de amenazas y prevención de ataques DDoS
- Test de penetración
- Logs de auditoria y monitoreo centralizado con sistemas de análisis de datos y alertas
- Cifrado de información AES-256
- Programa SDL, requisitos de seguridad en desarrollo de software
- Responsabilidad compartida

Google Cloud Plataform

(Google, 2016)

- Redundancia de servidores a nivel mundial
- Gestión de usuarios y credenciales de acceso
- Procedimientos especializados de borrado de información
- Auditoria automática periódica
- Canales cifrados SSL / TLS, Cifrado de datos AES256 para datos almacenados
- VPN, Firewall
- Ip Privadas

- IDS / IPS
- Análisis de seguridad basado en la nube
- Pruebas de penetración
- Gestión de datos sensibles
- Cuadros de mando para gestionar servicios de infraestructura y seguridad
- Cumplimiento de PCI – HIPAA y protección de datos de la UE

5 METODOLOGÍA

Para alcanzar el objetivo se realizará el enfoque en una investigación de tipo descriptivo, se hace necesario iniciar con una fase de detección de necesidades de la empresa, seguido por un estudio para comparar los tres grandes proveedores de servicios en la nube a nivel mundial con su producto de seguridad, luego se realizará un enfoque en la normatividad colombiana, para poder establecer la guía objeto de este Proyecto. Por medio de una investigación aplicada se profundizara en la técnica empleada por los proveedores de almacenamiento en la nube con producto de seguridad como servicio, y se hará un enfoque especial en los tres grandes proveedores a nivel mundial, como son Amazon, Microsoft Azure y Google, de los cuales se tienen que evaluar diferentes aspectos como la implementación de firewall, la existencia del IDS / IPS, análisis de SSL, manejo de certificados, conexiones VPN, herramientas de cifrado, integración con sistemas de administración de cuentas, y algunos otros que son determinantes para las empresas del sector servicios en Colombia

Conocer las necesidades de seguridad de las empresas del sector servicios.

Basados en la normatividad colombiana aplicable a este proyecto, se deben determinar los requerimientos mínimos de norma para buscar satisfacerlos en los servicios ofrecidos por los proveedores de almacenamiento en la nube.

Comparar los tres grandes proveedores a nivel mundial de SECaaS, disponibles en el mercado, mediante una matriz.

Los tres grandes proveedores de servicios de almacenamiento en la nube ofrecen en conjunto el servicio seguridad, el cual debe ser analizado de manera separada y determinar su nivel de complimiento respecto a la normatividad vigente al año 2017.

Seleccionar según los criterios de la normatividad colombiana de tratamientos de datos sensibles el proveedor de nube óptimo.

Según los datos arrojados en el numeral anterior se deben puntuar los ítems a fin de obtener la totalidad de los puntajes y poder así determinar el proveedor que más características ofrece y se ajusta a la normatividad exigida.

Documentar la guía para una correcta ejecución de la seguridad como servicio en el proveedor óptimo.

Teniendo elegido el proveedor de almacenamiento en la nube con componente de seguridad como servicio y que se acopla el cumplimiento de los requerimientos de la normatividad colombiana al año 2018, se deben establecer los ítems del checklist que cumplen con el requerimiento del objetivo.

6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

La matriz de controles en cloud (CCM de Cloud Security Alliance) proporciona los principios de seguridad fundamentales para orientar a los proveedores de la nube y para ayudar a los usuarios de la nube a evaluar el riesgo general de seguridad de un proveedor de la nube, presentando un marco de control que permite una comprensión detallada de los conceptos y principios de seguridad mediante 13 dominios. Los fundamentos de la matriz se apoyan con otros estándares de seguridad, regulaciones y marcos de control como ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum y NERC CIP. Brindando herramientas a las organizaciones para entender la estructura, los detalles y la claridad necesaria en relación con la seguridad de la información adaptada a la nube. Su objetivo es fortalecer los entornos existentes de controles de seguridad de la información, reducir e identificar amenazas de seguridad y vulnerabilidades en la nube y proporcionar seguridad y administración de riesgo operacional. La funcionalidad de la guía permite aplicarla de manera dinámica a otros proveedores que se quieran avaluar bajo los mismos estándares, permitiendo reemplazar los proveedores evaluados en las tablas y en adelante proveer la información del análisis de cada uno de ellos para poder obtener los resultados deseados.

1. Identificar las necesidades de seguridad para almacenamiento de información en la nube de las empresas de mensajería según la normatividad vigente en Colombia en el año 2017 y la exposición de riesgos inherentes a los servicios prestados.

En la tabla #1 se muestran los ítems de seguridad que deben estar disponibles en las plataformas de almacenamiento en la nube y que deben ser tenidos en cuenta al momento de elegir el proveedor del servicio de almacenamiento en la nube.

Detección de necesidades de la empresa	
N°	Necesidad
1	Almacenamiento seguro de informacion
2	administracion de parametros de seguridad
3	alta disponibilidad de la plataforma de almacenamiento
4	procedimientos de backup
5	alta disponibilidad en las conexiones
6	Metodos de cifrado para los datos
7	seguridad en el acceso a la plataforma, SSL, HTTPS
8	conectividad con servicios de directorio activo
9	configuracion de la plataforma
10	administracion de cuentas de usuario
11	calidad del servicio Qos
12	Adhesion a sistemas operativos de servidor
13	cumplimiento de normatividad
14	cumplimiento de leyes de proteccion de datos
15	contrato de responsabilidad

Tabla 1: Lista de ítems de las necesidades de seguridad de las empresas al contratar servicios de almacenamiento en la nube.

2. Comparar los tres grandes proveedores a nivel mundial de SECaaS, disponibles en el mercado.

La tabla 2 realiza un comparativo de los 3 grandes proveedores del servicio de almacenamiento en la nube y puntúa los elementos de su servicio.

Caracteristicas de seguridad en plataforma	Amazon	P	Azure	P	Google	P
Certificaciones	20	8	25	10	6	2
Disponibilidad	99,95%	10	99,95%	10	99,95%	10
Indisponibilidad real medida Hr/mes	1,02	10	33,22	1	9,42	1
centros de datos redundantes	44	10	20	4	4	1
backup	3	1	3	1	n	10
Autenticación y autorización	Administración de identidad y acceso Multi-Factor Authentication	10	Azure AD/control de acceso basado en roles Autenticación multifactor	10	Forzada de 2 factores/chip titan/API/ SSL / TLS	10
Cifrado	Key Management Service CloudHSM, TLS/SSL	10	Almacén de claves, claves publicas, TLS/SSL,IPSec, AES 256, Azure Disk Encryption	10	AES256	5
Firewall	Web Application Firewall	10	Presente	10	Presente	10
Modelo Seguridad	Amazon Macie	10	Security Center (versión preliminar)	10	SSL Default	10
Servicios de directorio	Directory Service	10	Active Directory de Azure Azure Active Directory B2C Servicios de dominio de Azure Active Directory	10	Administracion de cuentas	8
Cumplimiento proteccion de datos	Cumple alienado con la union europea	10	Presente y avanzando en america latina	6	Programa de prevencion de filtrado de datos	5
Responsabildiad compartida	Presente	10	No presente	1	No presente	1
Analisis de vulnerabilidades	Presente	10	Presente	10	Presente	10
IDS / IPS	Presente	10		10	Presente	10
Puntaje		129		103		93
Cumplimiento		92%		74%		66%

Informacion de Amazon tomada de la hoja del producto AWS: https://aws.amazon.com/es/security/
Informacion de Azure tomada de la hoja del producto: https://www.microsoft.com/en-us/trustcenter/security/azure-security
Informacion de Google tomada de la hoja del producto: https://cloud.google.com/security/
Las puntuaciones de cada caracteristica se identifican con 1 la puntuacion minima a 10 con la puntuacion maxima.

Tabla 2: Características de SECaaS por proveedor de servicios en la nube.

3. Seleccionar según los criterios de la normatividad colombiana de tratamientos de datos sensibles el proveedor de nube más adecuado.

En la tabla 3 podremos encontrar un extracto de los elementos fundamentales que tienden a dar cumplimiento a la ley de protección de datos vigente en Colombia.

	REQUERIMIENTOS DE LEY	Amazon	Azure	Google
1	cumplimiento de principios de disponibilidad, confidencialidad e integridad	X	X	X
2	acciones para dar continuidad al negocio	X	X	X
3	Plan de recuperacion de desastres	X	X	X
4	Baja duracion del tiempo fuera del aire por mantenimiento al mes	X	O	X
5	identicación y manejo de los riesgos asociados al tratamiento de datos personales	X	X	X
6	Informar a los titulares del tratamiento de informacion en la nube	N/A	N/A	N/A
7	cumplimiento de las normas sobre protección de datos personales de Colombia, Ley 1581 de 2012	O	O	O
8	implementar procedimientos de incidentes de seguridad	X	X	X
9	determinar si hay subcontratacion de servicios	N/A	N/A	N/A
10	determinar medidas de seguridad en transito de informacion	X	X	X
11	determinar formatos de almacenamiento y portabilidad de informacion	X	X	X
12	determinar mecanismos de entrega y destruccion de la informacion	X	X	X
13	determinar niveles de disponibilidad del servicio	X	X	X
14	determinar lozalizacion del almacenamiento de la informacion	X	X	X
15	permite adhesion del decreto 1074 de 2015	O	O	O
16	permite adhesion a la politica de tratamiento del responsable	O	O	O
17	determinar si cumple con la infraestructura y reputacion necesarias	X	X	X
18	utilizar y ejecutar una metodologia de gestion de riesgos	X	X	X
19	fortaleza en el control de acceso en plaforma y aplicativos	X	X	X
20	log de actividades	X	X	X
21	pruebas de seguridad	X	X	X
	Según los requerimientos expresados en : http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf			

Tabla 3: Requerimientos de seguridad según la ley de protección de datos en Colombia

Según los parámetros expuestos en los dos anteriores objetivos el proveedor que mas se ajusta al cumplimiento de la normatividad colombiana en términos de protección de datos es Amazon con su producto AWS.

