UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRÍA EN TELECOMUNICACIONES

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE PARA LA EMPRESA "MASIVA" DE LA CIUDAD DE QUITO, CON BASE EN LA NORMA ISO/IEC 27017"

Trabajo de Investigación previo a la obtención del Titulo de

Magíster en Telecomunicaciones

AUTOR:

GEOVANNY XAVIER RUIZ IMBAT

DIRECTOR:

VÍCTOR HUGO BENÍTEZ BRAVO

IBARRA - ECUADOR

2021

I

UNIVERSIDAD TÉCNICA DEL NORTE
INSTITUTO DE POSTGRADO
MAESTRÍA EN TELECOMUNICACIONES

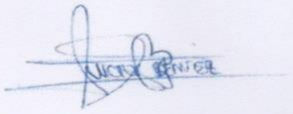
IBARRA - ECUADOR | Instituto de Posgrado

APROBACIÓN DEL TUTOR

Yo, **Víctor Hugo Benítez Bravo**, certifico que el estudiante **Geovanny Xavier Ruiz Imbat** con Cédula Nº 100366464-4 ha elaborado bajo mi tutoría la sustentación del trabajo de grado titulado: **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE PARA LA EMPRESA "MASIVA" DE LA CIUDAD DE QUITO, CON BASE EN LA NORMA ISO/IEC 27017".**

Este trabajo se sujeta a las normas y metodologías dispuestas en el reglamento del título a obtener, por lo tanto, autorizo la presentación a la sustentación para la calificación respectiva.

Ibarra, a los 25 días de octubre de 2021.



MsC. Víctor Hugo Benítez Bravo
CI: 0602990699

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA.

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD	1003664644
APELLIDOS Y NOMBRES	Ruiz Imbat Geovanny Xavier
DIRECCIÓN	Cotacachi
EMAIL	gxruiz@utn.edu.ec
TELÉFONO	0996915911
DATOS DE LA OBRA	
TÍTULO	Sistema de gestión de seguridad de la información de servicios en la nube para la empresa “Masiva” de la ciudad de Quito, con base en la norma ISO/IEC 27017
AUTOR	Geovanny Xavier Ruiz Imbat
FECHA: DD/MM/AAAA	25 días de octubre de 2021
PROGRAMA DE POSGRADO	Maestría en Telecomunicaciones
TÍTULO POR EL QUE OPTA	Magister en Telecomunicaciones
TUTOR	MsC. Víctor Hugo Benítez Bravo

2. CONSTANCIA

El autor Geovanny Xavier Ruiz Imbat, manifiesta que la obra objeto de la presente autorización es original y se la desarrollo, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que se asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad, en caso de reclamación por parte de terceros.

Ibarra, a los 25 días de octubre de 2021

El AUTOR

Geovanny Xavier Ruiz Imbat
CI: 1003664644

DEDICATORIA

Dedico el presente trabajo de titulación a mi familia quienes fueron un pilar fundamental para superarme cada día, agradezco por cada palabra, consejo y ayuda que me brindaron en cada instancia de mi vida, lo que me condujo poco a poco a cumplir esta meta tan anhelada.

RECONOCIMIENTO

Agradezco a Dios, por guiarme en el camino correcto y darme la perseverancia necesaria para cumplir esta meta profesional.

A mi familia por el apoyo fundamental que me brindaron para poder cumplir el objetivo propuesto.

Agradezco a mi Docente Tutor Ing. Víctor Hugo Benítez Bravo, por todo el apoyo brindado para la ejecución del presente trabajo. Al Ing. Edwin Marcelo Jurado Ávila por compartir desinteresadamente sus amplios conocimientos y brindar su ayuda y amplia experiencia hacia mi persona.

Y una mención especial a la Empresa Masiva de la cuidad de Quito, por todo el apoyo otorgado para la ejecución del proyecto.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE
INSTITUTO DE POSGRADO
PROGRAMA DE MAESTRÍA EN TELECOMUNICACIONES

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE PARA LA EMPRESA "MASIVA" DE LA CIUDAD DE QUITO, CON BASE EN LA NORMA ISO/IEC 27017"

Autor: Ing. Geovanny Xavier Ruiz Imbat.
Tutor: Ing. Víctor Hugo Benítez MSc.
Año: 2021

RESUMEN

El presente proyecto de investigación tiene como objetivo principal diseñar un Sistema de Gestión de Seguridad de la Información de Servicios en la nube (SGSI-C) para "Masiva", empresa ecuatoriana dedicada a la prestación de servicios y aplicaciones en la nube. Para ello, se tomaron como base las pautas establecidas en la norma de buenas prácticas ISO/IEC 27017 que hacen énfasis en la aplicación de dominios de seguridad, políticas, gestión del recurso humano, controles de acceso y evaluación de riesgos.

Se comienza realizando un análisis de los riesgos y vulnerabilidades actuales a través de la utilización de herramientas de recolección de datos como entrevistas y observación directa de campo siguiendo una metodología de investigación de tipo exploratoria con un enfoque descriptivo por cuanto se analizó el estudio de caso específico de la empresa en cuestión.

Posteriormente se llevó a cabo el planteamiento del SGSI-C con las políticas de acuerdo a los criterios de los estándares tomados en cuenta aplicables según las necesidades de la organización, para finalmente realizar su validación a través de una matriz de correlación que señala cada documento que debiera cumplir la organización para gestionar correctamente la seguridad de la información de sus servicios en la nube.

Palabras clave: SGSI, computación en la nube, ISO 27017, seguridad.

UNIVERSIDAD TÉCNICA DEL NORTE
INSTITUTO DE POSGRADO
PROGRAMA DE MAESTRÍA EN TELECOMUNICACIONES

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE PARA LA EMPRESA "MASIVA" DE LA CIUDAD DE QUITO, CON BASE EN LA NORMA ISO/IEC 27017"

Autor: Ing. Geovanny Xavier Ruiz Imbat.
Tutor: Ing. Víctor Hugo Benítez MSc.
Año: 2021

ABSTRACT

The main objective of this research project is to design an Information Security Management System for Cloud Services (ISMS-C) for "Masiva", an Ecuadorian company dedicated to providing services and applications in the cloud. For this, the guidelines established in the ISO / IEC 27017 good practice standard were taken as a basis, which emphasize the application of security domains, policies, human resource management, access controls and risk assessment.

It begins by conducting an analysis of current risks and vulnerabilities through the use of data collection tools such as interviews and direct field observation, following an exploratory research methodology with a descriptive approach, since the specific case study was analyzed. of the company in question.

Subsequently, the approach of the ISMS-C was carried out with the policies according to the criteria of the standards taken into account according to the needs of the organization, to finally carry out its validation through a correlation matrix that indicates each document that should meet the organization to properly manage the information security of its cloud services.

***Keywords*:** ISMS, cloud computing, ISO 27017, security.

CAPITULO I
EL PROBLEMA

1.1. Problema de investigación

La evolución de las tecnologías de información y comunicación dio lugar al crecimiento exponencial de la computación en la nube, haciendo que los proveedores de servicios de tecnologías de la información orienten su objetivo de negocio hacia las prestaciones cloud, reduciendo CAPEX, OPEX, costos de hardware, entre otros (Beltrán & Sevillano, 2013).

De esta manera surge Masiva, una empresa dedicada a la prestación de servicios relacionados con tecnologías de la información, consultoría y soluciones en la nube con matriz en la ciudad de Quito, destacándose en el levantamiento de plataformas cloud para envío y gestión de mensajes de texto (SMS), correos electrónicos (SMTP), configuración y gestión de envíos de mensajes transaccionales, software como servicio (SaaS) y plataformas como servicio (PaaS) (MASIVA EC, 2020).

A pesar de los múltiples beneficios que ofrece Masiva, aún existen brechas difíciles de cerrar, relacionadas directamente con los servicios en la nube, debido a lo complicado que se vuelve definir el perímetro de seguridad sobre el que se mueven los datos, esto da lugar a que el inconveniente más importante de resolver, sea garantizar la seguridad y privacidad de los datos, estableciendo claramente los roles de cliente y proveedor. (Sasko, Magdalena, & Marjan, 2015).

Según el informe de datos publicado por Shadow Data Theart Report, el 12% de información que atraviesa la nube es confidencial, el 63% de actividad se cataloga como riesgosa e indica intentos de transferir datos sin autorización, el 11% de aplicaciones de nube empresarial son vulnerables a exploits como Poodle TLS, SSLv3, CRIME, entre otros; en conclusión, la nube avanza, pero no su seguridad (FSA LATAM: Security Business Intellingence, 2016).

Masiva trabaja permanente en cubrir las necesidades de sus clientes, mostrándose como una organización segura y que respalda por sobretodo la información custodiada, por esta razón, es de vital importancia diseñar un sistema de gestión de seguridad de la información en la nube, que permita el control de seguridad para su satisfacción y la de sus clientes, la cual tome en consideración prácticas y códigos de conducta para la protección de información.

1.2. Objetivos de la investigación

1.2.1. Objetivo general

- Diseñar un sistema de gestión de seguridad de la información de servicios en la nube (SGSI-C) para la empresa “Masiva”, proveedora de Software como Servicio (SaaS), con base en la norma ISO/IEC 27017, a fin de garantizar el control de seguridad de la información que maneja esta organización.

1.2.2 Objetivos específicos

- Investigar los tipos de servicios de almacenamiento en la nube, estándares de seguridad en la nube, normativa ISO/IEC 27017, sistemas de seguridad y propuestas relacionadas con el control de seguridad en la nube.

- Analizar la situación actual de la empresa Masiva para identificar las necesidades actuales y brechas de seguridad.

- Desarrollar el sistema de gestión de seguridad de la información de servicios en la nube (SGSI-C) para la empresa “Masiva” de la ciudad de Quito, con base en el código de buenas prácticas ISO/IEC 27017.

- Validar el sistema de gestión de seguridad de la información de servicios en la nube (SGSI-C), a través la utilización de herramientas de recolección de datos, como encuestas, dirigidas al proveedor SaaS y sus clientes potenciales.

1.3. Justificación

El crecimiento exponencial de servicios en la nube ha tenido demasiado auge durante los últimos años; así lo evidencia la publicación realizada por Gartner Forecasts Worldwide Public Cloud, en donde se estima un crecimiento del mercado de la computación en la nube en 81% entre 2018 y 2022 (Gartner, 2019), mientras que, un estudio realizado por la Escuela Politécnica del

Litoral y Microsoft, en Ecuador, acerca de la adopción de computación en la nube, manifiesta que, el 78 % empresas encuestadas reportan el uso de al menos un servicio de computación en la nube (Guerra, 2019), hechos que permiten determinar un gran crecimiento en la adquisición de servicios en la nube por parte de empresas ecuatorianas.

Hoy en día, Masiva tiene una creciente proyección en cuanto a la prestación de servicios de computación en la nube, pues su visión en los próximos años, es convertirse en un referente en el mercado nacional en el sector de las herramientas de comunicación y las TIC; y a medida que se expanda en el campo, los desafíos a los se enfrentará también se incrementarán (MASIVA EC, 2020).

Es por ello que, la carencia de procedimientos y metodologías que permitan salvaguardar la información podrían constituir una rígida barrera para la expansión de Masiva como referente en el ámbito, pues, uno de principales problemas de seguridad en el uso de servicios en la nube es la definición de roles y responsabilidades que da lugar a los controles de seguridad de la información (Nist, 2011).

Con el presente trabajo de investigación se pretende analizar e identificar falencias de seguridad de la información en la nube, en Masiva, una empresa que brinda este tipo de soluciones en cloud, teniendo como base la norma internacional de buenas prácticas ISO/IEC 27017, a fin de abarcar aspectos de seguridad, tales como: gobierno de los datos, controles técnicos y responsabilidades contractuales. Obteniendo como beneficio identificar criterios y

recomendaciones de seguridad que ayuden a la organización, a implementar la seguridad en la computación en la nube con procedimientos y acuerdos de nivel de servicios explícitos.

Esta investigación corresponde a la línea de investigación Desarrollo, aplicación de software, cyber security, además se busca aportar con la misión de la Universidad Técnica del Norte que genera, fomenta, y ejecuta procesos de investigación, de transferencia de conocimientos científicos, tecnológicos y de innovación.

Se enmarca en el en el objetivo 5 del Plan Nacional de Desarrollo 2017-2021, que en su política cita "Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades". (Plan Nacional de Desarrollo , 2017)

CAPÍTULO II

MARCO REFERENCIAL

2.1. Computación en la nube

La computación en la nube o cloud computing es un modelo de negocio mediante el cual la información permanente se almacena en servidores localizados en la red global "internet", ésta se coloca temporalmente en "caché" en los dispositivos finales de usuario como computadoras, celulares, entre otros; en otras palabras, la información que se provee a los clientes es bajo demanda, pudiendo referirse a servicios o infraestructura (Puri, Tiwary, & Shukla, 2019).

El objetivo del cloud computing es optimizar recursos, tanto para proveedores como clientes, ya que utiliza sistemas distribuidos que se implantan gracias a la virtualización, garantizando de esta manera el correcto funcionamiento de diversos servicios simultáneamente, y satisfaciendo la demanda que el mercado requiere bajo el concepto de pago por consumo (Cornejo & Díaz, 2015).

2.1.1. Características de la computación en la nube

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) manifiesta que el cloud computing debe cumplir, al menos, con las siguientes características:

2.1.1.1. Servicio bajo demanda

El cliente está en la capacidad de solicitar y manejar su información por sí mismo, a través de APIs, sin necesidad de un agente externo que le brinde soporte (Ferraiolo, 2016).

2.1.1.2. Compartición de recursos

El cloud computing debe permitir acceder a los recursos almacenados a través de múltiples sesiones de usuario, independientemente de su localización física (Ferraiolo, 2016).

2.1.1.3. Ubicuidad

Los usuarios pueden acceder a los servicios cloud desde cualquier lugar, basta contar con una conexión a internet y un dispositivo final de usuario que le permita utilizar las aplicaciones o servicios contratados (Ferraiolo, 2016).

Esta característica también representa una gran ventaja para los administradores de TI, por cuanto podrían acceder a la infraestructura desde cualquier lugar, siempre y cuando se tomen en consideración controles de acceso previamente configurados.

2.2. Modelos de servicios de computación en la nube

Los modelos de cloud computing se han clasificado principalmente en tres grupos o categorías (véase figura 1): infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).

Figura 1. ***Modelos de cloud computing. IaaS, PaaS and SaaS: The Definitive Guide***

Nota: Tomado de (Martial, 2020)

2.2.1. IaaS

Inicialmente las organizaciones se encargaban de la gestión e implementación de sus recursos de red tanto físicos como lógicos, lo cual requería una inversión inicial, que dependiendo de diversos factores como escalabilidad o tipos de servicio, podría incurrir en elevados gastos de capital (CAPEX) y gastos operativos (OPEX) (Kirsch & Hurwitz, n.d.).

La infraestructura como servicio (IaaS) provee todos los recursos de red necesarios para operar centros de datos, incluyendo su mantenimiento; está dirigida principalmente a administradores de TI, en donde la principal ventaja para el cliente es la escalabilidad, pues tiene la posibilidad de ampliar o reducir su red según sus necesidades, en este tipo se encuentra Amazon Web Services (Marinescu, 2018).

2.2.2. PaaS

Plataforma como servicio es el modelo orientado a desarrolladores de aplicaciones que se preocupan netamente por la construcción de su aplicación, ya que su proveedor es quien se ocupa del almacenamiento y gestión. Un claro ejemplo de PaaS es Jelastic, una plataforma dirigida a desarrolladores, la cual les permite levantar sus aplicaciones con soporte a múltiples lenguajes como java, php, node.js, ruby, Python, entre otros (Cornejo & Díaz, 2015).

2.2.3. SaaS

Software como servicio abarca a cualquier tipo de servicio que está basado en la web, como por ejemplo Gmail, en donde el usuario accede al servicio con el mínimo esfuerzo y control, por cuanto el mantenimiento y gestión de éste, es responsabilidad exclusiva del proveedor (Marinescu, 2018).

La diferencia fundamental entre IaaS, PaaS y SaaS está relacionada al mantenimiento y soporte que proporciona el proveedor; mientras en IaaS el cliente se ocupa de todo, en PaaS solamente gestiona la plataforma, más no el servidor, y en SaaS, los usuarios ni si quiera tienen acceso al software.

2.3. Modelos de despliegue de computación en la nube

La clasificación que se presenta a continuación se fundamenta bajo la característica de “en dónde se encuentra instalada la infraestructura”; de esta forma se tienen nube pública, nube privada y nube híbrida.

2.3.1. Nube pública

Este tipo de nube es la más utilizada por los usuarios por cuanto está disponible para todo público, como es el caso de Google Drive, en donde a través de un correo electrónico y contraseña, se puede acceder a un tipo de almacenamiento que está disponible a cualquier hora y cualquier lugar (Puri et al., 2019).

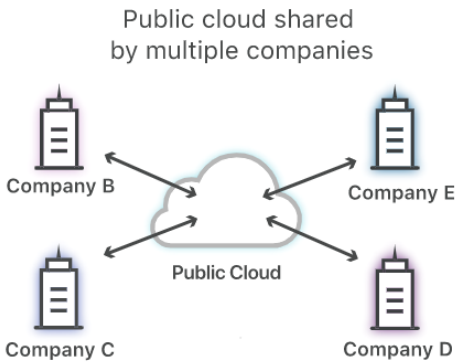


Figura 2. ***Modelo de negocio: nube pública.***

Nota: Tomado de (Cloudfare, 2020)

2.3.2. Nube privada

La nube privada consiste en almacenamientos “dedicados”, está dirigida principalmente a empresas u organizaciones que desean colocar su información de manera privada y no compartirla con el resto de usuarios (Puri et al., 2019). La principal diferencia entre una nube pública y privada

es la compartición del almacenamiento, en la nube pública muchos usuarios hacen uso del mismo almacenamiento mientras que en la nube privada solo el propietario puede hacerlo.

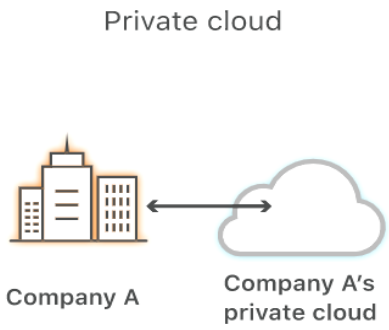


Figura 3. ***Modelo de negocio: nube privada.***

Nota: Tomado de (Cloudfare, 2020)

2.3.3. Nube híbrida

La nube híbrida combina los entornos de nube pública y nube privada, de manera que las empresas se benefician de las ventajas que tienen estos dos tipos de infraestructura cloud, lo que da como resultado, la interoperabilidad de diferentes entornos. El punto de inflexión entre una nube pública y privada es una API, que a través de software se encarga de orquestar las cargas de trabajo (Cabacas, 2018) .

