**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**


**Facultad de Ingeniería en Electricidad y Computación**

# “IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD EN BASE A LAS NORMAS DE CALIDAD ISO 27001 PARA UNA EMPRESA DE SERVICIO DE MENSAJES SIMPLES (SMS)”

**TRABAJO DE TITULACIÓN**

**PREVIA A LA OBTENCIÓN DEL TÍTULO DE:**

**MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA**

Presentado por:

GREGORIO ELIAS PAZMIÑO VÉLEZ
LUIS ENRIQUE SÁNCHEZ LOOR

GUAYAQUIL - ECUADOR
2019

## AGRADECIMIENTO

A nuestros padres porque siempre nos apoyaron y nos motivaron para lograr los objetivos que nos hemos propuesto y este trabajo no es la excepción.

Al Ing. Lenin Freire por ser un gran profesional, brindarnos con sus conocimientos y con su guía para la realización de este trabajo.

## DEDICATORIA

A mis padres, a mi hermano y a mis sobrinos que son el pilar fundamental en mi vida, mi gran motivación y esperan que cumpla con todos los objetivos que me proponga.

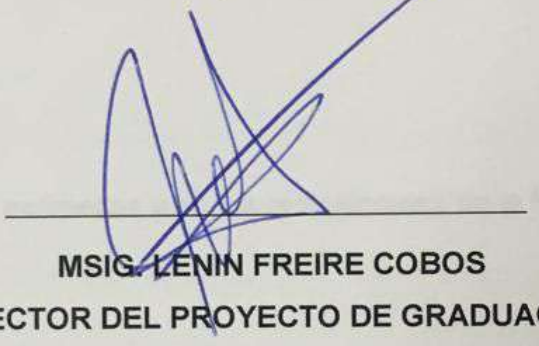
Gregorio Elías Pazmiño Vélez

El presente trabajo es dedicado a mi familia, a mi esposa y a mi futuro hijo quienes han sido parte fundamental en inspiración y esfuerzo para alcanzar la realización de este y posteriores objetivos de mi vida.

Luis Enrique Sánchez Loor

## TRIBUNAL DE SUSTENTACIÓN

MSIG. LENIN FREIRE COBOS
DIRECTOR MSIA



MSIG. LENIN FREIRE COBOS
DIRECTOR DEL PROYECTO DE GRADUACIÓN

MSIG. OMAR MALDONADO DAÑIN
MIEMBRO DEL TRIBUNAL

## DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este trabajo de titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Gregorio Elías Pazmiño Vélez

Luis Enrique Sánchez Loor

# RESUMEN

El trabajo de Titulación muestra el análisis, el desarrollo y la implementación de un esquema de seguridad informático para una empresa que brinda servicio de mensajes simples(SMS). El esquema de seguridad está basado en las normas de calidad ISO 27001:2013 en su versión más reciente la cual es la 2013 emitida por la Organización Internacional de Normalización (ISO).

Toda organización posee información crítica por la cual debe ser protegida ante cualquier tipo de amenaza que no comprometa con su disponibilidad, confidencialidad e integridad por este motivo es recomendable que se implemente un esquema de seguridad para proteger este activo tan valioso hoy en día. La empresa a la cual se le implementó este esquema de seguridad no contaba con políticas claramente definidas y por tal motivo presentaba fallos en la seguridad de la información.

Para llevar a cabo la implementación del esquema de seguridad se usó el método MAGERIT con el fin de gestionar los riesgos residuales e inherentes que están presentes en la organización, para esto se hizo la contextualización de la empresa, es decir, se conoció la información de la infraestructura de la empresa y la organización de la misma para así poder identificar el proceso central por la cual se le va aplicar el esquema de seguridad.

Luego se procedió a realizar un análisis de brecha para conocer la situación actual frente a los riesgos, para continuar con el análisis de riesgo, la cual fueron varios procedimientos a seguir: Identificación de los activos, clasificar los activos por su importancia, se identificaron las amenazas que están presentes en cada activo del proceso central, para poder hacer la debida valoración de las amenazas y por último clasificar los inventarios por la valoración de las amenazas y así realizar la evaluación de riesgos para identificar los riesgos residuales y riesgos inherentes.