4. Documentar la guía para una correcta ejecución de la seguridad como servicio en el proveedor más adecuado.

La tabla 4 expone el relacionamiento entre los controles de CCM versus los proveedores de nube líderes del mercado.

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Aplicación y seguridad de interfaz de seguridad de las aplicaciones	AIS-01	Aplicaciones e interfaces de programación (API) deberán diseñarse, desarrollar, desplegar y probados de acuerdo con los estándares líderes de la industria (por ejemplo, OWASP para aplicaciones web) y se adhieren a las obligaciones de cumplimiento legal, estatutaria, o reglamentarias aplicables.	X	X	X
De aplicación y seguridad de la interfaz Requisitos de acceso de cliente	AIS-02	Antes de conceder a los clientes acceso a los datos, activos y sistemas de información, de seguridad identificados, contractuales y requisitos reglamentarios para el acceso del cliente serán dirigidas.	Ok	Ok	Ok
Aplicación e interfaz de datos de seguridad Integridad	AIS-03	entrada de datos y la integridad de salida rutinas (es decir, la reconciliación y editar cheques) se aplicarán para interfaces de aplicación y bases de datos para prevenir manual o errores de procesamiento sistemáticas, la corrupción de datos, o mal uso.	Ok	Ok	Ok
Aplicación y seguridad de interfaz de seguridad de datos / Integridad	AIS-04	Políticas y procedimientos deben establecerse y mantenerse para garantizar la seguridad de datos para incluir (confidencialidad, integridad y disponibilidad) a través de múltiples interfaces del sistema, jurisdicciones y funciones de la empresa para evitar la divulgación indebida, alteración o destrucción.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Verificación de aseguramiento y cumplimiento de Planificación de Auditoría	AAC-01	Los planes de auditoría se desarrollan y se mantienen para hacer frente a las interrupciones de procesos de negocio. planes de auditoría se centrarán en la revisión de la eficacia de la ejecución de las operaciones de seguridad. Todas las actividades de auditoría deben ser acordados antes de ejecutar cualquier auditoría.	Ok	Ok	Ok
Verificación de aseguramiento y cumplimiento auditorías independientes	AAC-02	revisiones independientes y evaluaciones se realizaron al menos anualmente para asegurar que la organización se ocupa de las no conformidades de las políticas establecidas, las normas, los procedimientos y las obligaciones de cumplimiento.	Ok	Ok	Ok
Auditar Cartografía Sistema de Aseguramiento y Cumplimiento Información reguladora	AAC-03	Las organizaciones deberán crear y mantener un marco de control que capta las normas, normativo, jurídico y los requisitos legales pertinentes para sus necesidades de negocio. Las medidas de control se revisará al menos anualmente para asegurar que los cambios que podrían afectar el negocio de los procesos se reflejan.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Gestión de Continuidad Operacional y Resiliencia planificación de la continuidad	BCR-01	Se establecerá un marco unificado consistente para la planificación de la continuidad del negocio y el desarrollo del plan, documentado, y adoptó para asegurar que todos los planes de continuidad de negocio son consistentes en el tratamiento de las prioridades de los requisitos de pruebas, mantenimiento y seguridad de la información. Requisitos para los planes de continuidad de negocio son los siguientes: • El propósito y el alcance definidos, alineado con las dependencias pertinentes • accesible y comprensible para los que van a utilizarlos • Propiedad de una persona (s) nombrado que es responsable de su revisión, actualización y aprobación • líneas de comunicación específicos, funciones y responsabilidades • Los procedimientos detallados de recuperación, manual de trabajo en torno, e información de referencia • Método para invocación plan de	Ok	Ok	Ok
Gestión de Continuidad Operacional y resiliencia de negocio Prueba de continuidad	BCR-02	planes de respuesta de continuidad de negocio y de incidentes de seguridad estarán sometidas a las pruebas a intervalos planificados o en los cambios de organización o ambiental importante. planes de respuesta a incidentes debe involucrar clientes afectados (inquilino) y otras relaciones comerciales que representan las dependencias de procesos de negocio dentro de la cadena de suministro críticos.	Ok	Ok	Ok
Administración de la continuidad y de funcionamiento de centros de datos Resiliencia Utilidades / Condiciones ambientales	BCR-03	del centro de datos de servicios públicos servicios y las condiciones ambientales (controles por ejemplo, agua, potencia, temperatura y humedad, las telecomunicaciones, y la conectividad a Internet) ha de ser asegurado, supervisada, mantienen, y se ensayaron para la eficacia continua a intervalos planificados para garantizar la protección de la intercepción o daños no autorizado, y diseñado con conmutación por error automatizada o otros redundancias en el caso de interrupciones planificadas o no planificadas.	Ok	Ok	Ok

Gestión de Continuidad Operacional y Documentación Resiliencia	BCR-04	La documentación del sistema de información (por ejemplo, administrador y usuario, guías y diagramas de arquitectura) se pondrá a disposición del personal autorizado para asegurar los siguientes: • Configuración, instalación y operación del sistema de información • La utilización eficaz de las funciones de seguridad del sistema	Ok	Ok	Ok
Business Continuity Management y operacionales Los riesgos ambientales Resiliencia	BCR-05	La protección física contra daños por causas naturales y los desastres, así como los ataques deliberados, incluyendo incendios, inundaciones, descargas eléctricas atmosféricas, solar inducida tormenta geomagnética, viento, terremotos, tsunamis, explosiones, accidentes nucleares, actividad volcánica, riesgo biológico, disturbios civiles, deslave, la actividad tectónica, y otras formas de desastres naturales o de origen humano deberán ser anticipados, diseñados, y han aplicado contramedidas.	Ok	Ok	Ok
Gestión de Continuidad Operacional y Ubicación Equipamiento Resiliencia	BCR-06	Para reducir los riesgos de las amenazas ambientales, los peligros y las oportunidades de acceso no autorizado, el equipo deberá mantenerse alejado de lugares expuestos a riesgos ambientales de alta probabilidad y complementados con equipos redundantes situado a una distancia razonable.	Ok	Ok	Ok
Business Continuity Management y Mantenimiento Equipo Resiliencia operacional	BCR-07	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para el mantenimiento de equipos de garantizar la continuidad y disponibilidad de las operaciones y el personal de apoyo.	Ok	Ok	Ok
Business Continuity Management y fallas de energía Equipo Resiliencia operacionales	BCR-08	Las medidas de protección se ponen en su lugar de reaccionar a las amenazas naturales y artificiales en base a una evaluación de impacto en el negocio geográficamente específicos.	Ok	Ok	Ok
Business Continuity Management y Análisis de resiliencia al impacto operacional	BCR-09	Habrá un método definido y documentado para determinar el impacto de cualquier interrupción de la organización (proveedor de la nube, nube del consumidor) que debe incorporar los siguientes: • Identificar los productos y servicios • Identificar todas las dependencias, incluyendo procesos, aplicaciones, socios comerciales críticos, y proveedores de servicios de terceros • Entender las amenazas a los productos y servicios críticos • Determinar los impactos resultantes de interrupciones planificadas o no planificadas y cómo éstos varían con el tiempo • Establecer el período máximo tolerable de interrupción • Establecer prioridades para la recuperación • Establecer los objetivos de tiempo de recuperación para la reanudación de la crítica productos y servicios dentro de su período máximo tolerable de interrupción • estimar los recursos necesarios para la reanudación	Ok	Ok	Ok
Gestión de Continuidad Operacional y Política de resiliencia	BCR-10	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para el gobierno de TI apropiado y gestión de servicios para asegurar una adecuada planificación, entrega y apoyo de las capacidades de TI de la organización de apoyo funciones de negocios, mano de obra, y / o clientes basados en la industria normas aceptables (es decir, V4 ITIL y COBIT 5). Además, las políticas y procedimientos incluirán funciones y responsabilidades definidas con el apoyo de la formación regular la fuerza de trabajo.	N/A	N/A	N/A
Administración de la continuidad operativa y política de retención de resiliencia	BCR-11	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para definir y adherirse al período de conservación de cualquier activo crítico según las políticas y procedimientos establecidos, así como las obligaciones de cumplimiento legal, estatutaria, o reglamentarias aplicables. medidas de respaldo y recuperación serán incorporados como parte de la planificación de la continuidad del negocio y probados en consecuencia para la eficacia.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Control de Cambio y Gestión de Desarrollo de Nuevos Configuración / Adquisición	CCC-01	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para garantizar el desarrollo y / o la adquisición de nuevos datos, aplicaciones físicas o virtuales, redes de infraestructura, y componentes de sistemas, o cualquier corporativa, operaciones y / o centros de datos instalaciones han sido autorizados previamente por la dirección comercial de la organización o de otro tipo de rol de cuentas o función.	Ok	Ok	Ok
Control de Cambio y Gestión de Desarrollo de configuración Outsourced	CCC-02	socios de negocios externos deberán adherirse a las mismas políticas y procedimientos para la gestión del cambio, la liberación, y las pruebas de los desarrolladores internos dentro de la organización (por ejemplo, los procesos de gestión de servicios ITIL).	N/A	N/A	N/A
Control de cambios y configuraciones de Pruebas de Calidad de Gestión	CCC-03	Las organizaciones deberán seguir un proceso de control de cambios de calidad y pruebas definidas (por ejemplo, ITIL Service Management) con líneas de base establecidas, pruebas, y liberar las normas que se centran en la disponibilidad del sistema, la confidencialidad y la integridad de los sistemas y servicios.	Ok	Ok	Ok
El control de cambios y configuración de gestión de instalaciones de software no autorizado	CCC-04	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para restringir la instalación de software no autorizado en los dispositivos de propiedad organizativamente-o gestionados por el usuario de punto final (por ejemplo, estaciones de trabajo emitidos, portátiles y dispositivos móviles) y la red de infraestructura de TI y componentes de los sistemas.	Ok	Ok	Ok
Control de cambios y configuraciones cambios en la administración de Producción	CCC-05	Se establecerán políticas y procedimientos para la gestión de los riesgos asociados con la aplicación de cambios en: • aplicaciones -impacting críticos para el negocio o cliente (arrendatario) (físicos y virtuales) y diseños de interfaz del sistema-sistema (API) y configuraciones. • Red de infraestructura y componentes de los sistemas. Las medidas técnicas se llevarán a cabo para proporcionar la seguridad de que todos los cambios se corresponden directamente a una solicitud de cambio de domicilio, críticos para el negocio o cliente (arrendatario), y / o la autorización, el cliente (arrendatario) según el acuerdo (SLA) antes del despliegue.	N/A	N/A	N/A