La característica principal y ventaja de una nube híbrida es la escalabilidad horizontal y vertical, esto se traduce a que se pueden añadir unidades de procesamiento, así como asignar recursos a unidades de procesamiento ya existentes.

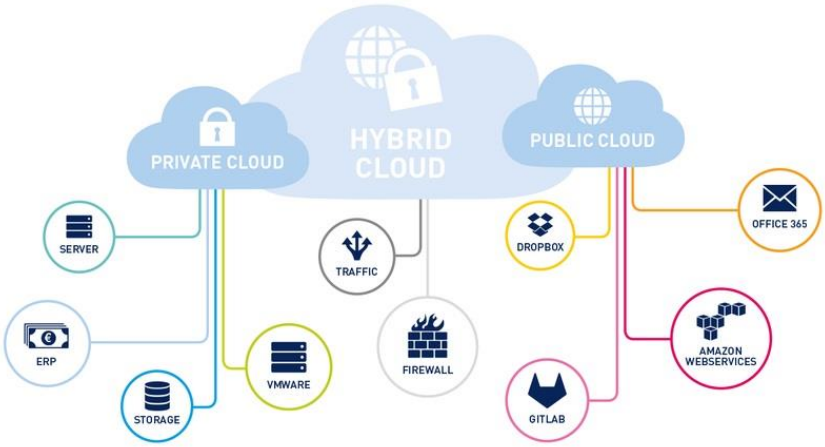


Figura 4. ***Modelo de negocio: nube híbrida.***

Nota: Tomado de (Cabacas, 2018)

2.4. Arquitectura de la computación en la nube

La computación en la nube posee una arquitectura en capas fundamentada en la arquitectura de red, debido a que se utilizan los mismos protocolos, la figura 5 evidencia los cinco niveles definidos:

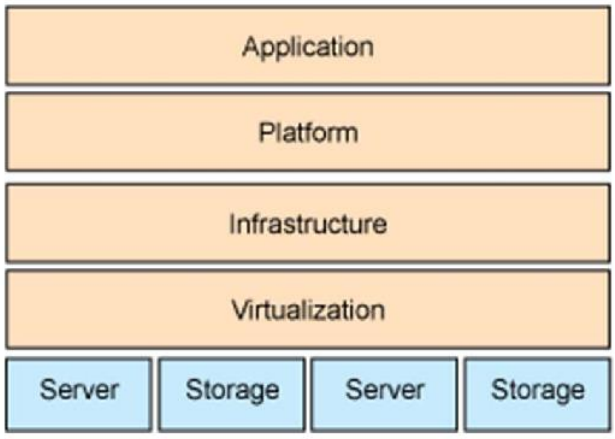


Figura 5. ***Arquitectura de la computación en la nube. Computación en la nube: arquitectura y sistema operativo.***

Nota: Tomado de (Hodan M & Lama A, 2016)

En la capa inferior, de abajo hacia arriba, se encuentran todos los recursos físicos, es decir todo el hardware sobre el que se levanta la infraestructura cloud, estos incluyen: dispositivos de almacenamiento, servidores, redes, equipos de enfriamiento, redundancia en hardware, entre otros.

La segunda capa corresponde a la virtualización, la cual se encarga de la abstracción de los recursos tomados de la capa inferior; en este nivel los recursos se observan como un "servicio".

El siguiente nivel es la capa de infraestructura que se ocupa de orquestar el software de la plataforma como servicio, aquí se pueden encontrar plataformas como OpenStack o CloudStack.

En el cuarto nivel de arquitectura se localizan los componentes de aplicación como servicio, es decir, los módulos en los cuales se implementan las aplicaciones.

Finalmente está la capa de aplicación en la cual se encuentran los servicios basados en la web y el software como servicio; es decir, las aplicaciones que gestiona el usuario final de un modelo de negocio de software como servicio (Joyanes, 2016).

2.5. Seguridad en la nube

Los proveedores actuales de cloud computing enfrentan serios desafíos en cuanto a la protección de datos de sus usuarios, debido a que la computación en la nube abarca distintas tecnologías y políticas de protección de datos, servicios o infraestructuras. La arquitectura de

seguridad tradicional difícilmente se aplica en este tipo de servicios, por cuanto el cliente ya no es el propietario de la infraestructura cloud (Puri et al., 2019).

2.6. Líderes en la industria de prestación de servicios en la nube

La apuesta hacia la computación en la nube ha crecido considerablemente durante los últimos años, haciendo que las grandes industrias destinen sus recursos a la implementación de servicios cloud; en este grupo se pueden encontrar empresas como Amazon, Microsoft, Google, entre otros. Según datos recolectados por el portal Synergy Research Group, los líderes en computación se describen en la figura 5:

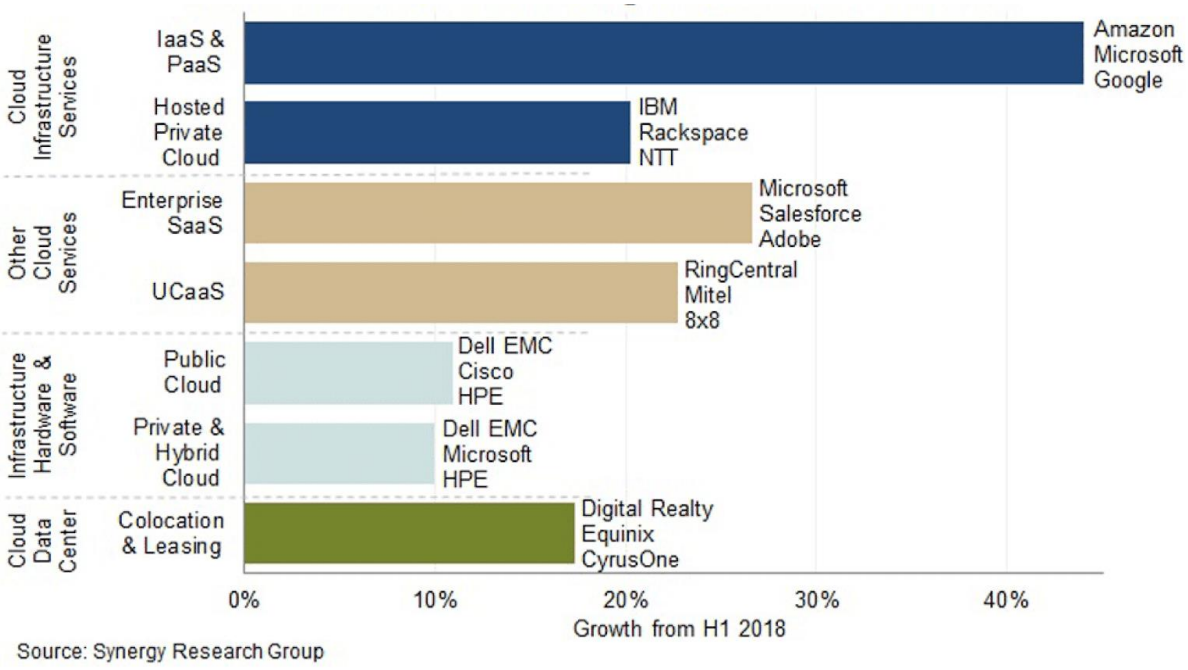


Figura 6. ***Líderes de cloud computing. Cloud Market Growth***

Nota: Tomado de Synergy Research Group.

2.7. Casos de éxito de servicios de computación en la nube

2.7.1. Amazon

Amazon Web Services (AWS) es considerado un pionero de la computación en la nube, por cuanto desde el año 2006 empezó a brindar infraestructura de TI a manera de containers web, lo que actualmente se conoce como computación en la nube. Actualmente, AWS cuenta con centro de datos en Estados Unidos, Japón, Australio, Brasil y Singapur a través de los cuales levantar servicios basados en cloud para todo el mundo.

AWS tiene certificación acorde a los estándares ISO/IEC 27001:2013 (Sistemas Gestión de la Seguridad de la Información), ISO/IEC 27018:2014 (Protección de la Información de Identificación Personal (PII) en Sistemas Cloud) e ISO/IEC 27017:2015 (Directrices para los Controles de Seguridad de la Información Aplicables a la Prestación y el Uso de Servicios en la Nube); Esta certificación la otorgó un agente externo autorizado por la Organización Internacional de Estandarización (ISO) (AWS, 2021a).

AWS expone que seguir las pautas detalladas en los estándares internaciones fue de vital importancia para conseguir una gestión organizacional sólida, en la cual la seguridad en la nube constituye su principal prioridad, sin embargo manifiesta que esta seguridad es compartida entre ellos como “proveedor” y sus “clientes”; así AWS se encarga de la protección global de su infraestructura en la cual se alojan los servicios AWS que cuentan con un mecanismo de gestión de identidades y accesos (IAM / Identity and Access Management) para la administración de recursos dirigido a usuarios individuales o grupos (AWS, 2021b).

Por otro lado, la responsabilidad del cliente depende del tipo de servicio contratado, no obstante siempre será responsable del contenido que aloje en los servicios contratados incluyendo la confidencialidad de sus datos y acatar la normativa vigente de su país (AWS, 2021b).

2.7.2. Microsoft

Windows Azure lanzada en octubre del 2008 es otro líder por excelencia puesto que combina lenguajes de bases de datos como SQL Azure y novedades como .NET Framework y Azure Active Directory en su infraestructura cloud, otorgándose el nombre de Microsof Azure en 2014; cuenta con alrededor de 130 nodos perimetrales con un ancho de banda de 1,6 Pbsp (“Microsoft Azure,” 2021).

En un artículo publicado en su web oficial en enero del año anterior, Azure se exhibe como el primer proveedor de servicios en la nube en obtener una certificación ISO/IEC 27701 (Gestión de la privacidad de la información o Privacy Information Management System PIMS) la cual le ha permitido brindar controles operativos y de administración utilizados a nivel mundial por cuanto dicho estándar comprende una extensión de la norma ISO/IEC 27001 (Gestión de Seguridad de la Información) logrando un marco de regulación para la administración de datos personales incluyendo el Reglamento General de Protección de Datos (GDPR) (Microsoft Azure, 2020).

Azure cuenta con un certificado registrado acorde a la ISO/IEC 27701: 2019 con las bases fundamentales para la administración de servicios como Germany Cloud, Azure Public y Government Cloud establecidos sobre la “Trusted Cloud” que no son nada más que garantías

contractuales de que como proveedor se encargan de la privacidad y confidencialidad de los datos de sus clientes (Microsoft, 2021).

2.7.3. Google

Google Cloud Platform surgió como una mejora a Google Docs en 2012 cambiando su denominación con centros de datos en todo el mundo, no existe un número oficial acerca de ellos, pero en un informe publicado por Google en 2016 manifestó que disponen de alrededor de 2,5 millones de servidores.

Según el portal de Google Cloud los servicios de Chrome, Apigee y Google Workspace cuentan con la certificación ISO/IEC/27001 lo cual lo convierte en un modelo de gestión de seguridad de la información (GCP, 2021).

El documento “Google Cloud Security Whitepapers” describe una visión general de como se estructura la política de seguridad en la infraestructura de google, esta infraestructura brinda a sus clientes un almacenamiento seguro y privacidad de sus datos, que van desde el navegador Chrome, correo electrónico, G Suite y Google Cloud plataforma que pone a disposición varios servicios empresariales. Google se encarga de levantar sus propios centros de datos con niveles sólidos de seguridad que incluyen barreras físicas de acceso pero también gestiona ciertos servidores en centros de datos externos que también cumplen estrictas medidas de seguridad física; para la administración de software se utilizan técnicas criptográficas que permiten la comunicación entre servicios proporcionando abstracción y granularidad, su enfoque de seguridad

no se basa solamente en segmentación LAN o firewall sino que aplican mecanismos de seguridad confidenciales y auditables basados en virtualización (Security Homeland, 2018).

2.8. Organizaciones que proveen estándares de computación en la nube (CC)

El portal web del Instituto de Ingeniería Eléctrica y Electrónica (IEEE) dedicado exclusivamente a la computación en la nube, describe tres organizaciones certificadas dedicadas a abordar normativas para el entorno cloud. Estas organizaciones impulsan el desarrollo de metodologías y mejores prácticas que garanticen un despliegue de infraestructura cloud adecuado para proveedores y clientes (IEEE, 2020).

2.8.1. IEEE – SA

La IEEE Standards Association promueve la iniciativa de computación en la nube impulsando la interoperabilidad de productos, por lo que ha originado dos grupos de trabajo: Grupo de estudio IEEE Adaptive Management for Cloud Computing (AMCC) y Computing (AMCC) y gestión adaptativa basada en políticas en entornos basados en la nube.

2.8.2. UIT – T

La Unión Internacional de Telecomunicaciones por su parte, expresa que la demanda por la tecnología en cuanto al despliegue de servicios cloud representa más de un tercio del tráfico de centros de datos, por lo que ya ha publicado un informe técnico sobre la nube, el cual se divide en

siete partes, que describen las conclusiones de los trabajos en la nube teniendo como líder a la Comisión de Estudio 13, supervisada por la Actividad de coordinación conjunta sobre la computación en la nube.

2.8.3. NIST

El Instituto Nacional de Estándares y Tecnología tiene por objetivo minimizar el ciclo de adopción de servicios en la nube, lo que a su vez permitirá reducir costos a largo plazo, fomentando buenas prácticas de computación en la nube con características que respalden seguridad, portabilidad e interoperabilidad.

2.9. Estándares de seguridad en la nube

Se define a un Sistema de Gestión de Seguridad de la Información (SGSI o ISMS en inglés) como un conjunto de políticas y procesos que permiten gestionar eficientemente la información preservando características fundamentales como: confidencialidad, integridad y disponibilidad. Un SGSI debe estar en la capacidad de adaptarse a cambios a largo plazo, minimizando considerablemente los riesgos de seguridad de la información, el término SGSI es mencionado con frecuencia en la norma ISO/IEC 27001.

2.9.1. ISO/IEC 27001: Sistema de gestión de seguridad de la información

Actualmente las organizaciones enfrentan niveles elevados de competencia a fin de crecer, desarrollarse y lograr "sobrevivir"; para ello deben mejorar continuamente, evolucionar e innovar; de esta manera, la norma ISO/IEC 27001 propuesta por la Organización Internacional de Estandarización especifica los requerimientos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el famoso "Ciclo de Deming": PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua, véase figura 7:

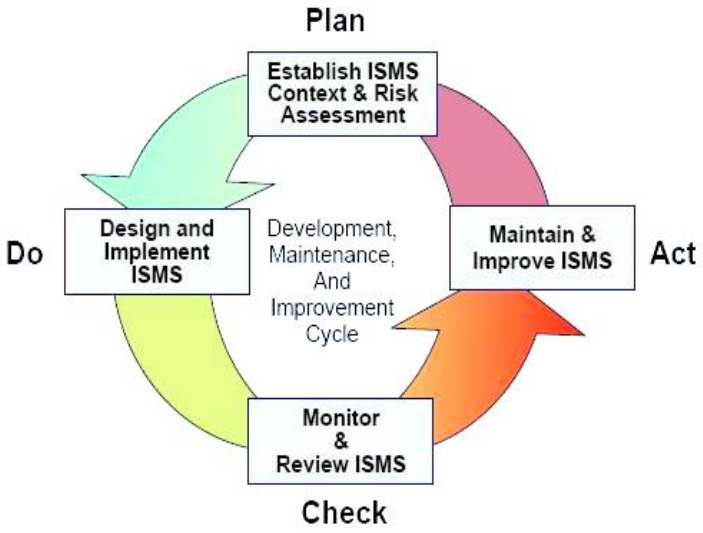


Figura 7. ***Ciclo de vida PDCA. Norma ISO/IEC 27001.***
Nota: Tomado de (IMS Guide, n,f)

2.9.2. ISO/IEC 27017: Control de seguridad de la información para servicios en la nube

Esta norma fue propuesta en el 2015 por la ISO/IEC y el ITU, por lo que existen dos documentos de contenido idéntico denominados ISO/IEC 27017 y ITU-T X.1631; surgió como complemento a la norma ISO 27002 que de cierta manera dejaba ciertas brechas en cuanto a la computación en la nube.

La ISO/IEC 27017 brinda orientación acerca de los aspectos de seguridad de la información en la nube, promoviendo la implementación de controles de seguridad de la información específicos para la nube; dicho de otra manera, constituye un código de buenas prácticas dirigido a clientes y proveedores de servicios en la nube.

De momento no existe una certificación internacional para esta norma, pues se ha catalogado como un compendio de la ISO 27001, pero no se descarta que en futuro se proponga la certificación como tal, no obstante, EY CertifyPoint se encuentra trabajando como agente certificador ISO acreditado por el Consejo holandés de acreditación, miembro del Foro internacional de acreditación (IAF, por sus siglas en inglés), el cual se encarga de emitir certificados válidos en todos los países con organismos miembros del IAF. Las organizaciones que se ajusten a la norma ISO/IEC 27017 darán paso a que sus usuarios disfruten de sus servicios con una mayor garantía de seguridad (ISO Security, 2015).

2.10. Criterios de seguridad de la información en la nube

Existe diversa documentación tanto de normativas como de buenas prácticas que incluyen criterios que deben cumplir las organizaciones para la implementación de servicios en la nube, se ha realizado el estado del arte correspondiente y en la tabla 1 se muestran los resultados:

Tabla 1.
Criterios de seguridad de la información en la nube

Item	Criterio	Parámetro de seguridad	Fuente
1	Capacidad de adaptación a la nube Recurso Humano	Sobrecarga de trabajo al personal de tecnologías de la información Metodologías	Department of Homeland Security, 2018 ISO/IEC 15408
2	Criptografía	Seguridad en el cifrado de datos	ISO/IEC 15408, Cloud Security Alliance, 2018
3	Continuidad del negocio	Adecuada gestión del negocio.	Department of Homeland Security, 2018

Nota: Elaboración propia.

2.11. Marco legal

En Ecuador, el Código Orgánico Integral Penal, sanciona los delitos contra la seguridad de los activos de los sistemas de información y comunicación, siendo estos: revelación ilegal de bases de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicaciones ***(COIP, 2018)***.

2.11.1. Protección de datos personales en el Ecuador

El pasado lunes 10 de mayo de 2021, la Asamblea Nacional aprobó el proyecto de Ley Orgánica de Protección de Datos Personales que tiene por objeto garantizar el derecho a la protección de datos, ya sea de personas naturales, jurídicas, personas fallecidas, datos anónimos o

bases de datos ; en este documento se detalla el derecho de las personas al acceso, eliminación, rectificación , oposición y portabilidad de sus datos; así como también el encargado del tratamiento de los datos deberá sujetarse al principio de seguridad de los datos mediante procedimientos de verificación, evaluación y valoración continua caso contrario deberá acatar las infracciones que pueden ser leves o graves (Asamblea Nacional del Ecuador, 2021).