Una vez con el análisis de riesgos se realizó la declaración de aplicabilidad con el fin de conocer que controles se pueden aplicar al proceso central y finalizar con el tratamiento de riesgos e implementación de los controles y políticas de seguridad.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

Con el avance de la tecnología y la gran dependencia que se tiene sobre ella, el flujo de información que se tiene físicamente en una empresa cada vez es menor y debido a esto, existe información sensible que se encuentra almacenada en algún dispositivo de almacenamiento de datos como puede ser un disco duro, un pendrive, entre otros, lo que es de alta importancia contar con algún medio de seguridad que garantice que la información esté disponible cuando sea debido, sea íntegro y sea confidencial cuando lo amerite.

La empresa que brinda servicios de mensajería simples(SMS) de manera masiva no es una excepción, esta empresa posee información importante sobre sus clientes, promociones que brindan los clientes y quieren que sea enviado masivamente por SMS, por tal motivo es necesario resguardar esta información ante cualquier tipo de amenaza contra su integridad, confidencialidad y la disponibilidad, siendo la finalidad de este trabajo, la cual consiste en la protección de los datos críticos mediante la implementación de un esquema de seguridad.

El esquema de seguridad planteado sigue las normas de la Organización Internacional de Normalización ISO 27001:2013 en su versión más reciente la 2013, la cual nos ha brindado la metodología adecuada para determinar las carencias y falencias en lo que seguridad respecta, ayudándonos con implementaciones de controles y políticas de seguridad que mitiguen las amenazas que tienen probabilidad

de ocurrir dentro del núcleo central de la empresa la cual es su sistema de envió de mensajería masivo.

Para encontrar los fallos más críticos dentro la empresa, se realizó el respectivo análisis de riesgo y después haciendo un análisis de brechas sobre el proceso de mayor importancia para ellos, con el fin de determinar cómo se encuentra la empresa antes de que se le implemente el esquema de seguridad, con esta información se procedió a desarrollar e implementar el esquema de seguridad que se ajusta a las necesidades de la empresa.

# CAPÌTULO 1

# GENERALIDADES

## 1.1 ANTECEDENTES

El principal negocio de la empresa es la mensajería masiva, esto es, el envío de mensajes de texto a destinatarios independientemente de la operadora de celular que estén suscritos. El cliente puede subir hojas electrónicas en Excel por medio de un portal web o enviar requerimientos de envío mediante un servicio web.

Otro servicio importante que ofrece la empresa es el servicio de botón de pánico, el cual debe poseer una disponibilidad muy alta para suplir las expectativas del cliente. Este servicio se encuentra en un servidor virtual dentro de un servidor físico HP el cual es administrado remotamente. Sin embargo, el

soporte no es monitoreado, únicamente se responde de manera manual a alertas por parte del cliente.

Actualmente la organización se está enfocando en mejorar la estructura tecnológica debido a que han tenido varios problemas de seguridad y estos incidentes han tenido grandes repercusiones al rendimiento del servicio que brinda la empresa, por lo cual han visto la necesidad de crear un esquema de seguridad para asegurarse de que esto no vuelva a ocurrir o mitigar estos incidentes, entre estos accidentes se encuentra la pérdida de información, la cual tuvieron que ingresar manualmente ya que no contaban con un respaldo sobre ello, indisponibilidad de servicio durante una hora, entre otros.

## 1.2 DESCRIPCIÓN DEL PROBLEMA

Dentro de la empresa se detectó que no existe un esquema de seguridad implementada, de hecho, ha habido algunos incidentes en la disponibilidad de los servicios, tales como pérdida de conexión, pérdida de información y aplicaciones web inaccesibles, lo que implica que los usuarios internos y externos se cuestionen sobre la calidad del servicio que brindan.