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Seguridad de datos e información Clasificación Lifecycle Management	DSI-01	Datos y objetos que contengan datos no podrán recibir una clasificación por parte del titular de los datos en función del tipo de dato, valor, sensibilidad y criticidad de la organización.	Ok	Ok	Ok
Seguridad de los datos e información del ciclo de vida de datos de gestión de inventario / Flujos	DSI-02	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para inventariar, documentar y mantener los flujos de datos para los datos residentes (permanente o temporal) dentro de las aplicaciones del servicio geográficamente distribuida (físicos y virtuales) y la red de infraestructuras y componentes de los sistemas y / o compartida con otros terceros para determinar cualquier impacto cumplimiento de la normativa, o un acuerdo legal cadena de suministro (SLA), y para hacer frente a cualquier otro riesgo de negocio asociadas con los datos. A petición, el proveedor deberá informar al cliente (arrendatario) de impacto cumplimiento y el riesgo, sobre todo si los datos del cliente se utiliza como parte de los servicios.	Ok	Ok	Ok
La seguridad de datos e información de gestión del ciclo de vida transacciones de comercio electrónico	DSI-03	Los datos relacionados con el comercio electrónico (comercio electrónico) que atraviesa las redes públicas deberán estar debidamente clasificados y protegidos de la actividad fraudulenta, la divulgación no autorizada, o la modificación de tal manera para evitar conflicto del contrato y compromiso de los datos.	Ok	Ok	Ok
Seguridad de datos y de información de administración del ciclo de vida de manipulación / Etiquetado / Política de Seguridad	DSI-04	Se establecerán políticas y procedimientos para el etiquetado, la manipulación, y la seguridad de los datos y objetos que contienen datos. Mecanismos para la herencia etiqueta se aplicarán para los objetos que actúan como contenedores agregados para datos.	Ok	Ok	Ok
Seguridad de datos e información del ciclo de vida de gestión de datos no producción	DSI-05	Los datos de producción no se replican o se utilizan en entornos no productivos. Cualquier uso de los datos del cliente en entornos no productivos requiere explícita, aprobación documentada de todos los clientes cuyos datos se ve afectada, y debe cumplir con todos los requisitos legales y reglamentarios para la depuración de elementos de datos sensibles.	N/A	N/A	N/A
Seguridad de datos e información del ciclo de vida de la Administración Propiedad / Administración	DSI-06	Todos los datos serán designados con la administración, la asignación de responsabilidades definidos, documentados y comunicados.	N/A	N/A	N/A
Seguridad de datos y de información de administración del ciclo de vida de eliminación segura,	DSI-07	Las políticas y procedimientos se establecerán con los procesos de negocio de apoyo y medidas técnicas aplicado para la eliminación segura y una retirada completa de datos de todos los medios de almacenamiento, asegurando que los datos no es recuperable por cualquier medio en informática forense.	X	X	X