CAPÍTULO III

MARCO METODOLÓGICO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE

3.1. Descripción del área de estudio

El objetivo de este trabajo es desarrollar un procedimiento técnico y detallado que regule el control de seguridad de servicios en la nube para la empresa Masiva, con base en la normativa ISO/IEC 27017, a fin de preservar la integridad de la información por medio de controles de seguridad específicos de la nube (AWS, 2020), aclarando roles y responsabilidades entra la empresa y sus clientes, para optimizar la prestación de servicios en la nube seguros, que permitan inclusive alcanzar un sistema de gestión de la información certificado. (BSI, Controles de Seguridad para Servicios Cloud, 2019).

3.2. Diseño y tipo de investigación

La presente investigación será de tipo exploratoria inicialmente, debido a que, se recabará toda la información necesaria que servirá de base para el desarrollo de las siguientes etapas, a continuación, se adoptará un modelo descriptivo puesto que se estudiará la situación actual de Masiva como proveedor de servicios Cloud y sus clientes, con el objetivo de plantear los requerimientos de diseño del SGSI-C.

Por último, se utilizará un enfoque cuantitativo a través de la puesta en marcha, que permitirá validar los procesos establecidos en el documento de control de seguridad de servicios de almacenamiento en la nube elaborado.

3.3. Procedimiento de investigación

3.3.1. Situación actual

La realización de un sistema de gestión exitoso se basa en la obtención explícita de los requerimientos y necesidades actuales, para ello, el presente capítulo recaba toda la información actual acerca de MASIVA. Se empieza detallando la estructura organizativa, infraestructura tecnológica, documentación legal y comercial, sistema de seguridad actual y análisis de amenazas y vulnerabilidades. La información que se presenta a continuación se obtuvo directamente a través de la organización, mediante la Ing. Mayra Viviana Alvear Rivas, CEO MASIVA, previo acuerdo de confidencialidad (véase Anexo A), especificando que dicha documentación será utilizada solamente para fines investigativos.

3.3.2. Estructura organizativa: roles y responsabilidades

Masiva cuenta con personal distribuido en diferentes áreas como: gerencia, monitoreo, soporte nivel 1, soporte nivel 2, software y contabilidad, cuyo organigrama se puede observar en la figura 8.

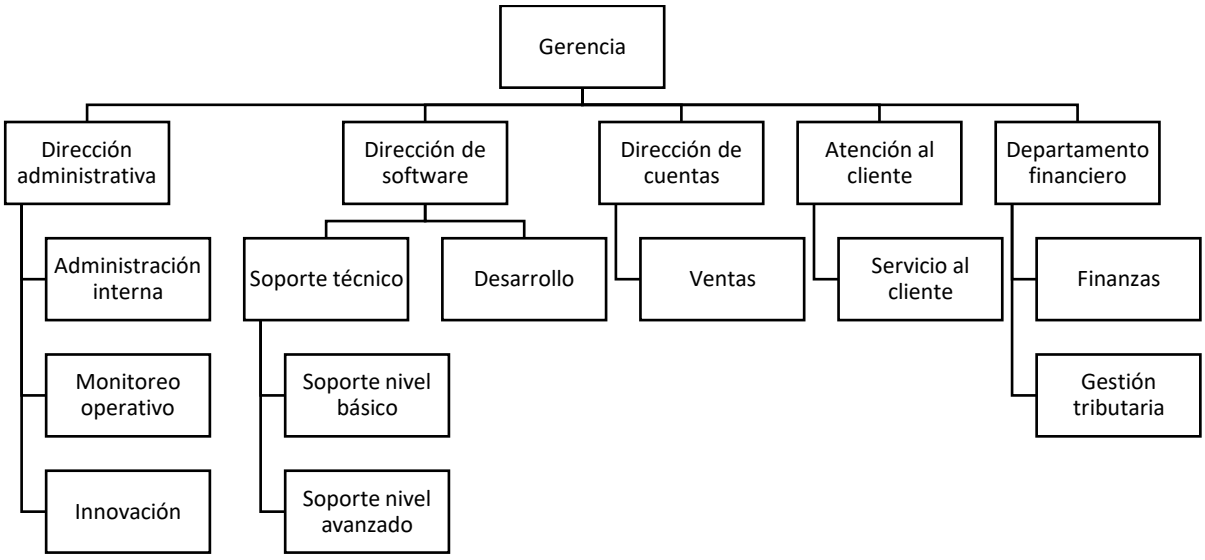


Figura 8. ***Estructura organizativa de MASIVA S.A***
Nota: Información extraída de MASIVA S.A

Todos estos departamentos cumplen roles específicos, es decir:

- El departamento gerencial se compone por el director general, gerente o "Chief Executive Officer", más conocido como CEO MASIVA, cuya función es llevar a cabo funciones gerenciales que encaminen a Masiva a un nivel estratégico elevado.
- La dirección administrativa se encarga de la supervisión de la empresa en general, monitoreando que todo atraviese un control de calidad antes de llegar al cliente.
- El departamento de Software es quien se encarga de todos los requerimientos técnicos, acorde a lo solicitado por el cliente, previo filtro de atención al cliente.
- La dirección de cuentas ocupa el tema de ventas y gestión con clientes externos personales o corporativos.

- El departamento financiero se centra en la planificación financiera que busca el correcto manejo de ingresos y salidas, que permitan alcanzar un punto de equilibrio que mantenga estable a la organización.

3.3.3. Infraestructura de TI

Masiva cuenta con una infraestructura física distribuida en departamentos para sus áreas, no obstante, el presente proyecto se basa en la seguridad de servicios en la nube, por lo que, en este apartado se tomarán en cuenta únicamente los recursos lógicos que dispone.

Masiva cuenta con infraestructura en la nube, ofreciendo software como servicio (SaaS), que utiliza principalmente servidores acordes a la arquitectura de la tabla 2.

Tabla 2.
Infraestructura cloud de servidores Masiva.

Item	Sistema Operativo	Recursos Lógicos Cloud	Propósito
1	Linux	4 Gb Ram CPU 2 (Virtuales) CPU 24 / h	Login-sms / login-emails.com
2	Linux	4 Gb Ram CPU 2 (Virtuales) CPU 24 / h	Servidor para despacho de mensajes asíncrono A

3	Linux	4 Gb Ram CPU 2 (Virtuales) CPU 24 / h	Servidor para despacho de mensajes asíncrono B
4	Linux	4 Gb Ram CPU 2 (Virtuales) CPU 24 / h	Servidor para despacho de mensajes asíncrono C
5	Linux	4 Gb Ram CPU 2 (Virtuales) CPU 24 / h	Servidor para despacho de mensajes asíncrono D

Nota: Información extraída de MASIVA S.A

3.3.4. Niveles de seguridad

- La seguridad que maneja la organización se basa en el acceso basado en roles o basado en usuarios:

  Usuarios: cuentas individuales que se crean en cada servidor.

  Roles: compuesto por uno o más usuarios.

Los roles facilitan la asignación de permisos a varios usuarios que desempeñan la misma función, mientras que los permisos para ejecutar ciertas operaciones se asignan a roles específicos. Así, por ejemplo, masiva tiene un usuario de acceso AWS, que corresponde al servidor raíz, mientras que para los procesos de backend de las plataformas cloud se tiene usuario super administrador, administrador y usuario final.

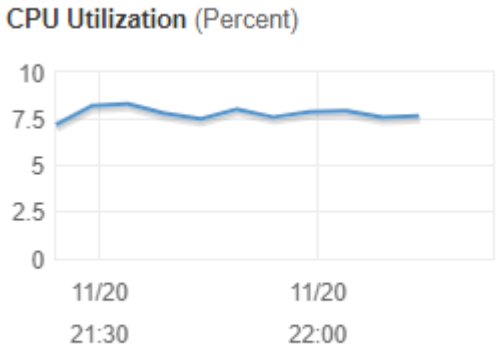
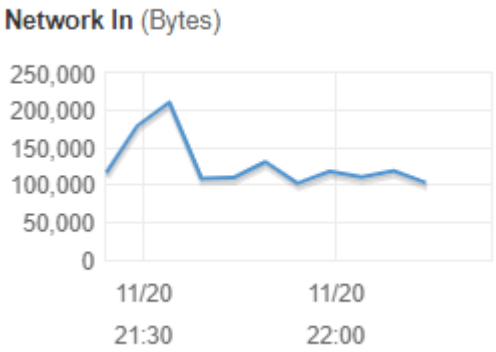
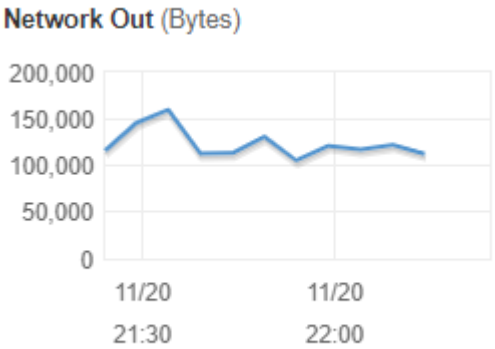
3.3.5. Monitoreo operativo

Masiva monitorea su infraestructura de TI interna para detectar dificultades o brechas y tomar decisiones proactivas. La idea es identificar problemas específicos que pueden afectar el rendimiento general de su infraestructura de red. Cuando se detecta algún problema, el personal de monitoreo en turno, alerta al nivel operativo, para corregir dichos inconvenientes antes de que puedan afectar mayormente a la organización.

El proceso de monitoreo de la red en la nube de Masiva, utiliza una variedad de configuraciones, incluidas soluciones de hardware o software o una combinación de ambos.

Parte del monitoreo operativo incluye la revisión de consumos de memoria en CPU, envío y recepción de paquetes según las instancias creadas. Por ejemplo, la tabla 3 indica muestras de los reportes obtenidos en la plataforma en la nube. Mientras que en el Anexo B se muestra un reporte en tiempo real, a manera de ejemplo.

Tabla 3.
Monitoreo de infraestructura cloud Masiva S.A

Item	Parámetros	Imagen
1	Monitoreo de utilización de CPU.	
2	Recepción de paquetes	
3	Envío de paquetes	

Nota: Información extraída de MASIVA S.A

3.3.6. Plan de contingencia

Masiva utiliza cuatro servidores en modo espejo, que duplican todos los procesos y transacciones del servidor primario. Si por cualquier motivo, uno de los servidores falla, el servidor de respaldo puede ocupar su lugar inmediatamente sin ningún tiempo de inactividad. La duplicación del servidor es una estrategia costosa pero eficaz para lograr la tolerancia a fallos.

3.3.7. Análisis de riesgos y vulnerabilidades

Con fundamento en la información recabada, es posible realizar un análisis de cómo se maneja actualmente la información en la nube en Masiva; está claro que para esta organización la disponibilidad de los servicios en la nube es fundamental, aun así, se detectaron algunas brechas, las cuales se detallan a continuación:

- Carencia de un plan de contingencia documentado y detallado, lo cual inicialmente podría no parecer un inconveniente, no obstante, si la organización continúa expandiéndose, ingresará personal nuevo, que al no tener por escrito ciertos lineamientos, le resultará más complicado salvaguardar u orquestar la información.
- La política de seguridad actual de la empresa no evidencia explícitamente los procedimientos de manejo correcto de la información, los roles cliente – proveedor no se encuentran detallados.
- No existe un procedimiento formal para la ejecución de procedimientos de respaldo, como, por ejemplo, copias de seguridad contenidas en equipos, servidores o dispositivos

externos, no se toma en cuenta la periodicidad o las condiciones de almacenamiento óptimo.

- Escasez de perfilamiento de usuarios al otorgar o revocar acceso a las máquinas virtuales o bases de datos. Dado que el personal que maneja estas credenciales es limitado, la organización no ha tenido la necesidad de crear o limitar los perfiles de administrador o superadministrador.

Aunque Masiva es una organización consiente del tratamiento que se le debe dar a la información para obtener una mayor seguridad, no está exenta de amenazas naturales o tecnológicas, para ello se define la siguiente clasificación, según Ghassan Dreibi en su artículo "Amenazas críticas de hoy: un informe de amenazas de seguridad":

- Amenazas naturales: sismos, tormentas, incendios forestales, inundaciones, maremotos, entre otros.
- Amenazas mecánicas: fallas mecánicas, fallos de energía, pérdida de acceso.
- Amenazas humanas: pérdida de personal clave, huelgas, epidemias.
- Amenazas tecnológicas: hacking, fallas de hardware, software, fallas en la red, caída del sistema global.
- Amenazas operacionales: crisis financieras, fallo de proveedores en tiempos de entrega, fallas en equipo, mala propaganda.

Las amenazas expuestas anteriormente pueden originarse de forma accidental o provenir de una fuente. Para que éstas amenazas logren causar daño, es necesario que exploten las vulnerabilidades de la organización, sistema, aplicaciones o servicios.

Así, las vulnerabilidades vienen a ser las debilidades asociadas a la organización, es decir, las debilidades de su sistema de seguridad. Una vulnerabilidad no causa daño, pero sí puede hacer que una amenaza afecte a la organización (Cardona, 2015). Las vulnerabilidades pueden ser clasificadas en:

- Seguridad del recurso humano: falencias en entrenamientos de seguridad, falta de políticas para el uso correcto de las telecomunicaciones, entre otros.
- Controles de acceso: políticas incorrectas de controles de acceso, no actualización de credenciales de seguridad, no revocar accesos cuando el personal se desvincula de la empresa, entre otros.
- Seguridad física y ambiental: controles de acceso inapropiados para el ingreso a oficinas o áreas restringidas, carencia de procedimientos para sustitución de equipos, susceptibilidad a variaciones de tensión.
- Gestión de operaciones: carencia de mecanismos que aseguren roles efectivos entre cliente y proveedor.

De esta manera, es posible concluir que las amenazas y vulnerabilidades deberían presentarse simultáneamente para causar daño, lo que se conoce como riesgo. Véase figura 9.

Figura 9. ***Análisis de riesgo. Amenaza vs Vulnerabilidad***
Nota: Tomado de (INCIBE, 2017)

Así, en la tabla 4 se indican los activos de información de Masiva con su correspondiente amenaza y vulnerabilidad:

Tabla 4.
Amenazas y vulnerabilidades de Masiva S.A

Item	Activo	Amenaza	Vulnerabilidad
1	Servidores de despacho o modo espejo (HW)	Ataque lógico intencionado Fallos físicos Fallos operativos	– Vulnerabilidad del S.O – Carencia de plan de contingencia. – S.O. obsoleto. – Desgaste natural del equipo. – Falta de mantenimiento preventivo. – Caída del sistema por asignamiento incorrecto de recursos.
2	Recurso humano	Indisponibilidad del personal Errores por desconocimiento u omisión. Ingeniería Social	– Enfermedad, calamidad – Falta de capacitación o difusión de políticas o reglamentos. – Desconocimiento de mejores prácticas de seguridad.

		Malware	– Dispositivos móviles del personal sin software de protección.
3	Políticas SGS	Brechas de información	– Uso de dispositivos extraíbles.
		Accesos no autorizados	– Carencia de privilegios o roles
		Pérdidas totales o parciales	– Falta de procedimientos de backup.
4	Servicios Cloud	Caída del sistema	– Incorrecta asignación de VM, recursos o discos.
		Denegación del servicio	– Falta de mecanismos de seguridad en la nube.
		No disponibilidad	– Carencia de límites y control de recursos.

Nota: Información extraída de MASIVA S.A

Si bien la computación en la nube ofrece muchos beneficios, estos servicios conllevan algunos problemas de seguridad:

- Falta de controles de seguridad en configuraciones de terceros.
- Poca visibilidad en entornos de múltiples nubes.
- Amplio espacio para el robo y uso indebido de datos.
- Las nubes son objetivos comunes de los ataques DDoS.
- Los ataques se propagan rápidamente de un entorno a otro.

Los riesgos de la computación en la nube afectan a todos los departamentos y dispositivos de la red. Por lo tanto, la protección debe ser sólida, diversa e inclusiva. Una política de seguridad en la nube confiable proporciona todas esas cualidades. Dado que MASIVA depende de los servicios en la nube, las prácticas descritas otorgan un nivel de visibilidad y control necesarios para proteger los datos en la nube.

El costo de arreglar una violación de datos supera con creces el precio de las precauciones adecuadas. El presente Sistema de Gestión de Seguridad en la Nube pretende mostrar los pasos de precaución adecuados cuando se opera en la nube. Esta política le permite aprovechar las ventajas de la nube sin asumir riesgos innecesarios.

3.4. Sistema de Gestión de Seguridad de la Información para Servicios en la Nube

3.4.1. Propósito

Esta política describe prácticas seguras para MASIVA CÍA LTDA y cualquier otra unidad operativa de la organización identificadas por el uso de administración de servicios en la nube y de almacenamiento. También destaca los riesgos de seguridad introducidos por el almacenamiento de datos confidenciales en la nube y exige la protección de los datos almacenados por los proveedores de servicios en la nube (CSP) con controles tecnológicos adecuados.

3.4.2. Alcance

Esta política se aplica a todos los datos empresariales almacenados o procesados por aplicaciones en la nube de terceros, y a todos los servicios en la nube externos, incluido el correo electrónico, mensajería SIM y el almacenamiento de documentos basados en la nube.

3.4.3. Antecedentes

Masiva brinda servicios tecnológicos y almacenamiento de datos a terceros, mediante la computación en la nube, misma que proporciona múltiples ventajas, que a medida que la empresa se extiende, los controles actuales pueden resultar no adecuados, provocando pérdida de datos o el acceso no autorizado a las redes corporativas. Debido a que las políticas de seguridad tradicionales

diseñadas para otras tecnologías no siempre se adaptan adecuadamente al entorno de la nube, estos entornos requieren consideración y análisis adicionales para garantizar que se cumplan los objetivos de seguridad y control. La División de Seguridad Empresarial debe determinar qué tipos de datos son apropiados para almacenar y compartir a través de servicios en la nube, y cómo proteger esos datos.

3.4.4. Políticas

Una política de seguridad en la nube es una guía formal bajo la cual MASIVA lleva a cabo sus operaciones. Estas instrucciones definen la estrategia de seguridad y orientan todas las decisiones relacionadas con la seguridad de los activos en la nube. La presente política está basada en la norma ISO/IEC 27017 e ISO 27001 y especifica los siguientes parámetros:

- Tipos de datos que pueden y no pueden moverse a la nube.
- Cómo los equipos abordan los riesgos para cada tipo de datos.
- Quién toma decisiones sobre el cambio de cargas de trabajo a la nube.
- Quién está autorizado para acceder o migrar los datos.
- Términos de la regulación y estado de cumplimiento actual.
- Respuestas adecuadas a amenazas, intentos de piratería y filtraciones de datos.
- Reglas que rodean la priorización de riesgos.

Este sistema de gestión de seguridad en la nube garantizará la integridad y privacidad de la información logrando una optimización del tiempo a la hora de tomar decisiones.