La red local está configurada con DHCP en un enrutador doméstico TP-Link TL-WR941ND, esto supone un riesgo alto ya que depender de las características de un enrutador doméstico la cual no está diseñado para

soportar una cantidad masiva de paquetes podría ocasionar que el servicio de internet se caiga, dando como solución el reinicio del enrutador. Además, los equipos servidores están bajo la misma red local y el enrutador no tiene configurado ninguna lista de acceso para filtrar peticiones de conexión hacia el servidor, esto es un riesgo alto ya que cualquier persona no autorizada puede tratar de acceder al servidor mediante protocolos SSH o Telnet.

Además, la empresa no cuenta con personal capacitado en el área de sistemas por lo cual se accede remotamente ante alguna alerta de los usuarios o clientes. En ocasiones el contador o alguien presencial no experto del tema colabora con soporte básico. De manera presencial, cuando el problema es más complejo, se contacta a un tercero para realizar respaldos, reconfigurar o restaurar los servidores afectados.

En lo que respecta a infraestructura, los servidores físicos comparten la misma red que los virtuales y a su vez con los empleados de la empresa. La empresa justifica esto, por el acceso que debe tener el departamento contable al sistema contable SACI (desarrollado por terceros) alojado en un servidor virtual, dentro del servidor físico DELL T20. De la misma manera el departamento de Inteligencia de Negocio accede al programa Splunk instalado en el servidor físico DELL T320. En el pasado la empresa sufrió una pérdida de información en el sistema contable, el encargado tuvo que levantar nuevamente la información en la base para mantener al día los registros perdidos, pues su último respaldo fue 1 año antes del incidente.

En conjunto, los problemas citados provocan estragos en la imagen y reputación de la empresa, tanto internamente como externamente. La fiabilidad de contar con un servidor para botón de pánico se iría perdiendo hasta ir en contra del contrato de servicios. Finalmente, la desventaja de competitividad con otras compañías del mercado, al no poder calificar para certificados de sistemas de gestión de calidad generará que los clientes actuales o futuros clientes potenciales elijan otra compañía ofreciendo el mismo servicio, pero certificados con la norma ISO 27001:2013.

## 1.3 SOLUCIÓN PROPUESTA

Se plantea la implementación de la norma ISO 27001:2013 para la optimización de procesos y servicios suministrados por la empresa, por la cual se llevará a cabo la creación de varias políticas de seguridad que abarque situaciones delicadas como la pérdida de información importante, esto se puede manejar con una política de respaldo de base de datos que están en la empresa para poder restablecer inmediatamente la información deseada si se llegara a perder por algún motivo o por algún error del personal autorizado al manejo de la base de datos como también una política para el manejo de acceso de personal no permitido, esto ayudará a decidir qué empleados están en capacidad para

acceder a cierta parte de información o del sistema que manejan ellos, con esta política se generarán niveles de acceso bien definidos.

También se plantea una política de respaldo de los servidores, ya que poseen archivos de configuración específicos para cada servicio que brindan y eso es algo de suma importancia por lo que si se llegara a perder sería muy complicado restaurar el sistema si no se tiene un respaldo de ello. Para los servidores físicos, los cuales poseen servidores virtuales, serán aplicadas normas para optimizar sus recursos y accesos a favor de proteger la disponibilidad de los servicios alojados.

De la misma manera se incluirá en la solución, el análisis y reconfiguración de la red interna de la empresa. Se revisará las configuraciones actuales del re direccionamiento de puertos, DMZ, DHCP, entre otras, para respaldar su existencia o en caso contrario removerlas u optimizarlas. Teniendo también como finalidad, establecer y justificar la presencia y correspondencia de usuarios y servidores dentro del mismo segmento de red. En caso de llegar a sugerencias o conclusiones que incluyan modificaciones físicas en la topología actual de la red, se las notificará a la empresa de manera que contemplen capital para nuevos equipos de red.

Adicionalmente se implementará una política de seguridad para el manejo de acceso de personal no permitido, esto ayudará a decidir qué empleados están en capacidad para acceder a cierta parte de información o del sistema que

manejan ellos, con esta política se generarán niveles de acceso bien definidos. Se plantea la implementación de la norma ISO 27001:2013 para la optimización de procesos y servicios suministrados por la empresa.