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Gestión de Activos centro de datos de seguridad	DCS-01	Los activos deben clasificarse en función de la criticidad de negocios, las expectativas de nivel de servicio y los requisitos de continuidad de funcionamiento. Un inventario completo de los bienes esenciales para la empresa ubicadas en todos los sitios y / o ubicaciones geográficas y su uso en el tiempo se mantiene y se actualiza con regularidad, y se le asigna la propiedad por los roles y responsabilidades definidos.	N/A	N/A	N/A
Centro de datos de seguridad puntos de acceso controlado	DCS-02	perímetros de seguridad física (por ejemplo, cercas, paredes, barreras, guardias, puertas, la vigilancia electrónica, mecanismos de autenticación físicas, mostradores de recepción, y las patrullas de seguridad) se aplicarán para salvaguardar los datos sensibles y sistemas de información.	Ok	Ok	Ok
La identificación de centros de datos Equipo de Seguridad	DCS-03	identificación de equipo automatizado se utiliza como un método de autenticación de la conexión. tecnologías de reconocimiento de ubicación se pueden utilizar para validar la integridad de autenticación de conexión basándose en la ubicación del equipo conocido.	Ok	Ok	Ok
Centro de datos de seguridad fuera del sitio de Autorización	DCS-04	Se debe obtener autorización antes de la reubicación o transferencia de hardware, software, o los datos a un local fuera del sitio.	Ok	Ok	Ok
Centro de datos de seguridad fuera del sitio Equipo	DCS-05	Se establecerán políticas y procedimientos para la eliminación segura de los equipos (por tipo de activo) que se utiliza fuera de las instalaciones de la organización. Esto incluirá un procedimiento en disolución o destrucción de limpiar que hace imposible la recuperación de la información. El borrado consistirá en una sobreescritura completa de la unidad para asegurarse de que la unidad de borrado se libera al inventario para su reutilización y despliegue o almacena de forma segura hasta que pueda ser destruido.	X	X	X
Política de Seguridad del centro de datos	DCS-06	Se establecerán políticas y procedimientos y procesos de negocio de apoyo implementados, para mantener un ambiente de trabajo seguro en oficinas, salas, instalaciones y áreas seguras que almacenan información sensible.	Ok	Ok	Ok
Seguridad centro de datos seguro Área de Autorización	DCS-07	De entrada y salida para asegurar áreas serán limitadas y controladas por mecanismos de control de acceso físico para garantizar que sólo el personal autorizado se permite el acceso.	Ok	Ok	Ok
Centro de datos de seguridad de entrada de personas no autorizadas	DCS-08	Ingress y puntos de salida, tales como áreas de servicio y otros puntos en los que personal no autorizado puede entrar en el local estarán controlados, controlados y, si es posible, aislado de las instalaciones de almacenamiento y procesamiento de datos para prevenir la corrupción no autorizado de datos, el compromiso y la pérdida.	Ok	Ok	Ok
Centro de datos de seguridad de acceso del usuario	DCS-09	El acceso físico a los activos y las funciones de información de los usuarios y el personal de apoyo deberá estar restringido.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Cifrado y clave de gestión de derechos	EKM-01	Las claves deben tienen los propietarios identificables (teclas que se unen a las identidades) y no habrá políticas de gestión de claves.	Ok	Ok	Ok
Encriptación y administración de claves de generación de claves	EKM-02	Se establecerán políticas y procedimientos para la gestión de claves criptográficas en criptosistema del servicio (por ejemplo, la gestión del ciclo de vida de la generación de claves de revocación y sustitución, infraestructura de clave pública, el diseño del protocolo criptográfico y algoritmos utilizados, los controles de acceso en su lugar para la generación de claves seguras, y intercambio y almacenamiento incluyendo segregación de claves utilizadas para los datos cifrados o sesiones). A petición, el proveedor deberá informar al cliente (arrendatario) de los cambios en el sistema de cifrado, especialmente si los datos (arrendatario) del cliente se utiliza como parte del servicio, y / o el cliente (arrendatario) tiene algo de responsabilidad compartida a través de la implementación del control .	Ok	Ok	Ok
Protección de Datos Sensibles encriptación y administración de claves	EKM-03	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para el uso de protocolos de cifrado para la protección de los datos sensibles de almacenamiento (por ejemplo, servidores de archivos, bases de datos y estaciones de trabajo de usuario final), los datos de utilización (memoria) , y los datos en la transmisión (por ejemplo, las interfaces del sistema, a través de redes públicas, y la mensajería electrónica) como por las obligaciones de cumplimiento legales, estatutarias y reglamentarias aplicables.	Ok	Ok	Ok
Cifrado y almacenamiento de administración de claves y Acceso	EKM-04	Plataforma y el cifrado de datos apropiado (por ejemplo, AES-256) serán requeridos en formatos abiertos / validados y algoritmos estándar. Las llaves no se deberán almacenar en la nube (es decir, al proveedor de la nube en cuestión), pero mantienen por el consumidor nube o de confianza proveedor de gestión de claves. gestión de claves y uso de claves serán funciones separadas.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Gobernabilidad y Requisitos de Gestión de Riesgos de línea de base	GRM-01	se establecerán los requisitos de seguridad de línea de base para los países desarrollados o adquiridos, organizativamente propiedad o administrado, físico o virtual, aplicaciones y sistema de infraestructura de red y componentes que cumplan con las obligaciones de cumplimiento legales, estatutarias y reglamentarias aplicables. Las desviaciones de configuraciones de referencia estándar deben ser autorizadas seguir las políticas y procedimientos previos a la implementación, el aprovisionamiento, o el uso de gestión del cambio. El cumplimiento de las exigencias mínimas de seguridad debe ser reevaluado por lo menos anualmente menos una frecuencia alternativa se ha establecido y autorizado en base a las necesidades del negocio.	Ok	Ok	Ok
Gobernabilidad y Riesgo de Gestión de Datos Focus Evaluación de Riesgos	GRM-02	Las evaluaciones de riesgo asociados con los requisitos de gobierno de datos se llevarán a cabo a intervalos planificados, y considerará lo siguiente: • El conocimiento de donde se almacena y se transmite a través de aplicaciones, bases de datos, servidores y red de infraestructura • El cumplimiento de los períodos de retención definidos y fin-de-datos sensibles requisitos de eliminación de la vida • La clasificación de datos y la protección contra el uso no autorizado, el acceso, la pérdida, destrucción, y falsificación	Ok	Ok	Ok
Gobernanza y Gestión de Riesgos Gestión de Supervisión	GRM-03	Los gerentes son responsables de mantener el conocimiento y el cumplimiento de las políticas de seguridad, procedimientos y normas que son relevantes para su área de responsabilidad.	Ok	Ok	Ok
Programa de Gestión de Administración de Riesgos y gobernabilidad	GRM-04	Un Programa de Gestión de la Información de Seguridad (ISMP) será elaborado, documentado, aprobado y aplicado que incluye medidas de seguridad administrativas, técnicas y físicas para proteger los activos y los datos de la pérdida, mal uso, acceso no autorizado, revelación, alteración y destrucción. El programa de seguridad deberá incluir, pero no limitarse a, las siguientes áreas en la medida en que se refieren a las características del negocio: • Gestión de riesgos • Política de Seguridad • Organización de la seguridad de la información de gestión de activos • seguridad de los recursos humanos • La seguridad física y ambiental • gestión de comunicaciones y operaciones • Control de acceso • adquisición de sistemas de información, el desarrollo y el mantenimiento	Ok	Ok	Ok
Gobernabilidad y Riesgo de Apoyo a la Gestión Gestión / Participación	GRM-05	Ejecutivo y gestión de la línea tomarán medidas formales para apoyar seguridad de la información a través de la dirección y el compromiso documentado claramente, y garantizarán se le ha asignado la acción.	Ok	Ok	Ok
Gobernabilidad y Política de Gestión de Riesgos	GRM-06	políticas y procedimientos de seguridad de la información se establecerán y pongan a disposición para su revisión por el personal de todos los afectados y las relaciones comerciales externas. las políticas de seguridad de la información deben ser autorizados por el liderazgo de la organización empresarial (o de otro tipo de rol de cuentas o función) y apoyado por un plan de negocio estratégico y un programa de gestión de la seguridad de la información inclusiva de las funciones de seguridad de información definidos y responsabilidades para el liderazgo empresarial.	Ok	Ok	Ok
Gobernabilidad y Política de Control de Gestión de Riesgos	GRM-07	Se establecerá una política disciplinaria o sanción formal para los empleados que han violado las políticas y procedimientos de seguridad. Los empleados deben ser conscientes de las medidas que podrían adoptarse en caso de una violación, y las medidas disciplinarias deberán indicarse en las políticas y procedimientos.	Ok	Ok	Ok
Gobernabilidad y Riesgo Impacto de las Políticas de Gestión sobre Evaluación de Riesgos	GRM-08	resultados de la evaluación de riesgos incluirán cambios a las políticas de seguridad, procedimientos, estándares y controles para asegurar que siguen siendo pertinentes y eficaces.	Ok	Ok	Ok
Gobierno y la gestión de riesgos comentarios Política	GRM-09	liderazgo empresarial de la organización (u otro rol de cuentas o función) deberán revisar la política de seguridad de la información a intervalos planificados o como resultado de cambios en la organización para asegurar su alineación continuar con la estrategia de seguridad, eficacia, precisión, relevancia y aplicabilidad a legal, estatutaria, o las obligaciones de cumplimiento de normativas.	Ok	Ok	Ok
Gobierno y la gestión de riesgos Evaluación de Riesgos	GRM-10	Alineado con el marco de toda la empresa, las evaluaciones de riesgo formales se llevarán a cabo al menos anualmente o en intervalos planificados, (y en conjunción con cualquier cambio en los sistemas de información) para determinar la probabilidad y el impacto de los riesgos identificados utilizando métodos cualitativos y cuantitativos. La probabilidad y el impacto asociado con el riesgo inherente y residual se determinarán de forma independiente, teniendo en cuenta todas las categorías de riesgo (por ejemplo, resultados de la auditoría, análisis de amenazas y la vulnerabilidad, y de cumplimiento normativo).	Ok	Ok	Ok
Marco de Gobierno y Gestión de Riesgos Gestión de Riesgos	GRM-11	Riesgos serán mitigados a un nivel aceptable. niveles de aceptación en base a criterios de riesgo serán establecidos y documentados en conformidad con los plazos razonables y resolución de aprobación de las partes interesadas.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Recursos Humanos rendimientos de los activos	HRS-01	A la terminación del personal de la fuerza de trabajo y / o de caducidad de las relaciones de trabajo, externos, todos los activos propiedad organizativamente- deberán ser devueltos dentro de un plazo establecido.	Ok	Ok	Ok
Recursos humanos de investigación de antecedentes	HRS-02	De conformidad con las leyes locales, regulaciones, ética, y las restricciones contractuales, todos los candidatos de empleo, contratistas y terceros estará sujeta a verificación fondo proporcional a la clasificación de los datos para ser visitada, los requisitos de negocio, y el riesgo aceptable.	Ok	Ok	Ok
Recursos Humanos acuerdos de empleo	HRS-03	contratos de trabajo deberán incorporar disposiciones y / o términos de la adhesión a las políticas de gestión y seguridad de la información establecida y debe ser firmado por el personal de la fuerza laboral de nuevo ingreso o sobre- embarcados (por ejemplo, los empleados a tiempo completo o parcial o personal contingente) antes de la concesión de usuario personal de mano de obra el acceso a las instalaciones corporativas, recursos y activos.	Ok	Ok	Ok
Terminación de Recursos Humanos Empleo	HRS-04	Roles y responsabilidades para llevar a cabo la terminación del empleo o cambio en los procedimientos de empleo se asignarán, documentados y comunicados.	Ok	Ok	Ok
Gestión de dispositivos móviles de Recursos Humanos	HRS-05	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para gestionar los riesgos de negocio asociados a permitir el acceso de dispositivos móviles a los recursos corporativos y pueden requerir la implementación de controles de compensación más alta de aseguramiento y las políticas de uso aceptable y procedimientos (por ejemplo, el mandato formación de seguridad, controles de identidad, del derecho de acceso y más fuertes, y la supervisión de dispositivos).	Ok	Ok	Ok
Acuerdos de Recursos Humanos de no divulgación	HRS-06	Requisitos para los acuerdos de no divulgación o confidencialidad que reflejan las necesidades de la organización para la protección de los datos y detalles operativos serán identificados, documentados y revisados a intervalos planificados.	Ok	Ok	Ok
Recursos Humanos Roles / responsabilidades	HRS-07	Funciones y responsabilidades de los contratistas, empleados y terceros usuarios deberán documentarse en lo que respecta a los activos de información y seguridad.	Ok	Ok	Ok
Recursos Humanos Tecnología Uso Aceptable	HRS-08	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para la definición de las prestaciones y las condiciones para permitir el uso de dispositivos de punto final usuario propiedad organizativamente o administrados (por ejemplo, estaciones de trabajo emitidos, ordenadores portátiles y dispositivos móviles) y la infraestructura de TI redes y sistemas componentes. Además, la definición de prestaciones y condiciones para permitir el uso de dispositivos móviles personales y aplicaciones asociadas con el acceso a recursos de la empresa (es decir, BYOD) se examinará y constituida como apropiado.	Ok	Ok	Ok
Formación de Recursos Humanos / conciencia	HRS-09	Se establecerá un programa de formación de conciencia de seguridad para todos los contratistas, terceros usuarios y empleados de la organización y el mandato cuando sea apropiado. Todos los individuos con acceso a datos de la organización deberán recibir una formación adecuada conciencia y actualizaciones regulares en los procedimientos de organización, los procesos y las políticas relacionadas con su función profesional en relación con la organización.	Ok	Ok	Ok
Recursos Humanos Responsabilidad del Usuario	HRS-10	Todo el personal debe estar al tanto de sus funciones y responsabilidades para: • El mantenimiento de la conciencia y el cumplimiento de las políticas y procedimientos establecidos y las obligaciones de cumplimiento legal, estatutarias o reglamentarias aplicables. • Mantener un ambiente de trabajo seguro	Ok	Ok	Ok
Espacio de trabajo de Recursos Humanos	HRS-11	Se establecerán políticas y procedimientos para requerir que los espacios de trabajo sin supervisión no tienen abiertamente visibles (por ejemplo, sobre un escritorio) documentos sensibles y sesiones de uso de equipos informáticos están desactivados después de un período de inactividad establecido.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Identidad y gestión de acceso Herramientas de auditoría de acceso	IAM-01	El acceso a, y el uso de herramientas de auditoría que interactúan con los sistemas de información de la organización serán debidamente segregados y acceso restringido para evitar la divulgación inapropiada y la manipulación de datos de registro.	Ok	Ok	Ok
Identidades y Accesos Administración de credenciales del ciclo de vida / Gestión de Suministro	IAM-02	Se establecerán políticas y procedimientos de acceso de usuario, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para asegurar su identidad apropiada, el derecho y la gestión de acceso para todos (arrendatario) usuarios internos corporativos y de clientes con acceso a los datos y propiedad organizativamente-o administrado (física y virtual) interfaces de aplicaciones y la infraestructura de red y componentes de sistemas. Estas políticas, procedimientos, procesos y medidas deben incorporar los siguientes: • Procedimientos, papeles y responsabilidades para el aprovisionamiento y los derechos-de aprovisionamiento de cuentas de usuario siguiendo la regla del mínimo privilegio basado en la función de trabajo (por ejemplo, los empleados internos y personal de plantilla contingentes cambios, acceso controlado por el cliente, las relaciones comerciales de los proveedores,	Ok	Ok	Ok
Identidades y Accesos manejo diagnóstico Puertos / Configuración de acceso	IAM-03	El acceso del usuario a los puertos de diagnóstico y configuración se limitará a los individuos y las aplicaciones autorizadas.	Ok	Ok	Ok
Gestión de identidades y acceso Políticas y Procedimientos	IAM-04	Se establecerán políticas y procedimientos para almacenar y gestionar la información de identidad sobre cada persona que accede a la infraestructura de TI y para determinar su nivel de acceso. Las políticas también se desarrollarán para controlar el acceso a recursos de red basadas en la identidad del usuario.	Ok	Ok	Ok
De identidades y accesos Gestión segregación de funciones	IAM-05	Se establecerán políticas y procedimientos de acceso de usuario, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para restringir el acceso de los usuarios de acuerdo con la segregación de funciones definidas para hacer frente a los riesgos de negocio asociados a un conflicto en roles de usuario de interés.	Ok	Ok	Ok
Restricción de la identidad y gestión de acceso Fuente Código de Acceso	IAM-06	El acceso a aplicaciones propias de la organización desarrollados, programa o código de origen del objeto, o cualquier otra forma de propiedad intelectual (IP), y el uso de software propietario estará restringido apropiadamente siguiendo la regla del mínimo privilegio basado en la función de trabajo de acuerdo con el acceso de usuarios establecida Policias y procedimientos.	Ok	Ok	Ok
Acceso Identidad y Acceso de Terceros Gestión	IAM-07	La identificación, evaluación y priorización de los riesgos planteados por los procesos de negocio que requieren el acceso de terceros a los sistemas y datos de información de la organización deberán ser seguidos por la aplicación coordinada de los recursos para minimizar, monitorear y medir la probabilidad y el impacto del acceso no autorizado o inapropiado. Los controles de compensación derivados del análisis de riesgos se ejecutarán antes de aprovisionamiento de acceso.	Ok	Ok	Ok
Gestión de identidades y acceso Fuentes de confianza	IAM-08	Se establecen las políticas y procedimientos para el almacenamiento permisible y el acceso de las identidades utilizadas para la autenticación para garantizar las identidades son sólo accesibles en base a reglas de menos limitación privilegio y la replicación sólo a los usuarios definidos explícitamente como negocio necesario.	Ok	Ok	Ok
Autorización de acceso de usuario de identidades y accesos Gestión	IAM-09	Aprovisionamiento de acceso de los usuarios (por ejemplo, empleados, contratistas, clientes (inquilinos), socios de negocios, y / o relaciones con los proveedores) para aplicaciones de propiedad organizativamente-o gestionados (físicos y virtuales) de datos y sistemas de infraestructura, y los componentes de la red deberá ser autorizada por el la gestión de la organización antes de su acceso se concede y apropiadamente restringido de acuerdo con las políticas y procedimientos establecidos. A petición, el proveedor deberá informar al cliente (arrendatario) de acceso a este usuario, especialmente si los datos del cliente (arrendatario) se utiliza como parte del servicio y / o cliente (arrendatario) tiene algo de responsabilidad compartida a través de la implementación del control.	Ok	Ok	Ok
La identidad y el acceso de administración de acceso de usuario Comentarios	IAM-10	El acceso del usuario estará autorizado y revalidado por conveniencia derecho, a intervalos planificados, por la dirección comercial de la organización o de otro tipo de rol de cuentas o función con el apoyo de pruebas para demostrar la organización se adhiere a la regla del mínimo privilegio basado en la función de trabajo. Para violaciónes de acceso identificados, remediación debe seguir las políticas y procedimientos de acceso de usuarios establecida.	Ok	Ok	Ok
De identidades y accesos Gestión de revocación de acceso de usuarios	TENGO 11	Oportuna de aprovisionamiento (revocación o modificación) de acceso de los usuarios a las aplicaciones propiedad organizativamente-o gestionados (físicos y virtuales) de datos y sistemas de infraestructura, y los componentes de la red, se llevará a cabo de acuerdo con las políticas y procedimientos establecidos y se basa en el cambio de usuario en el estado (por ejemplo, la terminación del empleo u otra relación de negocios, cambio de trabajo, o transferencia). A petición, el proveedor deberá informar al cliente (arrendatario) de estos cambios, especialmente si los datos del cliente (arrendatario) se utiliza como parte del servicio y / o cliente (arrendatario) tiene algo de responsabilidad compartida a través de la implementación del control.	Ok	Ok	Ok
Las credenciales de ID de usuario de administración de identidades y accesos	TENGO 12	credenciales (arrendatario) de cuentas de usuarios corporativos o los internos serán restringidos de acuerdo con el siguiente, lo que garantiza la identidad adecuada, el derecho y la gestión de acceso y de acuerdo con las políticas y procedimientos establecidos: • Aplicación de la comprobación de confianza Identidad y Servicio-al-servicio (API) e interoperabilidad procesamiento de la información (por ejemplo, SSO y Federación) • cuenta de administración de credenciales del ciclo de vida de ejemplificación a través de revocación • credencial de cuenta y / o identidad de tienda de minimización o reutilización cuando sea posible • La adhesión a la industria aceptable y / o reguladora compatible con la autenticación, autorización y contabilidad (AAA) normas (por ejemplo, / de múltiples factores fuerte, expireable, no compartido secretos de autenticación)	Ok	Ok	Ok
Programas de utilidad de identidades y accesos Access Management	TENGO 13	programas de utilidad capaz de sistema potencialmente primordial, objeto, de red, la máquina virtual, y los controles de aplicación estarán restringidas.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Infraestructura y registro de auditoría de seguridad de la virtualización / Detección de Intrusos	IVS-01	Se requieren mayores niveles de aseguramiento para la protección, conservación y gestión del ciclo de vida de los registros de auditoría, la adhesión a las obligaciones de cumplimiento legal, estatutaria o reglamentaria aplicable y proporcionar acceso de usuario única responsabilidad de detectar comportamientos de la red potencialmente sospechosos y / o presentar anomalías de integridad, y para apoyar capacidad de investigación forense en caso de un fallo de seguridad.	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización de detección de cambios	IVS-02	El proveedor deberá garantizar la integridad de todas las imágenes de máquinas virtuales en todo momento. Cualquier cambio realizado en imágenes de máquinas virtuales que estar registrado y plantearon una alerta independientemente de su estado de ejecución (por ejemplo, inactivo, apagado o en ejecución). Los resultados de un cambio o movimiento de una imagen y la posterior validación de la integridad de la imagen debe estar inmediatamente disponible para los clientes a través de métodos electrónicos (por ejemplo, portales o alertas).	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización de sincronización de reloj	IVS-03	A fiable y mutuamente acordado fuente horaria externa se utiliza para sincronizar los relojes del sistema de todos los sistemas de procesamiento de información pertinentes para facilitar el rastreo y la reconstitución de líneas de tiempo de actividad.	Ok	Ok	Ok
Documentación del Sistema de Información de Seguridad de la Infraestructura y Virtualización	IVS-04	La disponibilidad, la calidad y la capacidad y los recursos adecuados deberán planearse, prepararse y midieron para proporcionar el rendimiento requerido del sistema de conformidad con las obligaciones de cumplimiento legal, estatutarias y reglamentarias. Las proyecciones de las futuras necesidades de capacidad se realizarán para mitigar el riesgo de sobrecarga del sistema.	Ok	Ok	Ok
Gestión de vulnerabilidad de la Infraestructura y seguridad de la virtualización	IVS-05	Los ejecutores deberán asegurarse de que las herramientas o servicios de evaluación de la vulnerabilidad de seguridad acomodar las tecnologías de virtualización utilizadas (por ejemplo, la virtualización conscientes).	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización Red de Seguridad	IVS-06	Los entornos de red e instancias virtuales estarán diseñados y configurados para restringir y controlar el tráfico entre conexiones seguros y no seguros. Estas configuraciones serán revisados por lo menos anualmente, y apoyadas por una justificación documentada para el uso de todos los servicios permitidos, protocolos, puertos, y por los controles de compensación.	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización del sistema operativo endurecimiento y base controla	IVS-07	Cada sistema operativo se endurece para proporcionar sólo necesarias puertos, protocolos y servicios para satisfacer las necesidades del negocio y tienen lugar en el apoyo a los controles técnicos, tales como: antivirus, presentar supervisión de la integridad, y el registro como parte de su estándar de acumulación de operación de línea de base o plantilla.	Ok	Ok	Ok
Infraestructura y virtualización de entornos de producción Seguridad / No Producción	IVS-08	entornos de producción y de no producción deben estar separados para evitar el acceso o cambios en los activos de información no autorizada. La separación de los ambientes puede incluir: cortafuegos de inspección de estado, dominio / fuentes de autenticación reino, y la segregación clara de funciones para el personal que acceden a estos ambientes, como parte de sus obligaciones de trabajo.	N/A	N/A	N/A
Infraestructura y seguridad de la virtualización Segmentación	IVS-09	Multi-arrendatario de propiedad organizativamente o aplicaciones (físicos y virtuales) logró, y el sistema de infraestructura y componentes de red, se deben diseñar, desarrollar, desplegar y configurado de tal manera que el proveedor y el cliente (arrendatario) el acceso del usuario está segmentado adecuadamente a los demás usuarios de inquilinos, en base a las siguientes consideraciones: • las políticas y procedimientos establecidos • el aislamiento de los activos críticos de negocio y / o información confidencial del usuario, y las sesiones de ese mandato controles internos más fuertes y altos niveles de garantía • el cumplimiento de las obligaciones de cumplimiento legales, estatutarias y reglamentarias	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización VM Seguridad - Protección de Datos	IVS-10	Asegurado y canales de comunicación cifrados se utilizarán cuando la migración de servidores físicos, aplicaciones o datos a los servidores virtualizados y, cuando sea posible, deberá utilizar una red segregada de redes a nivel de producción para tales migraciones.	N/A	N/A	N/A