3.4.5. Organización de la seguridad de la información

Como en todo consenso empresarial, la relación comercial entre el proveedor de servicios en la nube y el cliente debe estar regulada. Así el SLA (Acuerdo de nivel de servicio) constituye un documento de negocio entre proveedor y cliente, en el cual se conceptualizan las especificaciones técnicas más relevantes en relación con los requerimientos funcionales, las variables monetarias y la calidad del servicio que se regirá durante el periodo de validez acordado. Se expone un acuerdo de nivel de servicio en el anexo C. Este contiene las partes más relevantes:

- Acuerdo entre las partes.
- Periodo de vigencia.
- Servicios cubiertos.
- Exclusiones.
- Responsabilidades del proveedor y cliente.
- Tiempos de respuesta.
- Sanciones.
- Derecho a la terminación del contrato.
- Firmas.

3.4.6. Seguridad del recurso humano

Algunas amenazas a la seguridad de los datos llegan a través de la red, como la piratería informática, sin embargo, existen formas más insidiosas en las que se puede violar la privacidad. En el documento Cloud Security Guidance, propuesto por el departamento de Defensa de Estados Unidos (Security Homeland, 2018) se menciona que, en la nube el personal de TI absorbe mayor carga de trabajo y complejidad en estos entornos, incrementando el riesgo de una mala configuración, como por ejemplo el "spear phishing", en el que los empleados dan inadvertidamente información confidencial de la contraseña que puede comprometer los datos.

Un informe de Verizon 2016 Data Breach Investigations Report encontró que el 63% de las violaciones de datos confirmadas implican aprovechar contraseñas débiles, predeterminadas o robadas (Verizon, 2016). Otros errores comunes incluyen enviar información confidencial a la persona equivocada, no deshacerse de la información de la empresa correctamente, mala configuración de los sistemas de TI y computadoras portátiles y dispositivos móviles perdidos o robados.

Los empleados también tienen un papel que desempeñar en la protección de los datos, pero deben ser orientados sobre cuál es ese papel, por cuanto son los responsables de administrar su conocimiento y herramientas para la gestión de activos en la nube.

De esta manera se vuelve imprescindible incorporar capacitación en seguridad de datos en el y protocolos de capacitación regulares, la organización estará mucho más segura de las amenazas cibernéticas.

Se podría incentivar el proceso, creando recompensas. Así lo propone “The Huffington Post” en su artículo “Why the Cloud Has a Security Problem” en el cual se sugiere que se otorgue un “incentivo” al mejor "detective de seguridad" del mes (The Huffpost, n.d.).

La seguridad de los datos en la computación en la nube, especialmente en lo que respecta a recursos humanos, es un proceso complejo y continuo. No se puede ignorar e involucra a todos en la empresa.

3.4.7. Control de autenticación

Las regulaciones de control interno evitan el acceso no autorizado a sus activos en la nube, permitiendo el acceso solo a personas que tengan una necesidad real de recursos. Algunos trabajadores necesitan acceso de solo lectura, como los encargados de ejecutar informes. Otros usuarios deben poder realizar algunas tareas de operaciones, como reiniciar las VM, pero no hay razón para otorgarles la capacidad de modificar las VM o sus recursos; aquí surge el término “Compromiso de credenciales”. Así se tienen las siguientes políticas:

- Modificar contraseñas de forma regular, y especificar cuándo y dónde se puede acceder a los datos.
- Minimizar las credenciales con permisos de superadministrador y establecer perfilamientos según las necesidades de cada usuario.
- Utilizar un factor de autenticación múltiple, que permita asegurar el uso adecuado de credenciales en la nube.

3.4.8. Criptografía

El cifrado y almacenamiento de los datos tienen que ser examinado para que solo el personal autorizado tenga acceso a la información, de esta forma se sugiere:

- Utilizar claves de acceso para proveedor y cliente, así como no utilizar las mismas para todos los activos.
- Indicar la vigencia de las llaves criptográficas durante el ciclo de vida.
- Revisar la normativa vigente de criptografía NIST SP-800-57, ANSI X9.69 y ANSI X9.73.

3.4.9. Seguridad física

El proveedor de servicios en la nube es quien asume la seguridad física de los servicios ofrecidos, por esto, es necesario implementar políticas y controles de ingreso físico que aseguren el bienestar de los activos.

- Masiva debe cumplir con las buenas prácticas y regulaciones de la infraestructura física.
- Las cargas de trabajo a las que son sometidos los conjuntos físicos pueden producir lentitud, bloqueos y cuellos de botella una vez que superan sus habilidades, por esto se tienen que conocer las restricciones y habilidades, para que los administradores logren configurarlas de manera correcta.

3.4.10. Seguridad contra hacking y malware

El departamento de defensa de Estados Unidos sugiere revisar periódicamente la actualización de parches y versiones que proporcionen mayor seguridad a los activos.

- Sugiere también realizar un análisis de vulnerabilidades a través de sistemas de detección de intrusos y Políticas de Seguridad del Contenido (CSP).
- Configuraciones a nivel de dispositivos intermedios también resultan válidas, como por ejemplo la utilización de cortafuegos o detectores de intrusos.

3.4.11. Desarrollo y mantenimiento

Masiva se encargará de proporcionar copias de seguridad automáticas de datos de sus clientes. Si una estación de trabajo o un dispositivo se bloquea o pierde energía mientras se trabaja, los datos que se ingresaron en la aplicación en la nube se guardan automáticamente hasta el momento de la interrupción. Una vez que se reinicia el dispositivo (o se restauran las conexiones de red o de energía), los empleados pueden retomar el trabajo desde donde comenzaron.

3.4.12. Redundancia y continuidad del negocio

Los repositorios de datos basados en la nube MASIVA deberán recuperarse o regenerarse automáticamente, si se pierden o el servicio en la nube los descarta intencionalmente o inadvertidamente, para ello se hace uso de sus servidores en modo espejo.

3.4.13. Gestión del cumplimiento

Una manera de validar el cumplimiento de un sistema de gestión de seguridad consiste en realizar auditorías que permitan evaluar el desempeño de las políticas organizacionales, logrando una retroalimentación que conlleve a alcanzar los niveles de seguridad adecuados. Este apartado se tratará con detalle el capítulo V.

3.5. Matriz de correlación ISO/IEC/27017 e ISO/IEC/27001

Se hace necesario realizar una matriz de correlación incluyendo los objetivos de control tomados de las normativas en cuestión, de esta manera, en la tabla 5 se indica cada punto. Los criterios que se muestran son los que permiten evaluar el cumplimiento del estándar de cada uno

Tabla 5.
Matriz de correlación ISO/IEC/27017 e ISO/IEC/27001

NORMATIVA	CRITERIO	OBJETIVO DE CONTROL	DESCRIPCIÓN
ISO 27001-2 005: A5. Política de Seguridad	A5.1	A5.1 Brindar una guía metodológica para regular la seguridad de la información en la nube.	Documento con políticas para que todos los empleados y externos necesarios tengan conocimiento. Revisión periódica de las políticas planteadas.
ISO 27001-2 005: A6. Organización de la seguridad de la información	A6.1 Organización interna	A6.1.1 Comprometer a todos los niveles jerárquicos de la empresa en preservar la seguridad de la información en la nube.	Compromiso de las cabezas de cada departamento en cuanto a hacer cumplir la política propuesta.
		A6.1.3 Responsabilidades	Definir las responsabilidades de los que conforman la organización.
		A6.1.4 Autorización para instalaciones de gestión de información	Proceso de autorización gerencial
		A6.1.5 Acuerdos de confidencialidad	Revisión periódica de los acuerdos de confidencialidad
	A6.2 Entidades externas	A6.2.3 Tratamiento de la seguridad en contratos con terceras personas	Establecer acuerdos que involucren el procesamiento de la información con terceros.
ISO 27001-2 005: A.7 Gestión de activos	A7.1. Responsabilidad por los activos	A.7.1.1. Identificar los activos	Levantar un inventario y mantenerlo actualizado constantemente

	A7.2 Clasificación de la información	A.7.2.2 Manejo de información	Etiquetar y clasificar la información
ISO 27001-2 005: A.7 Seguridad del recurso humano	A8.1 Antes del empleo	A8.1.1 Roles y responsabilidades	Documentar los roles y responsabilidades de empleados, contratistas o terceros.
		A8.1.3 Términos y condiciones	Revisar los términos y condiciones del contrato periódicamente.
	A8.2 Durante el empleo	A8.2.2 Capacitación en temas de seguridad de la información	Todos quienes conforman la organización ya sean empleados o terceros en caso de ser necesario, deben recibir capacitaciones y actualizaciones de los procedimientos que sean pertinentes
		A8.2.3 Proceso disciplinario	Documentar formalmente las posibles sanciones a las que se expone un empleado al cometer una infracción
	A8.3 Terminación del contrato	A8.3.3 Eliminación de derechos de acceso	Al término del contrato o acuerdo de nivel de servicio, se deben eliminar todos los derechos de acceso de la persona involucrada
ISO 27001-2 005: A.9 Seguridad física y ambiental	A9.1.1 Áreas seguras	A9.1.1. Perímetro de seguridad física	Utilizar barreras físicas para proteger el área que contiene la información
		A9.1.2 Controles de entrada	Solo el personal autorizado debe tener acceso a ciertas áreas.
		A9.1.4 Protección contra amenazas externas y ambientales	Diseñar e implementar métodos de protección frente a incendios, inundaciones, entre otros.
ISO 27001-2 005: A.10 Gestión de las comunicaciones y operaciones	A10.1 Procedimientos y responsabilidades operacionales.	A10.1.1. Procedimientos de operación documentados.	Documentar la información
		A10.1.2 Gestión de cambio	Documentar los cambios
	A10.2 Gestión de la entrega del servicio a terceros	A10.2.1 Entrega del servicio	Asegurarse que los “clientes” mantengan los controles de seguridad incluidos en el SLA
		A10.2.2 Monitoreo y revisión	Realizar auditorías periódicas.

	A10.3 Planeación y aceptación del sistema	A10.3.1 Gestión de capacidad	Realizar proyecciones del uso de recursos
	A10.4 Protección contra software malicioso	A10.4.1 Controles contra software malicioso	Implementar procedimientos de control frente a amenazas informáticas.
	A10.5 Procedimientos de respaldo	A10.5.1 Respaldo de la información	Mecanismos de respaldo de los servicios ofrecidos
	A10.6 Gestión de seguridad en redes	A10.6.1 Controles de red	Revisar periódicamente el estado de la red.
	A10.7 Gestión de medios	A10.7.4 Seguridad de documentación del sistema	Proteger los informes realizados de posibles accesos no autorizados.
	A10.9 Servicios de comercio electrónico	A10.9.1 Transacciones	Proteger las transacciones que sean realizadas en línea
	A10.10 Monitoreo	A10.10.3 Protección de la información del registro	Monitorear constantemente la gestión de cambios
ISO 27001-2 005: A.11 Control de acceso	A11.1 Política de control de acceso	A11.1.1. Política de control de acceso	Implementar y revisar la política de control de acceso.
	A11.2 Gestión de acceso al usuario	A11.2.2 Gestión de privilegios	Controlar la asignación de módulos y roles en el software.
		A11.2.4 Revisión de los derechos de acceso del usuario	Revisar periódicamente los derechos de acceso de sus empleados.
	A11.3 Responsabilidades del usuario	A11.3.1 Uso de clave	Implementar un manual de buenas prácticas de seguridad de la información.
	A11.4 Control de acceso a redes	A11.4.1 Política sobre servicios en red	Cada usuario solo debe tener permisos de acceso para los módulos que le corresponde
		A11.5.2 Autenticación del usuario	Controlar el acceso de usuarios.

	A11.5 Control de acceso al sistema de operación	A11.5.3 Sistema de gestión de claves	Utilizar sistemas de claves acorde a las necesidades.
		A11.5.5 Sesión inactiva	Después de un periodo de inactividad las sesiones deben cerrarse automáticamente.
		A11.5.6 Limitación del tiempo de conexión	Restringir el tiempo de conexión para proporcionar una mayor seguridad.
ISO 27001-2 005: A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	A12.2 Procesamiento correcto en las aplicaciones	A12.2.1 Integridad del mensaje	Implantar controles apropiados para salvaguardar la integridad del mensaje.
		A12.2.4 Validación de data output	Validar la data de salida para asegurar que se están realizando los procedimientos adecuados.
	A12.3 Controles criptográficos	A12.3.1 Política sobre el uso de controles criptográficos	Diseñar una política sobre el uso de criptografía.
		A12.3.2 Gestión de clave	Gestionar las claves acorde a los métodos de criptografía desarrollados.
	A12.5 Seguridad en los procesos de desarrollo y soporte	A12.5.1 Procedimientos de control de cambios	Controlar la gestión de cambios.
		A12.5.4 Filtración de información	Mitigar las brechas que puedan dar lugar a la filtración de información.
	A12.6.1 Gestión de vulnerabilidad técnica	A12.6.1 Control de vulnerabilidades técnicas	Valorar continuamente las amenazas a las que se expone la organización.
ISO 27001-2 005: A.13 Gestión de incidentes en la seguridad de la información	A13.1. Reportes de eventos		Los incidentes de seguridad de la información deben documentarse a la brevedad.
ISO 27001-2 005: A.15 Cumplimiento	A15.1 Cumplimiento con requerimientos legales	A15.1.1 Identificación de legislación aplicable	Toda la documentación debe enmarcarse acorde a la ley vigente en el país

	A.15.2 Cumplimiento de las políticas y estándares de seguridad y el cumplimento técnico	A15.2.1 Cumplimiento con las políticas y estándares de seguridad	Debe existir personal encargado de supervisar y guiar en el cumplimiento de los procedimientos planteados
	A.15.3 Consideraciones de auditoria de los sistemas de información	A15.3.1 Controles de auditoría de sistemas de información	Programar auditorías en intervalos que no irrumpan con las actividades comerciales del negocio.
ISO/IEC 27017:2015: Información de seguridad y recurso humano	6. Organización de la información	6.1. Organización interna	Clasificación correcta de la información
		6.2. Dispositivos móviles y teletrabajo	
	7. Seguridad del recurso humano	7.1. Antes del empleo	Accesos restringidos dependiendo del rol. Compromiso de credenciales
		7.2. Durante el empleo	
		7.3. Terminación del contrato	
ISO/IEC 27017:2015: Controles de acceso	8. Manejo de activos	8.1. Responsabilidad	Recurso humano capacitado para el manejo de información,.
		8.2. Información y clasificación	
	9. Control de acceso	9.4. Controles de acceso de sistemas y aplicaciones.	
	10. Criptografía	9.5. Seguridad mediante controles criptográficos	Protección de datos
ISO/IEC 27017:2015: Seguridad física	11. Seguridad física y del ambiente	11.1 Áreas seguras	Seguridad en infraestructura.
		11.2 Equipamiento	
		12.2 Protección antimalware	Capacidad de respuesta frente a ataques.

ISO/IEC 27017:2015: Seguridad lógica	12. Operaciones de seguridad	12.3 Procedimientos de backup	Redundancia sin afectar la integridad.
		12.4 Logging	Gestión de permisos e identidad
		12.6 Vulnerabilidades técnicas	Evaluación de vulnerabilidad
		12.7. Monitoreo de sistemas	Gestión del cumplimiento y auditorías
	13. Seguridad de las comunicaciones	13.1. Gestión de la seguridad de la red	Protección de datos
		13.2. Transferencia de información	
ISO/IEC 27017:2015: Mantenimiento y continuidad del negocio	14. Adquisición de sistemas y equipos	14.1 Seguridad y desarrollo	Mantener los activos disponibles para la operatividad.
	`15. Proveedores	15.1. Seguridad en relación con el proveedor	
		15.2 Acuerdos de envío	
	17. Seguridad frente a incidentes	17.2. Redundancia	Evitar que se pierda la información
ISO/IEC 27017:2015: Cumplimiento de políticas	18. Cumplimiento	18.1. Cumplimiento acorde a la normativa legal vigente	No interferir con los lineamientos legales vigentes.

Nota: Tomado de (ISO Security, 2015)

3.6. Brechas de datos personales

El Reglamento general de protección de datos (GDPR) de Europa define a las brechas de datos personales como una violación de datos que conduce a la destrucción, pérdida, alteración o divulgación no autorizada de, o acceso a, datos personales. Por ejemplo:

- Dispositivos de transferencia de datos perdidos, como memorias USB.
- Computadoras robadas.
- Hackear.
- Infección de malware.
- Ataques cibernéticos.
- Incendio en el centro de datos.
- Enviar un extracto bancario a la persona equivocada.

Una violación de los datos personales puede tener consecuencias como la pérdida de control sobre los datos personales, el robo de identidad o fraude, daño a la reputación o la anulación de la seudonimización o la pérdida de la confidencialidad de los datos personales (GDPR, 2018).

Tanto el responsable como el encargado del tratamiento de datos personales deben proteger los datos con medidas de seguridad correspondientes al riesgo relacionado con el tratamiento de datos personales. El responsable del tratamiento también debe prepararse para posibles violaciones de datos personales mediante la elaboración de directrices para la eventualidad de violaciones de

datos personales y ser capaz de reaccionar ante las violaciones de datos personales lo más rápido posible.

El responsable del tratamiento debe evaluar el nivel de riesgo causado por las violaciones de datos personales a las personas interesadas, por ejemplo:

- Sin riesgo.
- Riesgo.
- Alto riesgo.

El nivel de riesgo determina las medidas requeridas por parte del responsable del tratamiento. Tales medidas pueden incluir

- Documentación de la violación de datos personales.
- Notificación a la autoridad supervisora.
- Notificación a los interesados.

Documentar todas las violaciones de datos personales, sus efectos y las acciones correctivas tomadas, independientemente de las medidas eventualmente requeridas por la violación de datos personales. El descuido de las obligaciones de documentación o notificaciones constituye una infracción del Reglamento General de Protección de Datos (GDPR) y puede resultar en las sanciones especificadas en el mismo.