Los controles de creación y revisión de políticas para seguridad de la información, serán a su vez directrices para la implementación de controles adicionales aplicables a esta solución. Mediante la implementación de una política de control de accesos y control de acceso a las redes y servicios asociados, la confidencialidad de acceso a la información por parte de clientes internos o externos, será mayormente garantizada.

Para salvaguardar la disponibilidad e integridad de la información y protegerla de amenazas ambientales, se considera el control de mantenimiento de los equipos. En cuanto para amenazas a nivel digital, controles contra código malicioso, copias de seguridad de la información y restricciones de instalación de software, también son considerados en este proyecto.

Con la finalidad de mitigar conflictos en la red entre servidores y usuarios, el control de segregación de redes será puesto en funcionamiento, para reforzar la disponibilidad de los servicios.

Con los controles de mantenimiento de los equipos, de protección contra código malicioso, copias de seguridad de la información, restricciones de instalación de software y el control de acceso a las redes y servicios asociados

implementadas en las políticas de seguridad, los beneficios de esta solución son: se garantiza que incremente la disponibilidad de los servicios que ofrece la empresa, proveyendo una manera más eficiente de restaurar el servicio cuando se realice algún tipo de actualización, por lo cual el usuario final no se verá afectado de manera negativa durante el tiempo que demande este tipo de soportes. Se mitigará los posibles ataques informáticos o pérdidas de información por negligencia, generando una mejor confianza entre los usuarios que interactúan con los datos. Por último, la imagen de la compañía mejorará al poder calificar para certificados de calidad concerniente a sistemas informáticos, una vez se apliquen los controles planificados.

## 1.4 OBJETIVO GENERAL

Implementar un esquema de seguridad en base a las normas de calidad ISO 27001:2013 para una empresa de mensajería masiva por SMS, mediante la implementación de políticas de seguridad y el cumplimiento de controles que la empresa debe aplicar para garantizar la calidad del servicio brindado.

## 1.5 OBJETIVOS ESPECÍFICOS

Los objetivos específicos son los siguientes:

1. Identificar las vulnerabilidades o debilidades que presenta la empresa en la infraestructura tecnológica.
2. Diseñar políticas de seguridad que abarcan defensa contra accesos no autorizados, respaldo periódico de información crítica y acciones rápidas ante una caída de servicio.
3. Implementar y ejecutar las políticas de seguridad.
4. Verificar y evaluar el cumplimiento de las políticas de seguridad implementadas contra las vulnerabilidades detectadas.

## 1.6 METODOLOGÍA

Para la implementación del esquema de seguridad nos basamos en la metodología MAGERIT v3:

- Definición de los procesos.
- Asociación de los activos de información al proceso crítico.
- Análisis de brecha.
- Análisis de riesgo.
    - Definición del alcance.
    - Identificación de los activos.
    - Identificar amenazas sobre los activos.
    - Clasificación de los inventarios por la valoración de las amenazas.

- Declaración de aplicabilidad
- Tratamiento de riesgos.
- Plan de tratamiento de riesgos.

Se definen los procesos que tiene la empresa y nuestro enfoque radica en el proceso central o el más importante para la organización y a esta se la aplicará los controles necesarios para eliminar o mitigar las vulnerabilidades que pueden ser explotadas para perjudicar a la organización.

El alcance de la evaluación de riesgos y de las políticas de seguridad se centrará en los controles que son aplicables para el proceso central, la cual incluye áreas de software, hardware y redes.

# CAPÍTULO 2

# MARCO TEÓRICO

## 2.1 INTRODUCCIÓN

La ISO 27001:2013 es basado principalmente en el Sistema de Gestión de Seguridad de la Información (SGSI), la gestión de seguridad debe hacerse mediante un proceso organizado, correctamente elaborado, documentado y debe ser conocido por todos los miembros dentro de la organización.