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Infraestructura y seguridad de la virtualización de hipervisor Endurecimiento	IVS-11	El acceso a todas las funciones de gestión del hipervisor o consolas de administración para sistemas de alojamiento de sistemas virtualizados estará restringido al personal basada en el principio de privilegios mínimos y apoyado a través de controles técnicos (por ejemplo, la autenticación, pistas de auditoría, filtrado de direcciones IP, de dos factores cortafuegos, y TLS comunicaciones encapsulados a las consolas administrativos).	Ok	Ok	Ok
Infraestructura y seguridad de la virtualización de seguridad inalámbrica	IVS-12	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para proteger los entornos de red inalámbrica, incluyendo las siguientes: cortafuegos • perimetrales implementados y configurados para restringir el tráfico • La configuración de seguridad no autorizadas habilitados con una fuerte encriptación para la autenticación y la transmisión, en sustitución de proveedor ajustes por defecto (por ejemplo, claves de cifrado, contraseñas y cadenas de comunidad SNMP) • el acceso del usuario a los dispositivos de red inalámbricos restringido al personal autorizado • la capacidad de detectar la presencia de dispositivos de red no autorizados (rogue) inalámbrico de desconexión oportuna de la red	Ok	Ok	Ok
Infraestructura y arquitectura de seguridad de red de virtualización	IVS-13	diagramas de arquitectura de red deberán identificar con claridad los entornos de alto riesgo y los flujos de datos que pueden tener impactos de cumplimiento legal. Las medidas técnicas se aplicarán y se aplicarán las técnicas de defensa en profundidad (por ejemplo, análisis profunda de paquetes, el acelerador de tráfico, y negro-Holing) para la detección y respuesta oportuna a ataques asociados con la entrada anómala o los patrones de tráfico de egreso (por ejemplo, basados en red, MAC spoofing y ataques de envenenamiento de ARP) y / o (DDoS) distribuidos de denegación de servicio.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Interoperabilidad y portabilidad de las API	API-01	El proveedor deberá usar APIs abiertos y publicados para asegurar el apoyo para la interoperabilidad entre componentes y facilitar la migración de aplicaciones.	Ok	Ok	Ok
Solicitud Interoperabilidad y portabilidad de datos	API-02	Todos los datos estructurados y no estructurados estarán disponibles para el cliente y que se les proporciona a pedido en un formato estándar de la industria (por ejemplo, .doc, .xls, .pdf, registros y archivos planos).	Ok	Ok	Ok
Interoperabilidad y portabilidad Política y Legal	API-03	Políticas, procedimientos, y mutuamente acordados disposiciones y / o términos se establecen para satisfacer los requerimientos del cliente (arrendatario) para la aplicación de servicio a servicio (API) y la información de interoperabilidad de procesamiento, y portabilidad para el desarrollo de aplicaciones y el intercambio de información, el uso, y persistencia integridad.	Ok	Ok	Ok
Protocolos de red de Interoperabilidad y portabilidad	API-04	El proveedor deberá utilizar segura (por ejemplo, el texto no clara y autenticados) protocolos de red estandarizados para la importación y exportación de datos y para gestionar el servicio, y deberá hacer un documento a disposición de los consumidores (inquilinos) que detalla los estándares de interoperabilidad y portabilidad relevantes que estan involucrados.	Ok	Ok	Ok
Interoperabilidad y portabilidad de virtualización	API-05	El proveedor deberá utilizar una plataforma de virtualización reconocido por la industria y los formatos estándar de virtualización (por ejemplo, OVF) para ayudar a garantizar la interoperabilidad, y no tendrá cambios documentados personalizados hechos a cualquier hipervisor en uso y todos los ganchos específicos de la solución de virtualización disponibles para revisión del cliente.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Mobile Security Anti-Malware	MOS-01	formación de conciencia anti-malware, específica para dispositivos móviles, se incluirá en la formación de conciencia de seguridad de la información del proveedor.	Ok	Ok	Ok
Tiendas aplicación de seguridad móvil	MOS-02	Una lista documentada de las tiendas de aplicaciones aprobadas se ha definido como aceptable para dispositivos móviles que acceden o almacenamiento proveedor de datos administrado.	Ok	Ok	Ok
Aplicaciones autorizadas Mobile Security	MOS-03	La empresa debe tener una política documentada que prohíbe la instalación de aplicaciones no autorizadas o solicitudes aprobadas no han sido obtenidos a través de una tienda de aplicaciones previamente identificado.	Ok	Ok	Ok
Mobile Security software aprobado para BYOD	MOS-04	La política de BYOD y la formación que apoya conciencia establece claramente las solicitudes aprobadas, las tiendas de aplicaciones y extensiones de aplicaciones y plugins que se pueden utilizar para el uso BYOD.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Conciencia de la seguridad móvil y Formación	MOS-05	El proveedor debe tener una política de dispositivo móvil documentado que incluye una definición documentado para los dispositivos móviles y el uso aceptable y requisitos para todos los dispositivos móviles. El proveedor deberá publicar y comunicar la política y los requisitos de seguridad a través del conocimiento de la empresa y programa de entrenamiento.	Ok	Ok	Ok
Servicios de seguridad en la nube móvil basado	MOS-06	Todos los servicios basados en la nube utilizadas por los dispositivos móviles de la empresa o BYOD deberán ser previamente aprobados para el uso y el almacenamiento de los datos de negocio de la empresa.	Ok	Ok	Ok
Compatibilidad Mobile Security	MOS-07	La empresa debe tener un proceso de validación de la aplicación que se ha documentado la prueba de dispositivo móvil, el sistema operativo y los problemas de compatibilidad de aplicaciones.	Ok	Ok	Ok
Mobile Security Device Elegibilidad	MOS-08	La política BYOD definirá los requisitos de elegibilidad del dispositivo y para permitir el uso de BYOD.	Ok	Ok	Ok
Mobile Security inventario de dispositivos	MOS-09	Un inventario de todos los dispositivos móviles que se utilizan para almacenar datos de la empresa y el acceso deberán ser cuidado y mantenido. Todos los cambios en el estado de estos dispositivos (es decir, el sistema operativo y los niveles de parches, de estado perdido o fuera de servicio, y a los que el dispositivo se asigna o aprobado para el uso (BYOD)) se incluirán para cada dispositivo en el inventario.	Ok	Ok	Ok
Gestión de dispositivos de protección móvil	MOS-10	Una solución de gestión centralizada, el dispositivo móvil se desplegará a todos los dispositivos móviles permitidos para almacenar, transmitir, o datos de proceso del cliente.	Ok	Ok	Ok
Mobile Security Encryption	MOS-11	La política dispositivo móvil deberá exigir el uso de cifrado o bien para todo el dispositivo o para los datos identificados como sensibles en todos los dispositivos móviles, y deberá ser ejecutada a través de controles de la tecnología.	Ok	Ok	Ok
Mobile Security Jailbreaking y enraizamiento	MOS-12	La política dispositivo móvil prohibirán la elusión de los controles integrados de seguridad en dispositivos móviles (por ejemplo, jailbreaking o rooting) y deberá hacer valer la prohibición a través de controles de detección y prevención en el dispositivo oa través de un sistema de gestión centralizada de dispositivos (por ejemplo, administración de dispositivos móviles).	Ok	Ok	Ok
Mobile Security Legal	MOS-13	La política BYOD incluye la clarificación de idioma para la expectativa de privacidad, los requisitos para litigios, e-discovery y retenciones legales. La política BYOD deberá indicar claramente las expectativas en cuanto a la pérdida de datos externos de la empresa en el caso de que una limpieza del dispositivo que se requiere.	Ok	Ok	Ok
Móvil de la pantalla de bloqueo de seguridad	MOS-14	BYOD y / o dispositivos de propiedad de la compañía están configurados para requerir una pantalla de bloqueo automático, y el requisito serán ejecutadas a través de controles técnicos.	N/A	N/A	N/A
Sistemas operativos de seguridad móvil	MOS-15	Los cambios en los sistemas operativos de dispositivos móviles, los niveles de parches, y / o aplicaciones serán administrados a través de procesos de gestión del cambio de la compañía.	N/A	N/A	N/A
Mobile Security contraseñas	MOS-16	Las políticas de contraseñas, aplicables a los dispositivos móviles, se documentarán y se hacen cumplir a través de controles técnicos en todos los dispositivos de la empresa o dispositivos aprobados para el uso de BYOD, y prohibirán el cambio de contraseña / PIN longitudes y los requisitos de autenticación.	N/A	N/A	N/A
Política de Seguridad Móvil	MOS-17	La política de dispositivo móvil deberá requerir que el usuario BYOD para realizar copias de seguridad de datos, prohibir el uso de tiendas de aplicaciones no aprobadas, y requieren el uso de software anti-malware (donde compatible).	N/A	N/A	N/A
Mobile Security borrado remoto	MOS-18	Todos los dispositivos móviles cuyo uso se permite a través del programa BYOD empresa o un dispositivo móvil asignado por la empresa deberán permitir el borrado remoto de la compañía de TI corporativa o tendrá todos los datos proporcionados por la compañía limpiadas con las empresas de TI de la empresa.	N/A	N/A	N/A
Parches de Seguridad Mobile Security	MOS-19	dispositivos móviles que se conectan a las redes corporativas, o almacenar y acceder a información de la compañía, deberán permitir el software remoto validación de la versión / parche. Todos los dispositivos móviles se tienen los últimos parches relacionados con la seguridad disponibles instaladas después de la liberación en general por el fabricante del dispositivo o soporte y el personal de TI autorizado será capaz de realizar estas actualizaciones de forma remota.	N/A	N/A	N/A
Seguridad Los usuarios móviles	MOS-20	La política BYOD deberá aclarar los sistemas y servidores con autorización para el uso o acceso en un dispositivo habilitado para BYOD.	N/A	N/A	N/A