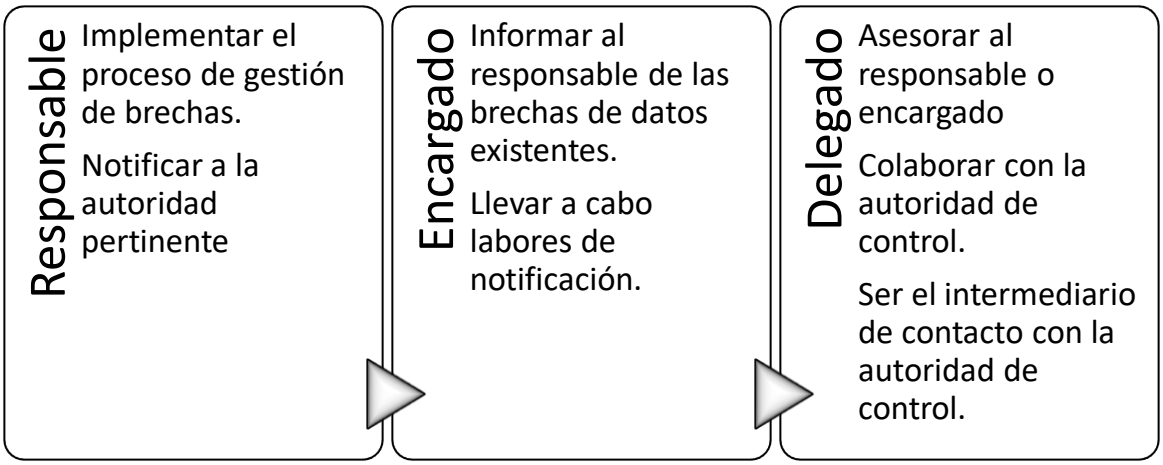


Figura 10. ***Responsables de la protección de datos personales.***
Nota: Tomado de (Creative & Atribuci, 2021)

3.6.1. Normativa legal en otros países

En Finlandia, por ejemplo, si una violación de datos personales puede suponer un riesgo para los derechos y libertades de las personas físicas, se debe notificar a la autoridad de control, en este caso la Oficina del Defensor del Pueblo para la Protección de Datos sin demoras indebidas y, cuando sea posible, a más tardar 72 horas después de que el controlador tenga conocimiento de la violación de datos personales. El procesador notificará primero al controlador de la violación de datos personales, a menos que se haya acordado específicamente que el controlador puede notificar a la Oficina del Defensor del Pueblo para la Protección de Datos directamente sobre las violaciones de datos personales. Sin embargo, la responsabilidad de realizar la notificación sigue siendo del responsable del tratamiento (Office of the Data Protection, 2018).

3.7. Consideraciones bioéticas

Esta investigación tiene como objetivo mitigar riesgos de seguridad en servicios de almacenamiento en la nube, con la utilización de lineamientos propuestos en la normativa ISO/IEC 27017, estudio que puede ser beneficioso para empresas que cuenten el servicio de almacenamiento en la nube o a su vez para empresas que quieran implementar dicho servicio, en sus diferentes fases de investigación toda información analizada será de uso exclusivo, confidencial y bajo los fines pertinentes, garantizando que el resultado de la investigación sea objetiva, metódica, honesta y profesional.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

El Sistema de Gestión de Seguridad de la Información planteado se llevó a cabo de manera gradual en MASIVA, siguiendo la estrategia de implementación con base en el ciclo PHVA (Planificar, Hacer Verificar y Actuar).

El primer paso corresponde a la recopilación de información de la empresa, todos los procesos que se realizan actualmente, mismos que servirán para identificar cuales se pueden mejorar, identificando los riesgos.

Se propone verificar periódicamente el cumplimiento de las políticas planteadas, llegando a una fase de mejora continua que constantemente debe estar en revisión.

4.1. Estado actual

En esta primera etapa se evaluó el estado actual de la infraestructura física de la empresa y el estado lógico de la red, lo cual permitió identificar las acciones correctivas que se deben tomar en cuenta para la implantación del SGSI-C. La fase de recolección de información ya se desarrolló en el apartado 2.10 de situación actual, el objetivo de éste es recabar toda la información posible y materializarla en diagramas o resúmenes que sirvan de base para la ejecución de las políticas establecidas. De allí se obtuvo la siguiente matriz de riesgos en la tabla 6:

Tabla 6.
Matriz de riesgos actuales

Item	Riesgo	Descripción	Nivel de aplicación actual
1	Interrupciones a nivel de red	Fallos con el proveedor	medio
2	No dimensionamiento de los requerimientos institucionales	Sub-dimensionamiento de recursos: lógicos (contratación de ancho de banda), físicos (servidores bajo demanda) y recurso humano	medio
3	Capacitación al recurso humano	La emergencia sanitaria no permite la capacitación óptima del personal	alto
4	Infraestructura física para el datacenter	Daños físicos en servidores sin respaldos.	alto
5	Sistemas de bitácoras y gestión de cambios	No se documentan los procedimientos realizados.	bajo
6	Help Desk	Procesos no estandarizados.	bajo
7	Áreas restringidas	Identificación de áreas de acceso del personal autorizado.	bajo

Nota: Elaboración propia.

4.2. Planeación

Lo siguiente fue seleccionar una estrategia de planificación para la implementación del SGSI-C, la opción requerida fue la denominada “autogestión” puesto que MASIVA cuenta con el recurso humano necesario para optimizar sus sistemas de seguridad.

4.3. Cronograma

Se propuso un cronograma de ejecución con los tiempos necesarios (véase figura 11) para la compilación de cada etapa, se optó por una implementación a corto plazo, definiendo las responsabilidades para cada rol: responsable, encargado y delegado, como lo establece la reciente aprobada Ley Orgánica de Protección de datos personales en el Ecuador (tabla 7);

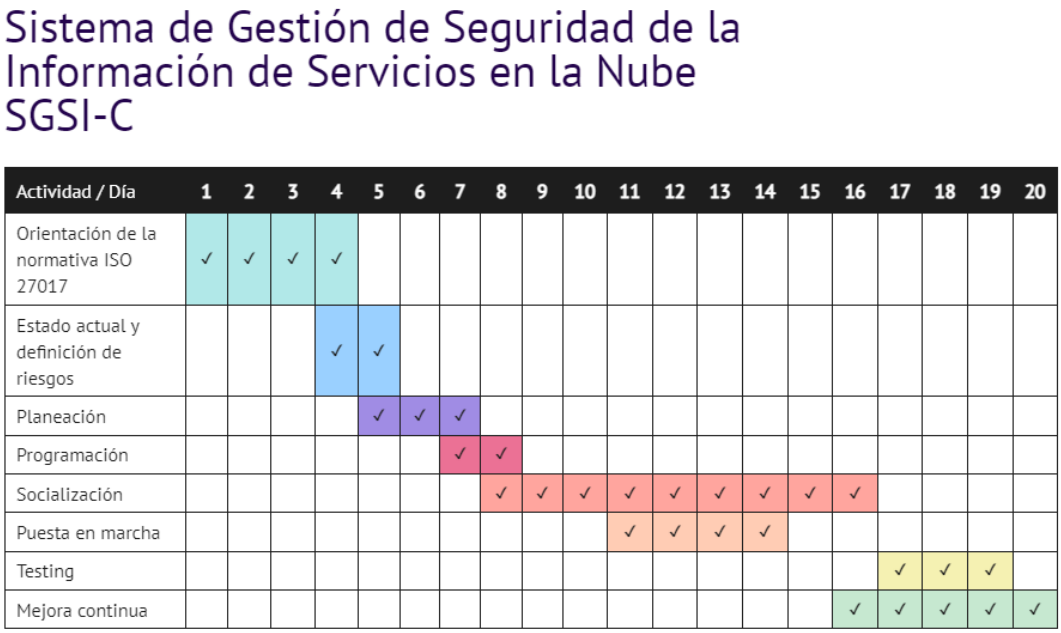


Figura 11. ***Cronograma de implementación del SGSI-C***

Nota: Elaboración propia.

Tabla 7.
Roles de usuario para la implementación del SGSI-C

Item	Rol	Personal designado
1	Responsable	Jefe de Operaciones
2	Encargado	Jefe de Seguridad
3	Delegado	Asistente de TI

Nota: Elaboración propia.

4.4. Socialización

Esta fase consistió en planificar una reunión con todos los involucrados a fin de socializar las políticas establecidas, mismas que se exponen en un manual que evidencia la necesidad del proyecto.

4.5. Puesta en marcha

Finalmente, y con la aprobación de los directivos se comenzó con la puesta en marcha del SGSI-C, implementando los procedimientos planteados, programas de capacitación y por supuesto el registro del control de cambios. La matriz de correlación de la tabla 8 muestra los criterios de validación a través de los anexos.

Tabla 8.
Matriz de correlación ISO/IEC/27017 e ISO/IEC/27001 vs mecanismo de validación

NORMATIVA	CRITERIO	VALIDACIÓN
ISO 27001-2 005: A5. Política de Seguridad	A5.1 Políticas	Implementación de un manual de políticas de seguridad para dar a conocer a todos los miembros de la organización. (Anexo D.1)
ISO 27001-2 005: A6. Organización de la seguridad de la información	A6.1 Organización interna	Acuerdos de confidencialidad firmados por las cabezas de los departamentos. (Anexo D.2)
	A6.2 Entidades externas	Acuerdos que involucren el procesamiento de la información con terceros. (Anexo D.3)
ISO 27001-2 005: A.7 Gestión de activos	A7.1. Responsabilidad por los activos	Inventario actualizado de los activos (Anexo D.4)
ISO 27001-2 005: A.7 Seguridad del recurso humano	A8.1 Antes del empleo	Definir por escrito los roles y responsabilidades de los empleados. (Anexo D.1)
	A8.2 Durante el empleo	
	A8.3 Terminación del contrato	
ISO 27001-2 005: A.9 Seguridad física y ambiental. ISO/IEC 27017:2015: Seguridad física	A9.1.1 Áreas seguras	Señalética y barreras físicas que indiquen áreas seguras. (Anexo D.5)
ISO 27001-2 005: A.11 Control de acceso	A10.3 Planeación y aceptación del sistema	Proyecciones del uso de recursos (Anexo D.6)
ISO/IEC 27017:2015: Controles de acceso	A10.4 Protección contra software malicioso	Implementar procedimientos de control frente a amenazas informáticas. (Anexo D.1)

	A10.5 Procedimientos de respaldo	Mecanismos de respaldo de los servicios ofrecidos (Anexo D.1)
	A10.6 Gestión de seguridad en redes	Revisar periódicamente el estado de la red. (Anexo D.1)
	A11.1 Política de control de acceso	Documento de revisión periódica de la política de control de acceso. (Anexo D.7)
	A11.2 Gestión de acceso al usuario	Controlar la asignación de módulos y roles en el software. (Anexo D.1) Revisar periódicamente los derechos de acceso de sus empleados. (Anexo D.1)
	A11.3 Responsabilidades del usuario	Manual de buenas prácticas de seguridad de la información. Puede asociarse a las políticas del punto 1. (Anexo D.1)
	A11.5 Control de acceso al sistema de operación	Mecanismo de asignación de contraseñas. (Anexo D.8)
	A12.3 Controles criptográficos	Política sobre el uso de criptografía. (Anexo D.1)
	A12.5 Seguridad en los procesos de desarrollo y soporte	Controlar la gestión de cambios. (Anexo D.1) Mitigar las brechas que puedan dar lugar a la filtración de información. (Anexo D.1)
	A12.6.1 Gestión de vulnerabilidad técnica	Valorar continuamente las amenazas a las que se expone la organización. (Anexo D.1)
ISO 27001-2 005: A.13 Gestión de incidentes en la seguridad de la información	A13.1. Reportes de eventos	Los incidentes de seguridad de la información deben documentarse a la brevedad. (Anexo D.1)
ISO 27001-2 005: A.15 Cumplimiento.	A15.1 Cumplimiento con	Toda la documentación debe enmarcarse acorde a la ley vigente en el país

ISO/IEC 27017:2015: Mantenimiento y continuidad del negocio	requerimientos legales	
	A.15.2 Cumplimiento de las políticas y estándares de seguridad y el cumplimento técnico	Debe existir personal encargado de supervisar y guiar en el cumplimiento de los procedimientos planteados
	A.15.3 Consideraciones de auditoria de los sistemas de información	Programar auditorías en intervalos que no irrumpan con las actividades comerciales del negocio. (Anexo D.7)

Nota: Elaboración propia. Tomado de (ISO Security, 2015)

4.6. Mejora continua del Sistema de Gestión de Seguridad de la Información de Servicios en la Nube

Es necesario llevar a cabo un monitoreo y control periódico del SGSI-C propuesto, por cuanto debe adaptarse a los riesgos, eventos y normativa legal vigente, a fin de que la integridad, confidencialidad y disponibilidad de la información no se vea afectada. Por tanto, el Departamento encargado de Seguridad será quien esté a la cabeza y proponga una gestión de cambios de ser el caso.

La etapa de mejora continua estará conformada por sub fases que tendrán que optimizarse o a su vez implementarse, así se tiene en la figura 11:

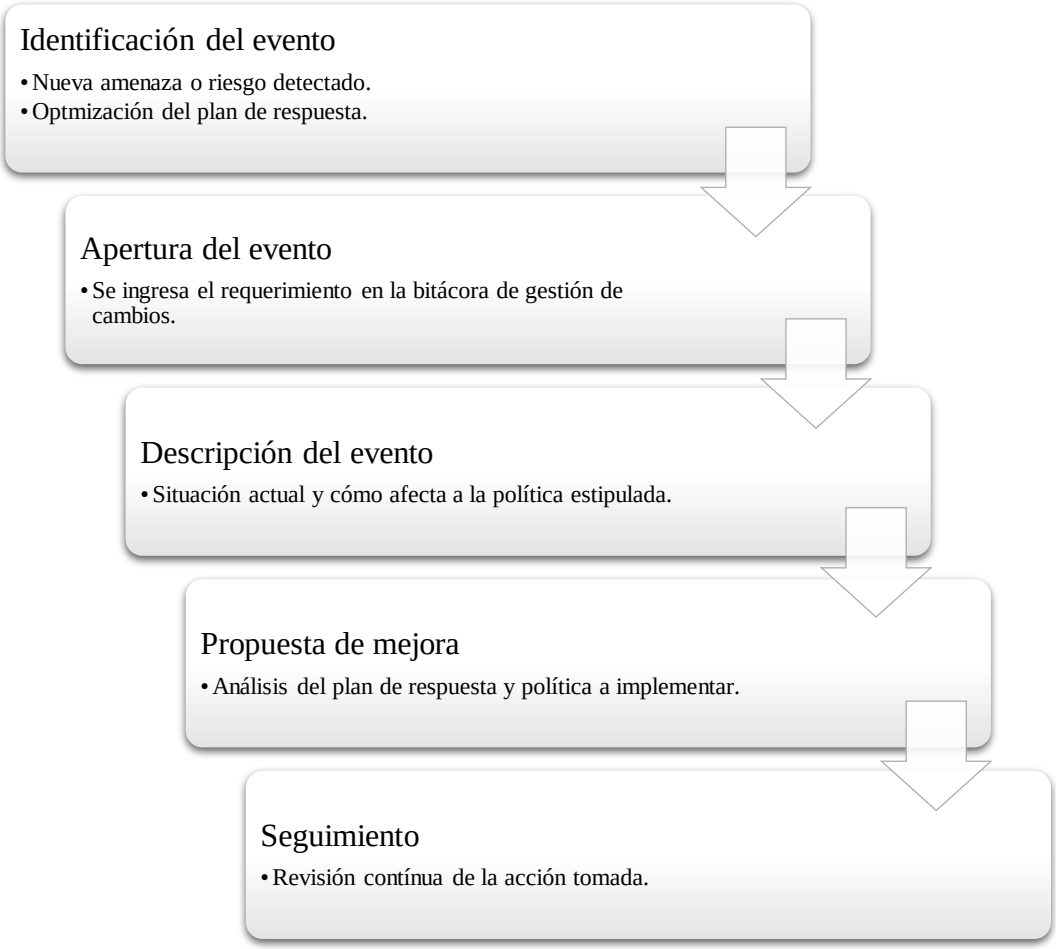


Figura 12. ***Mejora continua del SGSI-C***
Nota: Elaboración propia.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

La seguridad de la información para servicios en la nube requiere complementarse con el Sistema de Gestión de Seguridad de la información, de modo que, no solo se tomen en cuenta los aplicativos en la nube, sino más bien comprenda todos los recursos de la organización.

Las políticas planteadas en el presente trabajo de investigación responden a los criterios revisados en las normativas vigentes ISO/IEC 27001 para la seguridad de la información y las buenas prácticas para la información en la nube de ISO/IEC 27017 tomando como base el análisis de riesgos desarrollados en el marco referencial.

A la fecha en el país no existe una normativa legal vigente exclusiva para la protección de datos en la nube, por lo tanto, cuando MASIVA desee obtener su certificación bajo la normativa ISO/IEC 27017 será necesario revisar el punto de compliance o cumplimiento con requisitos legales y contractuales para no interferir con la legislación del Ecuador.

Masiva Cía Ltda, al ser una organización en crecimiento debe levantar su manual de procedimientos tomando en cuenta el Sistema de Gestión de Seguridad de la Información en la nube que se expone en el documento, del cual se desprende que actualmente cumple con nueve (9) de los catorce criterios de seguridad (14).

Masiva Cía Ltda, presenta un nivel de cumplimiento del 80% de cada uno de los criterios asociados a un cumplimiento “alto”, 15% a “criterios por mejorar” y 5% de cumplimiento escaso.

5.1. Recomendaciones

Para empresas, como cualquier nueva tecnología, los primeros en adoptar la computación en la nube intentan ganar ventaja competitiva dejando de lado los documentos que estipulen políticas claras. De esta manera se sugiere a las empresas en crecimiento desarrollar sus políticas basándose en estándares internacionales que permitan posteriormente avalar sus procedimientos al obtener una certificación.

Es fundamental para los prestadores de servicios en la nube esclarecer los límites de los servicios en la nube a prestar, y mantenerse actualizados en cuanto a mecanismos, metodologías, normas y estándares de gestión de la seguridad a fin de evitar conflictos legales y por supuesto salvaguardar los datos alojados de sus clientes con integridad, disponibilidad y confidencialidad.

La complejidad de la nube en el entorno informático es reconocido como uno de los factores que exacerban la computación en la nube en temas de seguridad, esto se debe a la utilización de tecnologías como máquinas virtuales, bases de datos, soporte de middleware, medición de recursos, replicación de datos, entre otros, que se combinan para fabricar computación en la nube. Es por ello que conviene levantar y definir políticas y roles de seguridad que abarquen todos los involucrados, esto incluye “a terceros”, como proveedores de servicios o subcontratistas.

Las organizaciones deben mejorar sus procesos de gestión de seguridad de la información periódicamente y por consiguiente retroalimentar su SGSI-C para lo cual deberán en primer lugar identificar los activos de seguridad de la información para después evaluar los riesgos a los que éstos se exponen y con ello poner en marcha mecanismos de control para reducir los riesgos hasta un nivel “aceptable”; finalmente mantener el monitoreo es vital para mejorar la efectividad de los controles arraigados a los activos de información.

REFERENCIAS BIBLIOGRÁFICAS

AWS. (2020). *aws.amazon*. Obtenido de aws.amazon: https://aws.amazon.com/es/compliance/iso-27017-faqs/

Beltrán, M., & Sevillano, F. (2013). *Cloud computing tecnología y negocio.* Madrid: Paraninfo.

BSI. (2019). Controles de Seguridad para Servicios Cloud. *bsigroup*.

COIP. (2018). Código ornánico integral penal. *Coip Asamblea Nacional del Ecuador*.

FSA LATAM: Security Business Intellingence. (2016). Obtenido de https://www.sites.oas.org/cyber/Documents/2016%20-%20Seguridad%20en%20la%20Nube%20Continuidad%20Operacional-Julio%20Balderrama.pdf

Gartner. (2019). *Gartner Forecasts Worldwide Public Cloud*. Obtenido de Gartner: https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

Guerra, V. (2019). *Panorama cloud en Ecuador, un futuro de posibilidade*. Obtenido de Datta: https://datta.com.ec/articulo/panorama-cloud-en-ecuador-un-futuro-de-posibilidades

Nist. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *Nist.*

Plan Nacional de Desarrollo . (2017). Plan Nacional de Desarrollo 2017-2021. *Constitución de la República del Ecuador*.