La SGSI está compuesta por cuatro procesos básicos que son indispensables para su correcta implementación y actualización, a esto se le conoce como el ciclo de vida de una SGSI. Estos procesos están circularmente enlazados por lo que es una mejora continua. En la Figura 1 se muestra estos procesos.

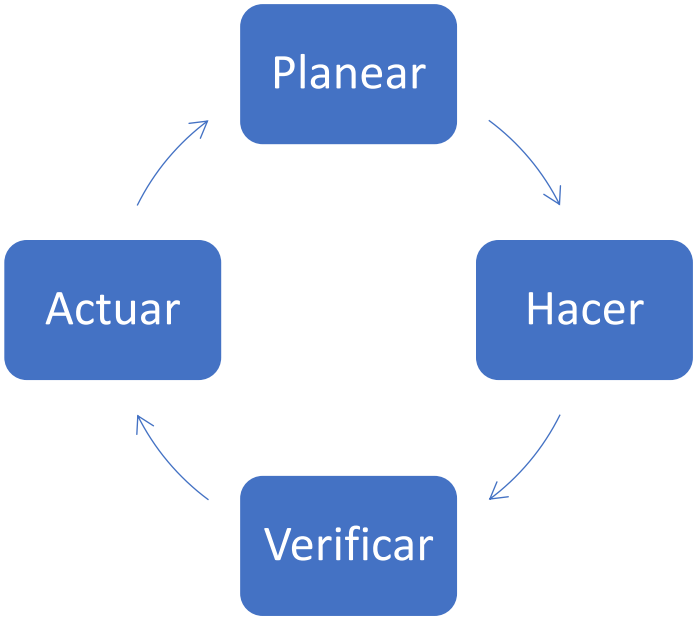



**Figura 2.1: Procesos básicos de un SGSI**

**Fuente:** http://maurikviking.wixsite.com/ingsoftudistrital/norma-iso-27001, consultado Octubre 2018

Cada proceso del SGSI cumple una función específica tal como se muestra en la Tabla 1.

**Tabla 1: Objetivos de los procesos básicos de la SGSI**

| Proceso | Descripción |
|---|---|
| Planear (Establecer el SGSI) | Se establecen los objetivos, el alcance del SGSI, las políticas, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática. |
| Hacer (Implementar y operar el SGSI) | Se realiza la implementación de los controles establecidos en el procedimiento previo |
| Verificar (Revisar y dar seguimiento al SGSI) | Revisar el desempeño de los procesos con respecto a la política y que estos cumplan con los objetivos establecidos en el primer proceso, luego de esto reportar los resultados a la alta dirección para su debida revisión. |

| | |
|---|---|
| Actuar (Mantener y mejorar el SGSI) | Realizar acciones correctivas y preventivas basadas en los resultados de la revisión. |

**Fuente:** https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/, consultado Octubre 2018

EL SGSI está enfocada en tres términos que son importantes en lo que respecta al sistema de información, los cuales son: la confidencialidad, la integridad y la disponibilidad [1] y esto es lo que principalmente se centra la ISO 27001:2013.

La información sensible dentro de la empresa solo debe ser accedida por cierto personal que está apto o autorizado para acceder y leer dicha información, si esta información está siendo accedida por personal no autorizado se está comprometiendo la confidencialidad.

Cuando se trata de que la información no debe ser modificada, alterada o eliminada y debe estar de manera completa estamos diciendo que dicha información tiene integridad.

La información debe estar disponible en cualquier momento, siempre y cuando quien la solicite tenga los accesos necesarios para poder obtener dicha información, esto tiene que ver con la disponibilidad de la información.

## 2.2 SEGURIDAD DE LA INFORMACIÓN

Es un conjunto de medidas de seguridad, que pueden ser controles y políticas de seguridad, cuyo objetivo es la de minimizar o erradicar la amenaza latente sobre algún sistema de información. Los equipos de hardware y de software que forman parte vital para el funcionamiento de la organización también son protegidos por la seguridad de la información [2].