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Mantenimiento Gestión de incidentes de seguridad, E-Discovery, y la nube Forense Contacto / Autoridad	SEF-01	Puntos de contacto de las autoridades pertinentes de regulación, aplicación de la ley nacional y local, y otras autoridades legales jurisdiccionales deben ser mantenidos y actualizados periódicamente (por ejemplo, el cambio en el alcance impactado y / o un cambio en ninguna obligación de cumplimiento) para asegurar los enlaces directos de cumplimiento han sido establecido y estar preparados para una investigación forense que requiere un compromiso rápido con la policía.	Ok	Ok	Ok
Gestión de incidentes de seguridad, E-Discovery, y la nube Forense Gestión de Incidencias	SEF-02	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para triaje eventos relacionados con la seguridad y garantizar la gestión de incidencias oportuna y completa, de acuerdo con las políticas de gestión de servicios de TI y los procedimientos establecidos.	Ok	Ok	Ok
Gestión de incidentes de seguridad, E-Discovery, y la nube Forense de notificación de incidentes	SEF-03	el personal de la fuerza de trabajo y las relaciones de trabajo, externos deberán ser informados de sus responsabilidades y, si es requerida, deberá dar su consentimiento y / o contractualmente de acuerdo en reportar todos los eventos de seguridad de la información en el momento oportuno. eventos de seguridad de la información se comunicarán a través de canales de comunicación predefinidos en el momento oportuno adherirse a las obligaciones de cumplimiento legal, estatutaria, o reglamentarias aplicables.	Ok	Ok	Ok
Gestión de incidentes de seguridad, E-Discovery, y la nube Forense de Respuesta a Incidentes Preparación Legal	SEF-04	procedimientos forenses adecuadas, incluyendo la cadena de custodia, son necesarios para la presentación de pruebas para apoyar el potencial de acciones legales sujetos a la jurisdicción pertinente después de un incidente de seguridad informática. Tras la notificación, los clientes y / u otros socios comerciales externos afectados por un fallo de seguridad, tendrán la oportunidad de participar como es legalmente permisible en la investigación forense.	Ok	Ok	Ok
Gestión de incidentes de seguridad, E-Discovery, y la nube Forense de Respuesta a Incidentes de métricas	SEF-05	Mecanismos se ponen en marcha para monitorear y cuantificar los tipos, volúmenes y costos de los incidentes de seguridad de la información.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Gestión de la cadena de suministro, transparencia, rendición de cuentas y calidad de los datos e Integridad	STA-01	Los proveedores deben inspeccionar, dar cuenta de, y trabajar con sus socios de la cadena de suministro en la nube para corregir errores de calidad de datos y los riesgos asociados. Los proveedores deben diseñar e implementar controles para mitigar y contener los riesgos de seguridad de datos a través de la separación de funciones adecuada, acceso basado en roles, y el acceso con privilegios mínimos para todo el personal dentro de su cadena de suministro.	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia, rendición de cuentas e incidentes de informes	STA-02	El proveedor deberá hacer que la información de incidentes de seguridad disponible para todos los clientes y los proveedores afectados periódicamente a través de medios electrónicos (por ejemplo, portales).	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia y rendición de cuentas de red / servicios de infraestructura	STA-03	Críticos para el negocio o cliente (arrendatario) impactando diseños de aplicaciones y sistema de sistema de interfaz (físicos y virtuales) (API) y las configuraciones y red de infraestructura y componentes de sistemas, deberá estar diseñado, desarrollado y desplegado de acuerdo con el acuerdo mutuo sobre el servicio y las expectativas de nivel de capacidad, así como de TI de gobierno y de gestión de servicios políticas y procedimientos.	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia y rendición de cuentas de proveedores evaluaciones internas	STA-04	El proveedor deberá llevar a cabo evaluaciones internas anuales de conformidad con, y la eficacia de sus políticas, procedimientos y medidas de apoyo y métricas.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Gestión de la cadena de suministro, la transparencia, la rendición de cuentas y la oferta de la cadena Acuerdos	STA-05	acuerdos de la cadena de suministro (por ejemplo, SLA) entre proveedores y clientes (arrendatarios) contendrán al menos la siguiente mutuo acuerdo disposiciones y / o términos: • Alcance de la relación de negocios y servicios ofrecidos (por ejemplo, al cliente (arrendatario) de adquisición de datos, el intercambio y el uso, conjuntos de características y funcionalidad, personal y red de infraestructura y componentes de sistemas para la prestación de servicios y soporte, funciones y responsabilidades del proveedor y el cliente (arrendatario) y eventuales relaciones de negocio subcontratadas o externalizadas, ubicación geográfica física de los servicios alojados, y cualquiera de los conocidos reguladora consideraciones de cumplimiento) • requisitos de seguridad de la información, el proveedor y el cliente (arrendatario) puntos de contacto principales para la duración de la relación comercial,y las referencias a los procesos detallados de apoyo y relevantes de negocio y medidas técnicas de ejecución para que efectivamente gobierno, gestión de riesgos, aseguramiento y obligaciones de cumplimiento legal, legales y reglamentarios de todas las relaciones comerciales impactado • Notificación y / o pre-autorización los cambios controlados por el proveedor con el cliente (arrendatario) impactos • la notificación oportuna de un incidente de seguridad (o incumplimiento de confirmación) a todos los clientes (inquilinos) y otras relaciones comerciales afectados (es decir, hacia arriba y corriente abajo cadena de suministro impactado) • Evaluación y verificación independiente del cumplimiento de disposiciones y / o términos del contrato (por ejemplo, la certificación aceptable para la industria, el informe de auditoría de certificación,o formas equivalentes de aseguramiento) sin que presenta un riesgo de negocio inaceptable de la exposición a la organización siendo evaluados • Caducidad de la relación de negocios y el tratamiento de cliente (arrendatario) de datos impactados • Cliente (inquilino) aplicación de servicio a servicio (API) y datos requisitos de	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia y la cadena de suministro de Responsabilidad de Gobierno Críticas	STA-06	Proveedores revisará la gestión de riesgos y los procesos de gobierno de sus socios para que las prácticas son coherentes y alineadas para dar cuenta de los riesgos heredados de otros miembros de la cadena de suministro nube de dicho socio.	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia, la rendición de cuentas y el suministro de métricas de la cadena	STA-07	Las políticas y procedimientos se aplicarán para asegurar el examen coherente de acuerdos de servicios (por ejemplo, SLA) entre los proveedores y clientes (inquilinos) a través de la cadena de suministro correspondiente (aguas arriba / aguas abajo). Los exámenes se realizan al menos anualmente e identificar cualquier no conformidad con los acuerdos establecidos. Los comentarios deben dar lugar a acciones para abordar los conflictos de nivel de servicio o inconsistencias que resultan de relaciones con los proveedores dispares.	Ok	Ok	Ok
Gestión de la cadena de suministro, Transparencia y Evaluación de Terceros Responsabilidad	STA-08	Los proveedores deben asegurar la seguridad de la información razonable a través de su cadena de suministro de información mediante la realización de una revisión anual. La revisión debe incluir todos los socios / terceros proveedores en los que la cadena de suministro de información depende.	Ok	Ok	Ok
Gestión de la cadena de suministro, la transparencia, la rendición de cuentas y auditorías de terceros	STA-09	proveedores de servicios de terceros deberán demostrar el cumplimiento de seguridad de la información y la confidencialidad, control de acceso, las definiciones de servicios y acuerdos de nivel de suministro incluidos en los contratos de terceros. informes de terceros, registros y servicios deberán someterse a auditoría y revisión al menos cada año para gobernar y mantener el cumplimiento de los acuerdos de prestación de servicios.	Ok	Ok	Ok