Sasko, R., Magdalena, K., & Marjan, G. (2015). Information Security Management System for Cloud Computing.

AWS. (2021a). AWS Amazon. Retrieved from https://aws.amazon.com/es/about-aws/

AWS. (2021b). Data protection in AWS Identity and Access Management. Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/data-protection.html

Cabacas, T. (2018). ¿Qué es la nube híbrida y por qué no paras de oír hablar de ella? Retrieved from https://www.muycomputerpro.com/2018/07/12/que-es-nube-hibrida

Cardona, O. D. (2015). *Los desastres no son naturales*.

Cloudfare. (2020). What Is a Public Cloud? | Public vs. Private Cloud. Retrieved from https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/

Cornejo, A., & Díaz, C. (2015). *Analisis,Diseño E Implementacion De Cloud Computig Para Una Red De Voz Sobre Ip*. 136. Retrieved from http://dspace.ups.edu.ec/bitstream/123456789/7921/1/UPS-CT004762.pdf

Creative, L., & Atribuci, C. (2021). *Guía para la notificación de brechas de datos personales*.

Ecuador, A. N. del. (2021). *Ley Orgánica de Protección de Datos Personales*.

Ferraiolo, D. (2016). Cloud Computing. Retrieved from https://csrc.nist.gov/projects/cloud-computing

GCP. (2021). Google Cloud services that are in scope for ISO/IEC 27001. Retrieved from https://cloud.google.com/security/compliance/iso-27001#:~:text=Google Cloud Platform%2C our Common,as ISO%2FIEC 27001 compliant.

GDPR. (2018). Personal Data Breaches. Retrieved from https://tietosuoja.fi/en/personal-data-breaches

Hodan M, M., & Lama A, A. (2016). Computación en la nube: arquitectura y sistema operativo. *Cumbre Mundial Sobre Tecnología Informática y de La Información (GSCIT)*. Retrieved from https://www.semanticscholar.org/paper/Cloud-Computing%3A-Architecture-and-Operating-System-Musse-Alamro/2c896bba7af1beaeb8ae54d88e32ec12e25be2e2/figure/0

IEEE. (2020). Standards in Cloud Computing. Retrieved from https://cloudcomputing.ieee.org/standards

ISO Security. (2015). ISO / IEC 27017: 2015. Retrieved from https://www.iso27001security.com/html/27017.html

Joyanes. (2016). Computación en la nube. *Revista Del Instituto Español de Estudios Estratégicos*.

Kirsch, D., & Hurwitz, J. (n.d.). *Cloud Computing for dummies*. Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=F93aDwAAQBAJ&oi=fnd&pg=PA3&dq=cloud+computing&ots=3aZeQuLsQ4&sig=_LpB1jWuvzH5KG-Lfq4UBVhORoM&redir_esc=y#v=onepage&q=cloud computing&f=false

Marinescu, D. C. (2018). *Cloud Computing: Theory and Practice*. Retrieved from https://books.google.es/books?hl=es&lr=&id=O9smDwAAQBAJ&oi=fnd&pg=PP1&dq=cloud+computing&ots=NOpWKyqTwQ&sig=hlN6rxvGWaOJiEk65ZFj_zfaNfc#v=onepage&q=cloud computing&f=false

Martial, C. (2020). IASS PAAS SAAS. Retrieved from https://cloudmartial.com/iaas-paas-saas/

Microsoft. (2021). Empowerment begins with trust. Retrieved from https://www.microsoft.com/en-us/trust-center

Microsoft Azure. (2020). Azure is now certified for the ISO/IEC 27701 privacy standard. Retrieved from https://azure.microsoft.com/en-us/blog/azure-is-now-certified-for-the-iso-iec-27701-privacy-standard/

Microsoft Azure. (2021). Retrieved from https://azure.microsoft.com/en-gb/

Office of the Data Protection. (2018). *personal-data-breaches*. Retrieved from https://tietosuoja.fi/en/personal-data-breaches

Puri, G. S., Tiwary, R., & Shukla, S. (2019). A review on cloud computing. *Proceedings of the 9th*

International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019, 63–68. https://doi.org/10.1109/CONFLUENCE.2019.8776907

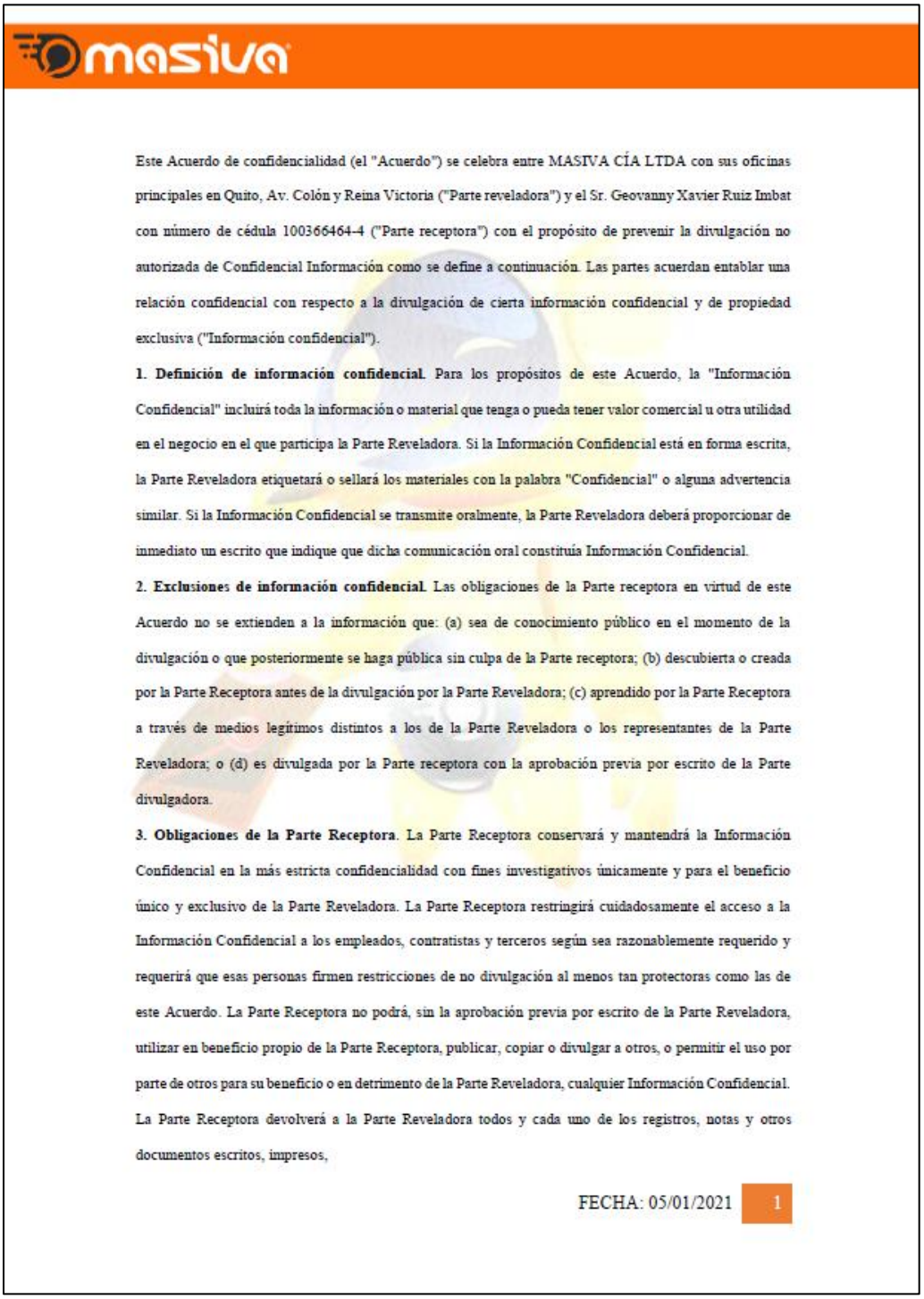
Security Homeland. (2018). Cloud Security Guidance. *Security*, (February), 1–22. Retrieved from https://www.ncsc.gov.uk/collection/cloud-security

The Huffpost. (n.d.). Why the Cloud Has a Security Problem. *2017*. Retrieved from https://www.huffpost.com/entry/why-the-cloud-has-a-secur_b_9093628

Verizon. (2016). 2016 Data Breach Investigations Report. *Verizon Business Journal*, (1), 1–65. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

ANEXOS

ANEXO A: Acuerdo de confidencialidad



masiva

Este Acuerdo de confidencialidad (el "Acuerdo") se celebra entre MASIVA CÍA LTDA con sus oficinas principales en Quito, Av. Colón y Reina Victoria ("Parte reveladora") y el Sr. Geovanny Xavier Ruiz Imbat con número de cédula 100366464-4 ("Parte receptora") con el propósito de prevenir la divulgación no autorizada de Confidencial Información como se define a continuación. Las partes acuerdan entablar una relación confidencial con respecto a la divulgación de cierta información confidencial y de propiedad exclusiva ("Información confidencial").

1. Definición de información confidencial. Para los propósitos de este Acuerdo, la "Información Confidencial" incluirá toda la información o material que tenga o pueda tener valor comercial u otra utilidad en el negocio en el que participa la Parte Reveladora. Si la Información Confidencial está en forma escrita, la Parte Reveladora etiquetará o sellará los materiales con la palabra "Confidencial" o alguna advertencia similar. Si la Información Confidencial se transmite oralmente, la Parte Reveladora deberá proporcionar de inmediato un escrito que indique que dicha comunicación oral constituía Información Confidencial.

2. Exclusiones de información confidencial. Las obligaciones de la Parte receptora en virtud de este Acuerdo no se extienden a la información que: (a) sea de conocimiento público en el momento de la divulgación o que posteriormente se haga pública sin culpa de la Parte receptora; (b) descubierta o creada por la Parte Receptora antes de la divulgación por la Parte Reveladora; (c) aprendido por la Parte Receptora a través de medios legítimos distintos a los de la Parte Reveladora o los representantes de la Parte Reveladora; o (d) es divulgada por la Parte receptora con la aprobación previa por escrito de la Parte divulgadora.

3. Obligaciones de la Parte Receptora. La Parte Receptora conservará y mantendrá la Información Confidencial en la más estricta confidencialidad con fines investigativos únicamente y para el beneficio único y exclusivo de la Parte Reveladora. La Parte Receptora restringirá cuidadosamente el acceso a la Información Confidencial a los empleados, contratistas y terceros según sea razonablemente requerido y requerirá que esas personas firmen restricciones de no divulgación al menos tan protectoras como las de este Acuerdo. La Parte Receptora no podrá, sin la aprobación previa por escrito de la Parte Reveladora, utilizar en beneficio propio de la Parte Receptora, publicar, copiar o divulgar a otros, o permitir el uso por parte de otros para su beneficio o en detrimento de la Parte Reveladora, cualquier Información Confidencial. La Parte Receptora devolverá a la Parte Reveladora todos y cada uno de los registros, notas y otros documentos escritos, impresos,

FECHA: 05/01/2021 1

masiva

4. Periodos de tiempo. Las disposiciones de no divulgación de este Acuerdo sobrevivirán a la terminación de este Acuerdo y el deber de la Parte Receptora de mantener la Información Confidencial en forma confidencial permanecerá en vigor hasta que la Información Confidencial ya no califique como un secreto comercial o hasta que la Parte Reveladora envíe una notificación por escrito a la Parte Receptora liberando a la Parte Receptora. de este Acuerdo, lo que ocurra primero.

5. Relaciones. Nada de lo contenido en este Acuerdo se considerará que constituye a cualquiera de las partes socio, empresa conjunta o empleado de la otra parte para cualquier propósito.

6. Divisibilidad. Si un tribunal determina que alguna disposición de este Acuerdo es inválida o inaplicable, el resto de este Acuerdo se interpretará de la mejor manera para lograr la intención de las partes.

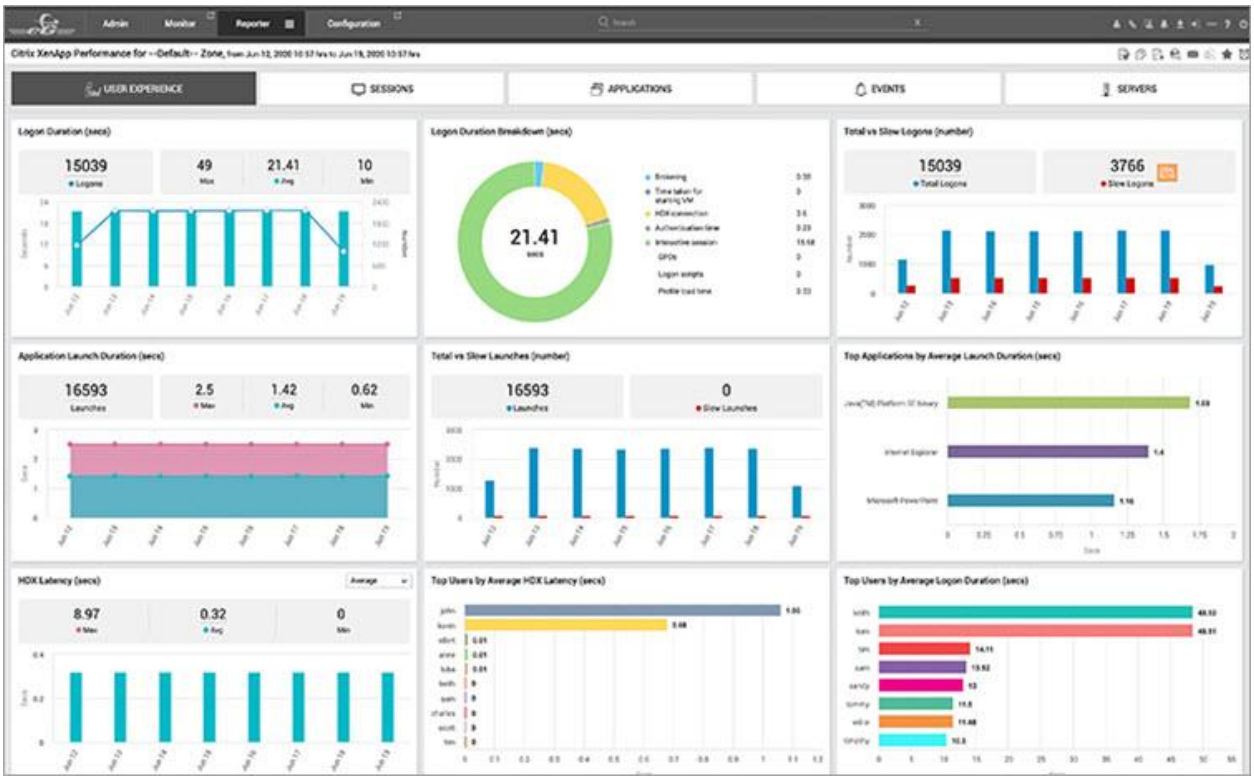
7. Integración. Este Acuerdo expresa el completo entendimiento de las partes con respecto al tema y reemplaza todas las propuestas, acuerdos, representaciones y entendimientos anteriores. Este Acuerdo no puede ser enmendado excepto por escrito firmado por ambas partes.

8. Renuncia. La falta de ejercicio de cualquier derecho provisto en este Acuerdo no será una renuncia a derechos anteriores o posteriores.

Este Acuerdo y las obligaciones de cada parte serán vinculantes para los representantes, cesionarios y sucesores de dicha parte. Cada parte ha firmado este Acuerdo a través de su representante autorizado.

MASIVA	Geovanny Xavier Ruiz Imbat
Parte reveladora	Parte receptora

ANEXO B: Reporte de monitoreo



ANEXO C: Acuerdo de nivel de servicio

masiva

Acuerdo de nivel de servicio (SLA)

Introducción

Este acuerdo de nivel de servicio (SLA) describe los niveles de servicio que nombre de la empresa ('el cliente') recibirá de MASIVA ('el proveedor').

Este SLA debe leerse junto con el contrato de soporte de TI entre el cliente y el proveedor. Aunque el SLA cubre áreas clave de los sistemas de TI y el soporte del cliente, el contrato de soporte puede incluir áreas no cubiertas por este SLA.

Objetivo

El cliente depende de los equipos, software y servicios de TI (en conjunto: "el sistema de TI") que proporciona, mantiene y respalda el proveedor. Algunos de estos elementos son de vital importancia para el negocio.

Este acuerdo de nivel de servicio establece qué niveles de disponibilidad y soporte se garantiza que el cliente recibirá para partes específicas del sistema de TI. También explica qué sanciones se aplicarán al proveedor en caso de que no cumpla con estos niveles.

Este SLA forma una parte importante del contrato entre el cliente y el proveedor. Su objetivo es permitir que las dos partes trabajen juntas de manera efectiva.

Alcance

Partes:

Este SLA se encuentra entre:

El cliente:	**El proveedor:**
(Datos del cliente)	Datos de MASIVA

Periodo de vigencia

Este acuerdo comienza el **fecha** y tendrá una duración de **número meses.**

Puede revisarse en cualquier momento, de común acuerdo. También se puede revisar si hay algún cambio en el sistema de TI del cliente .

Equipo, software y servicios cubiertos

Este SLA cubre solo el equipo, el software y los servicios de la siguiente tabla . Esta lista puede actualizarse en cualquier momento, con el acuerdo tanto del cliente como del proveedor.

Tenga en cuenta:

- El proveedor garantiza **tiempos de respuesta** para todos los artículos enumerados en esta sección .
- El proveedor garantiza el **tiempo de actividad** solo para los artículos con una marca en la casilla ¿ **Cubierto por tiempo de actividad ?**

A estos elementos se les ha asignado un nivel de prioridad, de 1 (más importante) a 3 (menos importante). Los niveles de prioridad ayudan a determinar el tiempo de actividad y el tiempo de respuesta garantizados .

masiva

Tipo de artículo	Número de ítems	Prioridad	¿Cubierto por tiempo de actividad?
Servicios de mensajería	1	1	☐
Agregue elementos adicionales según sea necesario	Número	Prioridad	☐

Exclusiones

El proveedor siempre hará todo lo posible para corregir cada problema de manera oportuna. Sin embargo, existen algunas exclusiones. Este SLA no se aplica a:

- Cualquier equipo , sofrware, servicios u otras partes del sistema de TI que no se enumeradas anteriormente.
- Software, equipos o servicios que no se compró o gestionó por el proveedor

Adicionalmente, este SLA no aplica cuando:

- El problema ha sido causado por el uso de equipos, software o servicio (s) en una forma que se **no se recomienda.**
- El cliente ha realizado **cambios no autorizados** en la configuración o la instalación de los equipos, sofrware o servicios afectados.
- El cliente ha impedido que el proveedor **realice las** tareas de **mantenimiento y actualización necesarias** .
- El problema ha sido causado por equipos, sofrware u otros servicios **no compatibles** .