Cuando se trata de la norma ISO27001:2013, la seguridad de la información está enfocada en la confidencialidad, integridad y la disponibilidad de la información y los datos relevantes dentro de la organización, pero para esto se requiere mantener los programas, controles y las políticas de seguridad correctamente implementadas.

No contar con alguna medida de seguridad en contra a una amenaza puede provocar la pérdida de una gran suma de dinero y quizás a la quiebra de la organización y esto causado por algún fallo a nivel de software o algún desperfecto a nivel de hardware, por ese motivo la seguridad de la información es un punto vital que toda organización debe considerar.

## 2.3 ISO 27001:2013

Norma internacional emitida por la Organización Internacional de Normalización (ISO) y cuyo principal objetivo es de proveer los requerimientos para establecer, implementa y mejorar continuamente la gestión de la seguridad de información, y esto es mediante la implementación de políticas de seguridad y controles.

La norma ISO 27001:2013 posee la siguiente estructura [3]:

1. Objeto y campo de aplicación: Orienta sobre el uso y la aplicación del estándar.
2. Referencias Normativas: Contiene todos los términos y definiciones sobre la norma ISO 27001:2013.
3. Términos y Definiciones: Describe la terminología del estándar.
4. Contexto de la Organización: Recoge información la organización y su contexto.
5. Liderazgo: Indica que todos los empleados dentro de la organización deben participar al establecimiento de la norma.
6. Planificación: Se debe determinar los riesgos al momento de realizar una planificación para un sistema de gestión de seguridad.
7. Soporte: Es necesario que la organización cuente con los recursos, competencias, conciencia, comunicación e información documentada en cada caso.

8. Operación: Se debe realizar una evaluación de os riesgos encontrados en los procesos analizados y luego realizar el plan de tratamiento de ellos.
9. Evaluación del Desempeño: Describe la manera de hacer la auditoria interna y la revisión por la dirección.
10. Mejora: Son las obligaciones que tendrá la organización cuando encuentre una no conformidad para la mejora continua y la eficacia del SGSI.

## 2.4 RIESGO INFORMÁTICO

Un riesgo informático es la probabilidad de que existe alguna amenaza hacia los equipos informáticos, estas amenazas no se refieren solamente a la parte de software como los virus informáticos que un servidor o una máquina de algún usuario pueda llegar a tener, sino también se refiere a la parte de hardware que no están exentos de tales riesgos como algún desastre natural, algún desperfecto a las partes del activo o simplemente al mal uso que se le da al activo.

Para conocer cuáles son los riesgos dentro de una organización, se realiza un análisis de riesgos por lo que se les da cierta valoración a los activos basados en la importancia que tiene el activo para la organización y la probabilidad que ese activo puede ser afectado por dichos riesgos. Para hacer este análisis de

riesgo se debe conocer cuáles son los tipos de riesgos, entre estos tenemos [4]:

- Riesgos de integridad.
- Riesgos de acceso.
- Riesgos en la infraestructura.
- Riesgos de seguridad general.

Tomando en cuenta estos riesgos ya se puede determinar, analizar, valorar y clasificar el riesgo existente dentro de la organización y esto es lo que se conoce como gestión de riesgo.

## 2.5 EVALUACIÓN DE RIESGOS

Es un conjunto de pasos para determinar los riesgos que pueden existir en todos los procesos dentro de una organización y cuyo objetivo es de minimizar estos riesgos encontrados.

La Gerencia General o los Altos Directivos son los responsables de que una evaluación de riesgo se lleve a cabo y se debe consultar a los participantes sobre el método a emplear, ya que existen varias metodologías, entre los más conocidos son Magerit y Octave [5].

## 2.6 RIESGO INHERENTE

Es el riesgo propio de cada actividad, sin considerar los controles que se puedan aplicar, este riesgo surge de la exposición que se tenga a una actividad en particular y de la probabilidad que resulte en un efecto negativo para la salud del individuo y la rentabilidad de la empresa [6].