dominio de control	CCM V3.0 Control de ID	Especificación de control Actualización	Google	Amazon	Azure
Amenaza y la vulnerabilidad de administración Anti-Virus / software malicioso	TVM-01	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para evitar la ejecución de malware en los dispositivos de punto final usuario propiedad organizativamente-o gestionados (es decir, las estaciones de trabajo emitidos, ordenadores portátiles y dispositivos móviles) y la red de infraestructura de TI y componentes de los sistemas.	Ok	Ok	Ok
Gestión de amenazas y vulnerabilidad vulnerabilidad / Patch Management	TVM-02	Se establecerán políticas y procedimientos y procesos de apoyo y medidas técnicas implementadas, para la detección oportuna de vulnerabilidades en las aplicaciones de propiedad organizativamente-o gestionados, red de infraestructura y componentes del sistema (por ejemplo, evaluación de la vulnerabilidad de la red, pruebas de penetración) para asegurar la eficiencia de la seguridad implementada controles. Se utilizará un modelo basado en el riesgo para priorizar la solución de vulnerabilidades identificadas. Los cambios serán administrados a través de un proceso de gestión del cambio para todos los parches proporcionados por los proveedores, cambios de configuración, o cambios en el software desarrollado internamente de la organización. A pedido,	Ok	Ok	Ok
De amenazas y vulnerabilidades Código Móvil de Gestión	TVM-03	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para evitar la ejecución de código móvil no autorizado, definido como software transferida entre los sistemas a través de una red de confianza o desconocidas y se ejecutan en un sistema local sin necesidad de instalación explícita o ejecución por parte del destinatario, en los dispositivos de punto final de usuario propiedad organizativamente-o gestionados (por ejemplo, estaciones de trabajo emitidos, portátiles y dispositivos móviles) y la red de infraestructura de TI y componentes de sistemas.	Ok	Ok	Ok