Este SLA no se aplica en circunstancias de las que se pueda razonablemente decir que están fuera del control del proveedor. Por ejemplo: inundaciones, guerras, casos fortuitos, etc.

Este SLA tampoco se aplica si el cliente incumple su contrato con el proveedor por cualquier motivo (por ejemplo, pago tardío de las tarifas).

Habiendo dicho todo eso, proveedor tiene como objetivo ser útil y complaciente en todo momento, y hará todo lo posible para ayudar al cliente siempre que sea posible.

Responsabilidades

Responsabilidades del proveedor

El proveedor proporcionará y mantendrá el sistema de TI utilizado por el cliente. El contrato de soporte de TI entre el proveedor y el cliente incluye todos los detalles de estas responsabilidades.

Además, el proveedor:

- Asegúrese de que el sofrware, los servicios y los equipos relevantes estén disponibles para el cliente de acuerdo con los niveles de tiempo de actividad que se indican a continuación.
- Responder a las solicitudes de soporte dentro de los plazos que se enumeran a continuación.
- Tome medidas para escalar y resolver problemas de manera adecuada y oportuna .
- Mantener una buena comunicación con el cliente en todo momento.

Responsabilidades del cliente

El cliente utilizará el sistema de TI proporcionado por el proveedor según lo previsto. El contrato de soporte de TI entre el proveedor y el cliente incluye detalles completos del sistema de TI y sus usos previstos .

Además, el cliente:

- Notifique al cliente de problemas o problemas de manera oportuna.
- Proporcionar al proveedor acceso a equipos, software y servicios con fines de mantenimiento, actualizaciones y prevención de fallas.
- Mantener una buena comunicación con el proveedor en todo momento.

Tiempo de actividad garantizado

Niveles de tiempo de actividad

Para permitir al cliente hacer negocios de manera efectiva, el proveedor garantiza que ciertos artículos estarán disponibles durante un cierto porcentaje de tiempo.

Estos niveles de tiempo de actividad se aplican a los elementos de la tabla a continuación.

El nivel de tiempo de actividad garantizado depende del nivel de prioridad de cada elemento:

Nivel de prioridad	Tiempo de actividad garantizado
1	99,9%
2	99,5%
3	99%

Medición y sanciones

El tiempo de actividad se mide el sistemas automatizados usando del proveedor, a través de cada mes. Se calcula al minuto más cercano, basado en la cantidad de minutos en el mes dado (por ejemplo, un mes de 31 días contiene 44,640 minutos).

Si el tiempo de actividad de cualquier artículo cae por debajo del umbral correspondiente, se aplicará una penalización en forma de crédito para el cliente.

Esto significa que la tarifa del mes siguiente pagadera por el cliente se reducirá en una escala móvil.

El nivel de penalización se calculará en función de la cantidad de horas durante las cuales el servicio no estuvo disponible, menos el tiempo de inactividad permitido por el SLA:

Nivel de prioridad	Penalización por hora (prorrateado al minuto más cercano)
1	5% de la tarifa mensual total
2	2% de la tarifa mensual total
3	1% de la tarifa mensual total

Notas importantes:

- Las multas por tiempo de actividad en cualquier mes tienen un límite del 50% de la tarifa mensual total

masiva

- Las mediciones de tiempo de actividad excluyen los períodos de mantenimiento de rutina. Estos deben acordarse previamente entre el proveedor y el cliente.

Tiempos de respuesta garantizados

Cuando el cliente plantea un problema de soporte con el proveedor, el proveedor se compromete a responder de manera oportuna.

Tiempos de respuesta

El tiempo de respuesta mide cuánto tiempo le toma al proveedor responder a una solicitud de soporte planteada a través del sistema de soporte en línea del proveedor.

Se considera que el proveedor ha respondido cuando responde a la solicitud inicial del cliente. Esto puede ser en forma de correo electrónico o llamada telefónica, para brindar una solución o solicitar más información.

Los tiempos de respuesta garantizados dependen de la prioridad de los artículos afectados y de la gravedad del problema. Se muestran en esta tabla:

		Gravedad del problema (consulte la sección **Niveles de gravedad** , a continuación)			
		Fatal	Grave	Medio	Menor
Prioridad de artículo	1	15 minutos	15 minutos	30 minutos	60 minutos
	2	30 minutos	30 minutos	45 minutos	60 minutos
	3	60 minutos	60 minutos	75 minutos	90 minutos

Los tiempos de respuesta se miden desde el momento en que el cliente envía una solicitud de soporte a través del sistema de soporte en línea del proveedor.

Los tiempos de respuesta se aplican únicamente durante el horario laboral estándar (de 9:00 a. M. A 5:30 p. M.) , A menos que el contrato entre el cliente y el proveedor incluya específicamente disposiciones para el soporte fuera de horario.

Niveles de gravedad

Los niveles de gravedad que se muestran en las tablas anteriores se definen de la siguiente manera:

- **Fatal**: degradación completa: **todos los usuarios y funciones críticas afectadas.** Es un servicio completamente indisponible.
- **Grave**: degradación significativa: **gran número de usuarios o funciones críticas afectadas.**
- **Medio**: degradación **limitada: número limitado de usuarios o funciones afectadas.** Los procesos comerciales pueden continuar.
- **Menor**: pequeña degradación: **pocos usuarios o un usuario afectado.** Los procesos comerciales pueden continuar.

Medición y sanciones

masiva

Los tiempos de respuesta se miden utilizando el sistema de tickets de soporte del proveedor, que rastrea todos los problemas desde el informe inicial hasta la resolución.

Es vital que el cliente plantee todos los problemas a través de este sistema. Si un problema no se produce de esta manera, el tiempo de respuesta garantizado no es se aplica a esa cuestión.

Si el proveedor no cumple con una respuesta garantizada, se aplicará una penalización en forma de crédito para el cliente.

Esto significa que la tarifa del mes siguiente pagadera por el cliente se reducirá en una escala móvil.

El nivel de penalización se calculará en función de la cantidad de horas en las que el proveedor perdió el tiempo de respuesta, menos el tiempo de inactividad permitido por el SLA:

Nivel de prioridad	**Penalización por hora** (prorrateado al minuto más cercano)
1	5% de la tarifa mensual total
2	2% de la tarifa mensual total
3	1% de la tarifa mensual total

Notas importantes:

- Las multas por tiempo de respuesta en cualquier mes tienen un límite del 50% de la tarifa mensual total
- Los tiempos de respuesta se miden durante el horario laboral (9 a. M. - 5 .30 p. M.).

  Por ejemplo, si se informa un problema en 5 . 00 pm con un tiempo de respuesta de 6 0 minutos, el proveedor tiene hasta las 9.30 am del día siguiente para responder.

Tiempos de resolución

El proveedor siempre se esforzará por resolver los problemas lo más rápidamente posible. Reconoce que los sistemas informáticos del cliente son clave para su negocio y que cualquier tiempo de inactividad puede costar dinero.

Sin embargo, el proveedor no puede proporcionar tiempos de resolución garantizados. Esto se debe a que la naturaleza y las causas de los problemas pueden variar enormemente.

Por ejemplo, puede ser posible resolver un problema fatal del servidor en minutos, simplemente reiniciando el servidor. Pero si un servidor falla debido a un error de disco o una falla de hardware (también clasificado como un problema fatal), puede llevar mucho más tiempo volver a funcionar.

En todos los casos, el proveedor hará todo lo posible para resolver los problemas lo antes posible. También proporcionará informes de progreso frecuentes al cliente.

Terminación del contrato

El proveedor reconoce que brinda servicios que son críticos para el negocio del cliente.

Si el proveedor constantemente no cumple con los niveles de servicio descritos en este documento, el cliente puede rescindir todo su contrato con el proveedor, sin penalización.

Este derecho está disponible para el cliente si **el proveedor no cumple con estos niveles de servicio más de cinco veces en un solo mes calendario.**

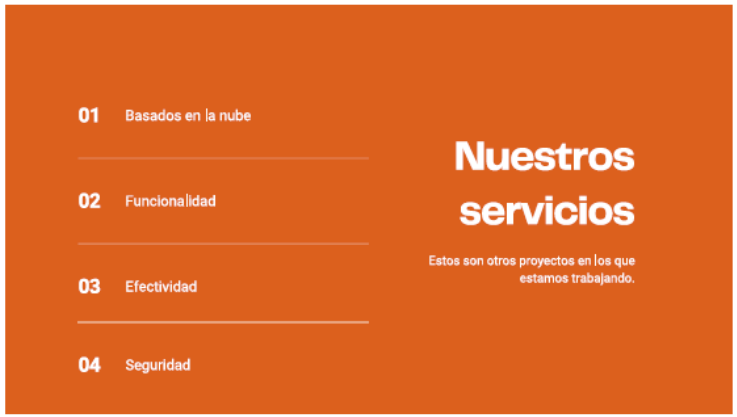
Firmas

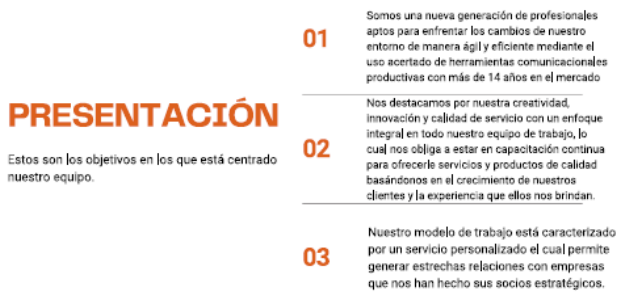
Este acuerdo de nivel de servicio se acuerda como parte del contrato de soporte de TI entre nombre del cliente y nombre del proveedor:

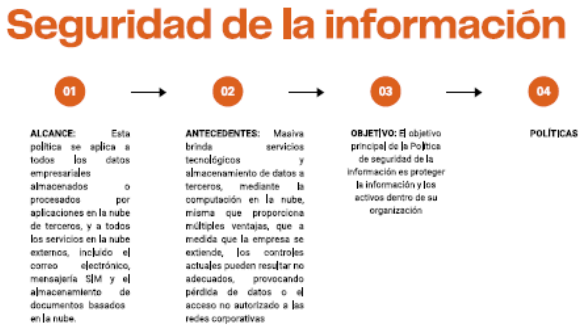
MASIVA	.....
PROVEEDOR	**CLIENTE**

ANEXO D: Documentos de validación de políticas de seguridad

Anexo D.1: Manual de políticas del SGSI-C







01

ORGANIZACIÓN DE LA SERGURIDAD DE LA INFORMACIÓN

Implementación de Acuerdos de Nivel de Servicio SLA

Constituye un documento de negocio entre proveedor y cliente, en el cual se conceptualizan las especificaciones técnicas más relevantes en relación con los requerimientos funcionales, las variables monetarias y la calidad del servicio que se regirá durante el periodo de validez acordado

Contiene las siguientes partes: acuerdo entre las partes, periodo de vigencia, servicios cubiertos, exclusiones, responsabilidades del proveedor y cliente, tiempos de respuesta, sanciones, derecho a la terminación del contrato, firmas.

02

SEGURIDAD DEL RECURSO HUMANO

CAPACITACIONES A NUESTROS COLABORADORES

Algunas amenazas a la seguridad de los datos llegan a través de la red, como la piratería informática, sin embargo, existen formas más insidiosas en las que se puede violar la privacidad

MASIVA se compromete a proporcionar capacitaciones periódicas a nuestros colaboradores, que permitan evitar ataques de ingeniería social u otros

03

CONTROL DE AUTENTICACIÓN

EVITAR EL ACCESO NO AUTORIZADO

Las regulaciones de control interno evitan el acceso no autorizado a sus activos en la nube, permitiendo el acceso solo a personas que tengan una necesidad real de recursos.

MASIVA se compromete a gestionar el control de autenticación con las políticas:
-Nuestros colaboradores deberán modificar contraseñas de forma regular, y especificar cuándo y dónde se puede acceder a los datos.
-Minimizar las credenciales con permisos de superadministrador y establecer perfilamientos según las necesidades de cada usuario.
-Utilizar un factor de autenticación múltiple, que permita asegurar el uso adecuado de credenciales en la nube.

04

CRIPTOGRAFÍA

CLAVES DE ACCESO CLIENTE – PROVEEDOR

El cifrado y almacenamiento de los datos tienen que ser examinado para que solo el personal autorizado tenga acceso a la información

-Utilizar claves de acceso para proveedor y cliente, así como no utilizar las mismas para todos los activos.
-Indicar la vigencia de las llaves criptográficas durante el ciclo de vida.
-Revisar la normativa vigente de criptografía NIST SP-800-57, ANSI X9.69 y ANSI X9.73.

05

SEGURIDAD FÍSICA

INFRAESTRUCTURA FÍSICA

MASIVA como el proveedor de servicios en la nube es quien asume la seguridad física de los servicios ofrecidos, por esto, es necesario implementar políticas y controles de ingreso físico que aseguren el bienestar de los activos

-Masiva debe cumplir con las buenas prácticas y regulaciones de la infraestructura física.
-Las cargas de trabajo a las que son sometidos los conjuntos físicos puede producir lentitud, bloqueos y cuellos de botella una vez que superan sus habilidades, por esto se tienen que conocer las restricciones y habilidades, para que los administradores logren configurarlas de manera correcta.

06

SEGURIDAD LÓGICA

EVITAR ATAQUES

Tomamos las medidas necesarias para desarrollar y testar amenazas de seguridad contra nuestros sistemas asegurando la protección de sus datos.

-Configuraciones a nivel de dispositivos intermedios también resultan válidas, como por ejemplo la utilización de cortafuegos o detectores de intrusos.

07

DESARROLLO Y MANTENIMIENTO

ASEGURAR LA CONTINUIDAD DEL NEGOCIO

Masiva se encargará de proporcionar copias de seguridad automáticas de datos de sus clientes.

Si una estación de trabajo o un dispositivo se bloquea o pierde energía mientras se trabaja, los datos que se ingresaron en la aplicación en la nube se guardan automáticamente hasta el momento de la interrupción. Una vez que se reinicia el dispositivo (o se restauran las conexiones de red o de energía), los empleados pueden retomar el trabajo desde donde comenzaron.

08

REDUNDANCIA

PROCEDIMIENTOS DE BACKUP

Masiva garantiza la integridad de la información.

Los repositorios de datos basados en la nube MASIVA deberán recuperarse o regenerarse automáticamente, si se pierden o el servicio en la nube los descarta intencionalmente o inadvertidamente, para ello se hace uso de sus servidores en modo espejo.

09

GESTIÓN DEL CUMPLIMIENTO

MONİTOREO CONSTANTE

Masiva asegurará la revisión de sus políticas de seguridad garantizando una correcta gestión del cumplimiento

Información de contacto

Email: info@masiva.ec

Av. Colón E6-49 y Reina Victoria
Quito-Ecuador
Código Postal: 170522
Phone: +593 (2) 2502058
Movil: +593987777007

Anexo D.2: Acuerdo de confidencialidad para empleados internos

masiva

ACUERDO DE CONFIDENCIALIDAD ANEXO AL CONTRATO No.....

Confidencialidad

(a) Sujeto a las siguientes Subcláusulas, la parte trabajadora mantendrá la confidencialidad y no deberá, sin el consentimiento previo por escrito de la otra parte, revelar a ningún tercero los términos y condiciones del Contrato o cualquier documento u otra información proporcionada directa o indirectamente por cualquiera de las Partes en relación con el Contrato o los Servicios, independientemente de si dicha información se ha proporcionado antes de la celebración del Contrato o en cualquier momento.

(b) La parte trabajadora únicamente podrá divulgar los términos y condiciones del Contrato y cualquier documento e información que haya adquirido en virtud del Contrato o en virtud del mismo sin el consentimiento previo por escrito de la otra Parte si dicha divulgación se realiza de buena fe:

  (a) en la medida requerida por las leyes aplicables;

  (b) a cualquier asegurador bajo una póliza de seguro emitida de conformidad con el Contrato;

  (c) a sus órganos internos, incluidos sus directores, empleados y funcionarios y la Asamblea General en el caso del Empleador;

  (d) a cualquier Subcontratista para el cumplimiento de las obligaciones de esa Parte en virtud del Contrato;

  (e) a consultores o asesores externos contratados por o en nombre de la Parte reveladora y que actúen en esa capacidad en relación con los Servicios (incluidos los asesores legales, fiscales y de seguros); o

  (f) a las autoridades competentes de los Estados miembros de conformidad con las obligaciones del empleador en virtud de la Convención sobre Prerrogativas e Inmunidades de las Naciones Unidas.

(c) Las obligaciones en virtud de esta Subcláusula no se aplicarán a la información y los documentos que:

  (a) ahora o en el futuro han ingresado al dominio público sin culpa de la Parte reveladora; o

  (b) de lo contrario, estar legalmente disponible para la Parte reveladora de un tercero sin obligación de confidencialidad.

(d) Esta Subcláusula sobrevivirá a la expiración o terminación del Contrato.

Debidamente autorizado para firmar el Contrato para y en nombre del Empleador, MASIVA CÍA LTDA:

En la presencia de: _____

Firma _____ (testigo)

Habla a _____

Ocupación _____

FIRMADO POR _____

Debidamente autorizado para firmar el Contrato en nombre y representación del Trabajador:

En la presencia de: _____

Firma _____(testigo)

Habla a _____

Ocupación _____

Anexo D.3: Acuerdo de confidencialidad para terceros

masiva

ACUERDO DE CONFIDENCIALIDAD ANEXO AL CONTRATO No.....

1.1 Derechos de propiedad intelectual de terceros (DPI)

(a) Si los DPI del Tercero forman parte de los Servicios o son necesarios para el funcionamiento o el funcionamiento de los Entregables, el cliente o tercero se asegurará de que a MASIVA CÍA LTDA se le otorgue una licencia para usar dichos derechos considerando:

(a) evaluación del desempeño de los Servicios;

(b) la operación, soporte y mantenimiento

1.2 Sistema de gestión de documentos del empleador

(a) Además de las obligaciones expuestas en el contrato suscrito, si el cliente lo solicita, MASIVA cargará copias de todos los avisos, instrucciones y otras comunicaciones en virtud del Contrato en el Sistema de gestión de documentos del Contratante.

(b) MASIVA proporcionará a su cliente la capacitación necesaria para el uso del servicio brindado, según lo solicite razonablemente el cliente, para permitirle cumplir con sus propósitos.

1.3 Confidencialidad

(a) Sujeto a las siguientes Subcláusulas, las Partes mantendrán la confidencialidad y no deberán, sin el consentimiento previo por escrito de la otra Parte, revelar a ningún tercero los términos y condiciones del Contrato o cualquier documento u otra información proporcionada directa o indirectamente por cualquiera de las Partes en relación con el Contrato o los Servicios, independientemente de si dicha información se ha proporcionado antes de la celebración del Contrato o en cualquier momento.