Tabla 4: Controles específicos SECaaS por proveedor versus CCM

7 CONCLUSIONES

- Al momento de establecer un marco de referencia para la nube, el cual cumpla con la legislación colombiana de protección de datos 1581 de 2012, lo mejor es partir de un diseño con componentes claramente definidos desde el punto de vista de su función y con interfaces entre componentes basadas en estándares. Esto facilita reemplazar un componente por otro a medida que surgen nuevas ofertas en el mercado o avanza la tecnología. El resultado suele ser mejor desempeño, costos más bajos y mayor facilidad de evolución. El estándar construido por la Cloud Security Alliance resulta útil en la realización de dichos contrastes.

- Aunque las especificaciones vertidas en este documento están basadas en selecciones de productos concretos (soluciones de nube) considerados los más adecuados para la situación, nuestro marco de referencia minimiza la dependencia del esquema de seguridad en productos específicos. En particular, cualquier repositorio en la nube o servicio de almacenamiento distribuido, que ofrezcan y sean configurados con un nivel equivalente o mayor de seguridad listados en nuestro marco de referencia, tras su verificación mediante pruebas de seguridad, pueden ser utilizados para cumplir con las exigencias de la ley colombiana de protección de datos 1581 de 2012.

- Al migrar hacia plataformas en la nube se ingresa a un ciclo acelerado de innovación continua. Guardando la estabilidad y prudencia tecnológica requerida para una plataforma de servicios en la nube es viable diseñar la arquitectura de seguridad tomando en cuenta la evolución de tecnología y servicios previsibles, para dar la opción de mejoras en costos y servicios ofrecidos. Nuestro marco de referencia permite acercarse a ese propósito evaluando las tres soluciones con mayor grado de madurez hasta el momento, también indica cuales requisitos previstos en la legislación colombiana de protección de datos 1581 de 2012 requieren un control de seguridad digital complementario.

8 TRABAJOS FUTUROS

A partir de esta guía se pueden desarrollar:

- estudios de profundización de la ley de protección de datos en Colombia y a nivel mundial,
- investigar los ítems que han impedido el cumplimiento cabal de la ley de protección de datos en Colombia por parte de los proveedores de servicios en la nube.
- Definir un esquema que permita la contratación con responsabilidades contractuales con los proveedores de servicios en la nube en Colombia para dar cumplimiento a la ley de protección de datos.
- Definir una solución de infraestructura hibrida, la cual combine tecnologías de seguridad basadas en la nube, apoyada con soluciones de infraestructura propietaria para el cumplimiento de la ley de protección de datos en Colombia.
- Realizar la normalización de la ley de protección de datos con el nuevo reglamento general de protección de datos de la unión europea.

9 REFERENCIAS

AEPD. (2014a). Guía para una Evaluación de Impacto en la Protección de Datos Personales, 71. Retrieved from https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

AEPD. (2014b). Guía para una Evaluación de Impacto en la Protección de Datos Personales, 71.

Agencia Española de Protección de Datos. (n.d.). Paises proteccion de datos en el mundo. Retrieved from http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

Akamai's State of the Internet / Security Team. (2016). akamai's [state of the internet] / security, *3*, 52. Retrieved from https://content.akamai.com/pg7053-es-soti-security-report.html

Amazon Web Services, I. o sus empresas afiliadas. (n.d.). Seguridad en la Nube - Amazon Web Services (AWS). Retrieved February 10, 2017, from https://aws.amazon.com/es/security/

Areitio, J. (2011). Protección del Cloud Computing en seguridad y privacidad. *Revista Española de Electrónica*, *Mayo*, 42–48.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187–223.

https://doi.org/10.1093/ijlit/ear005

Casasola Robles Mario, Maqueo Ramírez María Solange, Molina Rodríguez Marlon, Moreno González Jimena, & Recio Gayo Miguel. (2014). La nube : nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo. *Centro de Investigaciones Y Docencia Economica A.A.*, 74.

Cloud Security Alliance. (2012). Category 8 // Encryption, (September), 1–28. Retrieved from http://now.dstv.com/livetv/play/0866e73b-6ece-42c9-8b87-68ad31db5847?acc_pg_sec=livetv channel list

Colombia. Congreso de la República. (2009). LEY POSTAL 1369, 22. Retrieved from https://www.mintic.gov.co/portal/604/articles-3708_documento.pdf

Colombia. Congreso de la República. (2012). Ley Estatutaria No. 1581 "por la cual se dictan disposiciones generales para la protección de datos personales". *Superintendencia de Industria Y Comercio*, *ley 1581*, 1–15. https://doi.org/Research Study 292

David López Jiménez. (2013). Computacion en la Nube - Ordenamiento Juridico.

De La Hoz Freyle, J., Carrillo Rincón, E., & Gómez Flórez, L. C. (2014). Memorias organizacionales en la era del almacenamiento en la nube. (Spanish). *Organizational Memories at Cloud Storage Age. (English)*, *18*(40), 115–126. https://doi.org/http://dx.doi.org/10.14483/udistrital.jour.tecnura.2014.2.a09

Đorđević, B. S., Jovanović, S. P., & Timčenko, V. V. (2014). Cloud Computing in Amazon and Microsoft Azure platforms: Performance and service comparison.

In *Telecommunications Forum Telfor (TELFOR), 2014 22nd* (pp. 931–934). https://doi.org/10.1109/TELFOR.2014.7034558

Europea, C. (n.d.). Guía del escudo de la privacidad UE-EE. UU., 1–11. Retrieved from http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

Google. (2016). Security and Compliance on the Google Cloud Platform — Google Cloud Platform. Retrieved February 10, 2017, from https://cloud.google.com/security/

Guenane, F., Nogueira, M., & Serhrouchni, A. (2015). DDOS mitigation cloud-based service. In *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015* (Vol. 1, pp. 1363–1368). https://doi.org/10.1109/Trustcom.2015.531

Hussain, M., & Abdulsalam, H. (2011). SECaaS: security as a service for cloud-based applications. *Proceedings of the Second Kuwait Conference on E-Services and E-Systems - KCESS '11*, 1–4. https://doi.org/10.1145/2107556.2107564

Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication 800-144*, 80. https://doi.org/10.3233/GOV-2011-0271

Joyanes Aguilar, L. (2012). COMPUTACIÓN EN LA NUBE. Notas para una estrategia española en cloud computing. *Revista Del Instituto Español de Estudios Estratégicos*, 89–112. Retrieved from

http://revista.ieee.es/index.php/ieee/article/viewFile/10/8

Mahendiran, A., Saravanan, N., & Sairam, N. (2012). A review on leaders in cloud computing service providers and cloud SQL a case study. *Research Journal of Applied Sciences, Engineering and Technology*, *4*(17), 2926–2933.

Martínez Martínez, R. (2012). Derecho y cloud computing, 8–11. Retrieved from https://dialnet.unirioja.es/servlet/libro?codigo=653445

Microsoft. (n.d.). Microsoft Trust Center | Security overview. Retrieved February 10, 2017, from https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx

Oppenheim, C. (2012). Legislación sobre computación en la nube y negociación de contratos. *El Profesional de La Información*, *21*(5), 453–457. https://doi.org/10.3145/epi.2012.sep.02

Services, A. W., Azure, M., & Platform, G. C. (n.d.). Midiendo a los gigantes del cloud computing empresarial.

Susana Navas Navarro. (2015). Computación en la nube: Big Data y protección de datos personales. *InDret*. Retrieved from http://www.indret.com/pdf/1193_es.pdf

Tobergte, D. R., & Curtis, S. (2013). Cisco, La Seguridad como servicio. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Van Niekerk, B., & Jacobs, P. (2013). Cloud-based security mechanisms for critical

information infrastructure protection. In *IEEE International Conference on Adaptive Science and Technology, ICAST*. https://doi.org/10.1109/ICASTech.2013.6707515

Vazquez-Moctezuma Salvador E. (2015). Tecnología de almacenamiento de información en el ambiente digital. *E-Ciencias de La Información* , *5*(2). https://doi.org/DOI: http://dx.doi.org/10.15517/eci.v5i2.19762

Wang, C., Wang, Q., Ren, K., & Lou, W. J. (2009). Ensuring Data Storage Security in Cloud Computing. *Iwqos: 2009 Ieee 17th International Workshop on Quality of Service*, 37–45\n302. https://doi.org/10.1109/IWQoS.2009.5201385