(b) Cualquiera de las Partes podrá divulgar los términos y condiciones del Contrato y cualquier documento e información que haya adquirido en virtud del Contrato o en virtud del mismo sin el consentimiento previo por escrito de la otra Parte si dicha divulgación se realiza de buena fe:

(a) en la medida requerida por las leyes aplicables;

(b) a cualquier asegurador bajo una póliza de seguro emitida de conformidad con el Contrato;

(c) a sus órganos internos, incluidos sus directores, empleados y funcionarios y la Asamblea General en el caso del Empleador;

(d) a cualquier Subcontratista para el cumplimiento de las obligaciones de esa Parte en virtud del Contrato;

(e) a consultores o asesores externos contratados por o en nombre de la Parte reveladora y que actúen en esa capacidad en relación con los Servicios (incluidos los asesores legales, fiscales y de seguros); o

(f) a las autoridades competentes de los Estados miembros de conformidad con las obligaciones del empleador en virtud de la Convención sobre Prerrogativas e Inmunidades de las Naciones Unidas.

(c) Las obligaciones en virtud de esta Subcláusula no se aplicarán a la información y los documentos que:

(a) ahora o en el futuro han ingresado al dominio público sin culpa de la Parte reveladora; o

(b) de lo contrario, estar legalmente disponible para la Parte reveladora de un tercero sin obligación de confidencialidad.

(d) Esta Subcláusula sobrevivirá a la expiración o terminación del Contrato.

Debidamente autorizado para firmar el Contrato para y en nombre del Empleador, MASIVA CÍA LTDA:

En la presencia de: _____

Firma _____ (testigo)

Habla a _____

Ocupación _____

FIRMADO POR _____

Debidamente autorizado para firmar el Contrato en nombre y representación del Trabajador:

En la presencia de: _____

Firma _____(testigo)

Habla a _____

Ocupación _____

Anexo D.4: Inventario de activos

masiva

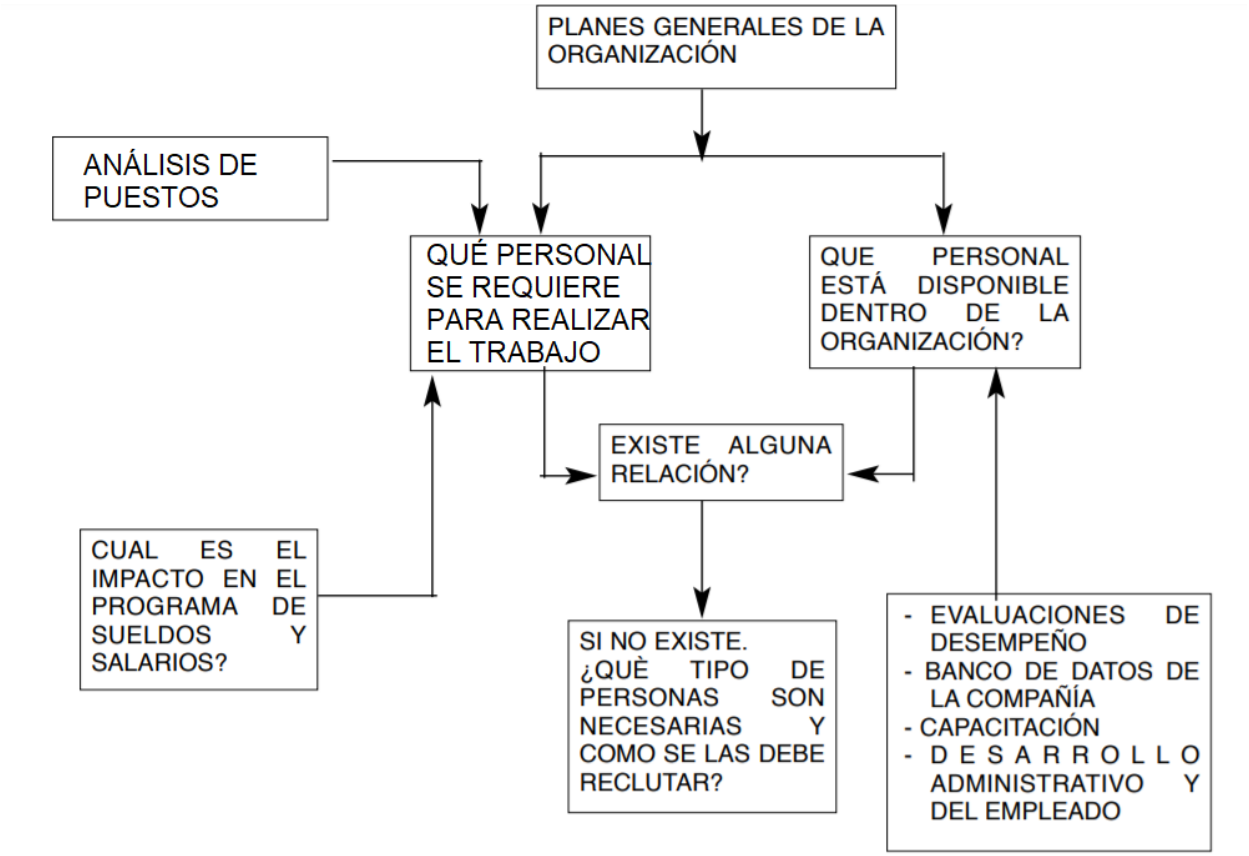
INVENTARIO TECNOLÓGICO MASIVA CÍA LTDA								
							Código: MAS-2021-V1	
							Versión: v1.0	
							Página: 1	
							Fecha: 25/06/2021	
Registro información de activo				Criticidad (1 < 5 más crítico)				
Área	Categoría	Descripción	Características	Confidencial	Integri	Disponibili	Niv	Fecha
DIRECCIÓN GERENCIAL	Activo Tecnológico	PC de escritorio	INTEL CORE I9 - 9980XE				5	10/05/2021
DIRECCIÓN	Activo Tecnológico	PC de escritorio	INTEL CORE I7-7				4	10/05/2021
ADMINISTRACIÓN	Activo Tecnológico	PC de escritorio	INTEL CORE I5				5	10/05/2021
MONITOREO OPERATIVO	Activo Tecnológico	PC de escritorio	INTEL CORE I5				3	10/05/2021
MONITOREO OPERATIVO	Activo Tecnológico	PORTÁTIL	INTEL CORE I5				3	10/05/2021
INNOVACIÓN	Activo Tecnológico	PORTÁTIL	INTEL CORE I5				3	10/05/2021
DIRECCIÓN DE	Activo Tecnológico	PC de escritorio	INTEL CORE I5				4	10/05/2021
SOPORTE TÉCNICO	Activo Tecnológico	PC de escritorio	INTEL CORE I7-7				3	10/05/2021
SOPORTE NIVEL BASICO	Activo Tecnológico	PC de escritorio	INTEL CORE I5				3	10/05/2021
SOPORTE NIVEL	Activo Tecnológico	PC de escritorio	INTEL CORE I5				3	10/05/2021
DESARROLLO	Activo Tecnológico	PC de escritorio	INTEL CORE I5				3	10/05/2021
DIRECCIÓN DE CUENTAS	Activo Tecnológico	PC de escritorio	INTEL CORE I5				3	10/05/2021
VENTAS 1	Activo Tecnológico	PORTÁTIL	INTEL AMD				2	10/05/2021
VENTAS 2	Activo Tecnológico	PORTÁTIL	INTEL AMD				2	10/05/2021
ATENCIÓN AL CLIENTE	Activo Tecnológico	PORTÁTIL	INTEL AMD				2	10/05/2021
SERVICIO AL CLIENTE	Activo Tecnológico	PORTÁTIL	INTER CORE I5				2	10/05/2021
DEPARTAMENTO	Activo Tecnológico	PC de escritorio	RYZEN 2990 WX				5	10/05/2021
FINANZAS	Activo Tecnológico	PC de escritorio	INTEL CORE I5				5	10/05/2021
GESTIÓN TRIBUTARIA	Activo Tecnológico	PC de escritorio	INTEL CORE I3				5	10/05/2021
SERVIDOR	Activo Tecnológico	HP PROLIANT GEN 9	ML110 GEN9				5	10/05/2021
SERVIDOR	Activo Tecnológico	HP PROLIANT GEN 9	ML110 GEB9				5	10/05/2021
SERVIDOR	Activo Tecnológico	HP PROLIANT	ML150 GEN6				5	10/05/2021
SERVIDOR	Activo Tecnológico	HP PROLIANT	ML310E GEN8				5	10/05/2021

Anexo D.5: Implementación de señalética para áreas seguras

Ç


MEDIA
MACHINE
MEDIA
MACHINE
MEDIA
MACHINE

Anexo D.6: Proyecciones de uso de recursos

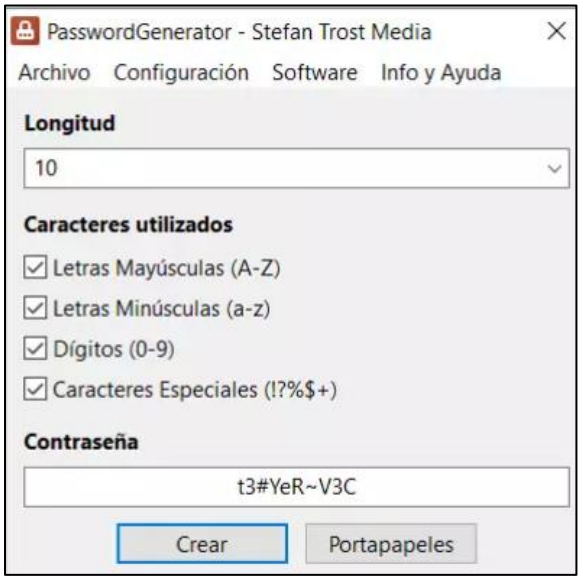


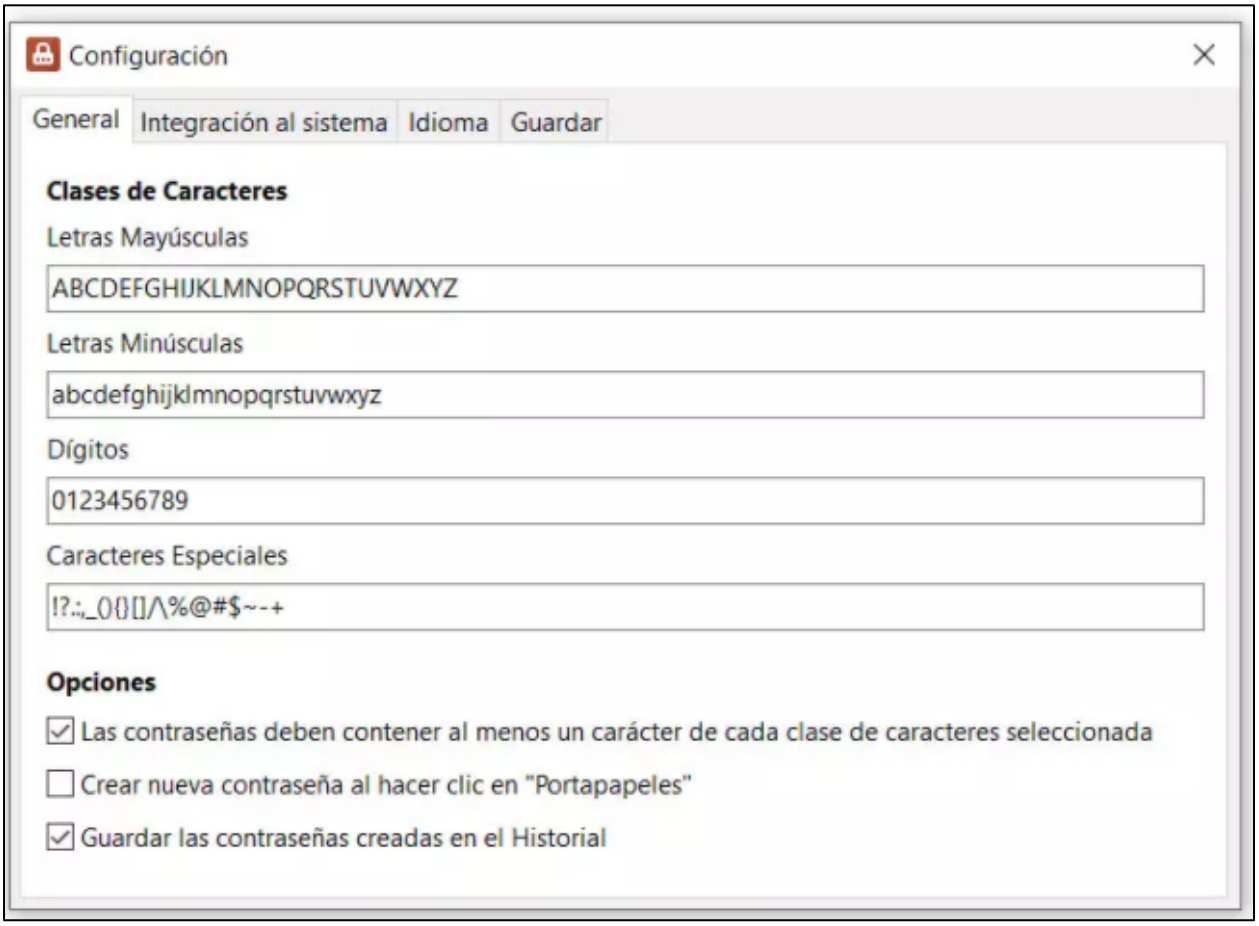
Anexo D.7: Bitácora de auditorías internas y gestión de cambios

masiva	MASIVA CÍA LTDA	Codigo:
	SISTEMA DE GESTION INTEGRADO	Version
	PROCESO: GESTION DE SEGURIDAD DE LA INFORMACIÓN	Fecha: 25-06-2021
	FORMATO: BITACORA DE GESTIÓN DE CAMBIOS Y CONTROLES DE ACCESO	Pag 1 de 1

Fecha Ingreso	Hora Ingreso	Fecha Salida	Hora Salida	Nombre	Identificación	Actividad Realizada	Funcionario Responsable	Firma Ingreso	Firma Salida

Anexo D.8: Mecanismo de asignación de contraseñas





ANEXO E: Matriz de cumplimiento

masiva

			NIVEL DE APLICABILIDAD (1 mín - 5 máx)					
NORMATIVA	CRITERIO	VALIDACIÓN	1	2	3	4	5	OBSERVACIÓN
ISO 27001-2 005: A5. Política de Seguridad	A5.1 Políticas	Implementación de un manual de políticas de seguridad para dar a conocer a todos los miembros de la organización.					X	Se implementó y socializó el manual de políticas internamente
ISO 27001-2 005: A6. Organización de la seguridad de la información	A6.1 Organización interna	Acuerdos de confidencialidad firmados por las cabezas de los departamentos.			X			Se firmaron acuerdos de confidencialidad con el 50% de los gerentes de cada departamento
	A6.2 Entidades externas	Acuerdos que involucren el procesamiento de la información con terceros.				X		Se desarrollaron acuerdos de confidencialidad con los clientes, mismos que se implementarán a partir de la fecha de aprobación
ISO 27001-2 005: A.7 Gestión de activos	A7.1. Responsabilidad por los activos	Inventario actualizado de los activos				X		Se levantó la información de activos actualizada,
ISO 27001-2 005: A.7 Seguridad del recurso humano	A8.1 Antes del empleo	Definir por escrito los roles y responsabilidades de los empleados					X	Se definieron roles para el recurso humano, por escrito en las políticas planteadas.
	A8.2 Durante el empleo						X	
	A8.3 Terminación del contrato						X	
ISO 27001-2 005: A.9 Seguridad física y ambiental.	A9.1.1 Áreas seguras	Señalética y barreras físicas que indiquen áreas seguras.					X	Se implementó señalética para las diferentes áreas
ISO/IEC 27017:2015: Seguridad física							X	
ISO 27001-2 005: A.11 Control de acceso	A10.3 Planeación y aceptación del sistema	Proyecciones del uso de recursos				X		Se planteó un diagrama de flujo para proyectar los recursos
	A10.4 Protección contra software malicioso	Implementar procedimientos de control frente a amenazas informáticas.					X	Se documentó la información que la organización ya manejaba.
ISO/IEC 27017:2015: Controles de acceso	A10.5 Procedimientos de respaldo	Mecanismos de respaldo de los servicios ofrecidos					X	Se documentaron los mecanismos de respaldo que la organización ya manejaba aún si poseer un manual de procedimientos previo.
	A10.6 Gestión de seguridad en redes	Revisar periódicamente el estado de la red.					X	Se propone una bitácora de gestión de control y cambios
	A11.1 Política de control de acceso	Documento de revisión periódica de la política de control de acceso.					X	
	A11.2 Gestión de acceso al usuario	Controlar la asignación de módulos y roles en el software.			X			Procedimiento crítico que está en proceso.
		Revisar periódicamente los derechos de acceso de sus empleados.					X	Se revisaron roles de usuario a la fecha
	A11.3 Responsabilidades del usuario	Manual de buenas prácticas de seguridad de la información. Puede asociarse a las políticas del punto 1.					X	Se implementó y socializó el manual de políticas internamente
	A11.5 Control de acceso al sistema de operación	Mecanismo de asignación de contraseñas.				X		Se propone la utilización de un software para asignación de contraseñas.
	A12.3 Controles criptográficos	Política sobre el uso de criptografía.					X	Se socializan las medidas de seguridad mediante capacitaciones
	A12.5 Seguridad en los procesos de desarrollo y soporte	Controlar la gestión de cambios.					X	
		Mitigar las brechas que puedan dar lugar a la filtración de información.					X	
	A12.6.1 Gestión de vulnerabilidad técnica	Valorar continuamente las amenazas a las que se expone la organización.					X	

ISO 27001-2 005: A.13 Gestión de incidentes en la seguridad de la información	A13.1. Reportes de eventos	Los incidentes de seguridad de la información deben documentarse a la brevedad.					X	Se propone una bitácora de gestión de control y cambios
ISO 27001-2 005: A.15 Cumplimiento.	A15.1 Cumplimiento con requerimientos legales	Toda la documentación debe enmarcarse acorde a la ley vigente en el país					X	
ISO/IEC 27017:2015: Mantenimiento y continuidad del negocio	A.15.2 Cumplimiento de las políticas y estándares de seguridad y el cumplimento técnico	Debe existir personal encargado de supervisar y guiar en el cumplimiento de los procedimientos planteados					X	A partir de la fecha de aprobación se propone registrar la gestión y cumplimiento del sistema de gestión de información de seguridad planteado.
	A.15.3 Consideraciones de auditoria de los sistemas de información	Programar auditorías en intervalos que no irrumpan con las actividades comerciales del negocio.			X			Queda a disposición de la organización, se hacen las debidas sugerencias.

MASIVA

Representante:

CC:

ANEXO F: Socialización del SGSI-C con los directivos de MASIVA