Este riesgo no puede ser eliminado completamente ya que es propio del trabajo, es posible que se mitigue el daño provocado, tomando ciertas medidas de seguridad para un posible suceso, como ejemplo tenemos daño de los ojos por estar mucho tiempo expuesto frente a un computador o laptop, para algún desarrollador de software la exposición frente al computador será excesiva y no es posible evitar esto, para evitar daño de sus ojos se puede usar un protector de pantalla o lentes anti-reflectivos.

## 2.7 RIESGO RESIDUAL

El riesgo residual es aquel que aún persiste después de haber implementado los controles y puede ser calculado con la diferencia entre riesgos inherentes menos la efectividad de controles o multiplicando la probabilidad residual por el impacto residual [6].

## 2.8 MAGERIT

Metodología usada para realizar una evaluación de riesgos sobre un proceso acordado con alta, fue elaborada por el Consejo Superior de Administración Electrónica de España. Esta metodología consta de cinco pasos, las cuales son [7]:

1. Identificación de los activos en el proceso.

2. Identificación de las amenazas sobre los activos.

3. Salvaguardas.

4. Impacto residual.

5. Riesgo residual.

## 2.9 POLÍTICAS DE SEGURIDAD

Según Antonio Villalón, “una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema” [8]. Para implementar una política de seguridad requiere de un alto compromiso para con la empresa, se necesitan de reuniones continuas para discutir sobre los riesgos presentados y los posibles controles a

ser implementados, identificar las fallas y debilidades, constancia para renovar y actualizar la política de seguridad de acuerdo a las necesidades que van surgiendo en la organización.

Según la norma ISO 27001:2013, una política de seguridad debe transmitir claramente los objetivos que la alta dirección pretende alcanzar con la implementación del sistema, debe ser un documento que resulta fácil de entender para las partes interesadas. [8] La política de seguridad debe incluir:

- Adaptabilidad: La organización no debe adaptarse a un documento. La política debe adaptarse a los requerimientos de la organización.

- Definición de los objetivos: El documento precisa definir los objetivos de seguridad de la información, su forma de aprobación y la manera en que han de ser revisados.

- Compromiso: La alta dirección de la organización debe expresar su compromiso total con el sistema y con su propósito final.

- Comunicación: El documento debe establecer quién o quiénes son los encargados de comunicar a las partes interesadas.

- Revisiones: La política de seguridad debe ser revisada de forma periódica, y estas revisiones, así como los responsables de las mismas, y los periodos de tiempo en los que se efectuaran, son temas que se deben incluir en el documento.

## 2.10 CONTROLES

Es lo que permite garantizar que cada aspecto por la cual se valoró con cierto riesgo, quede cubierto y auditable. Un control, cuando hablamos sobre el ISO 27001:2013 abarca un conjunto de acciones, documentos y procedimientos para proporcionar la seguridad de la información [9].

En ISO 27001:2013 existen 114 controles, las cuales están clasificados en los anexos de esta norma. Para la implementación de un esquema de seguridad no es obligatorio aplicar todos, sino depende de si la organización la necesite o no.

# CAPÍTULO 3

# LEVANTAMIENTO DE LA INFORMACIÓN

## 3.1 ORGANIZACIÓN

La organización de la empresa está encabezada por la Gerencia General, seguido de la Coordinación de Proyectos. Esta última área supervisa tres departamentos, como son: Departamento de Sistemas, Departamento de Marketing Digital y Departamento Financiero. La comunicación directa con Gerencia, sin embargo, también puede ocurrir directamente por parte de cada líder de los departamentos. Como soporte de terceros, se encuentra el servicio de HiVelocity para hosting en la nube y un experto en servidores que se contacta de manera esporádica.

En la Figura 2 se presenta el organigrama de la organización.

El Departamento de Sistemas se encarga del mantenimiento de los sistemas informáticos, desarrollo e implementación de nuevos proyectos de software y por último del mantenimiento de servidores. Entre los mantenimientos y actualizaciones de software, se encuentra el servicio de mensajería masiva que es el proceso principal de la empresa.

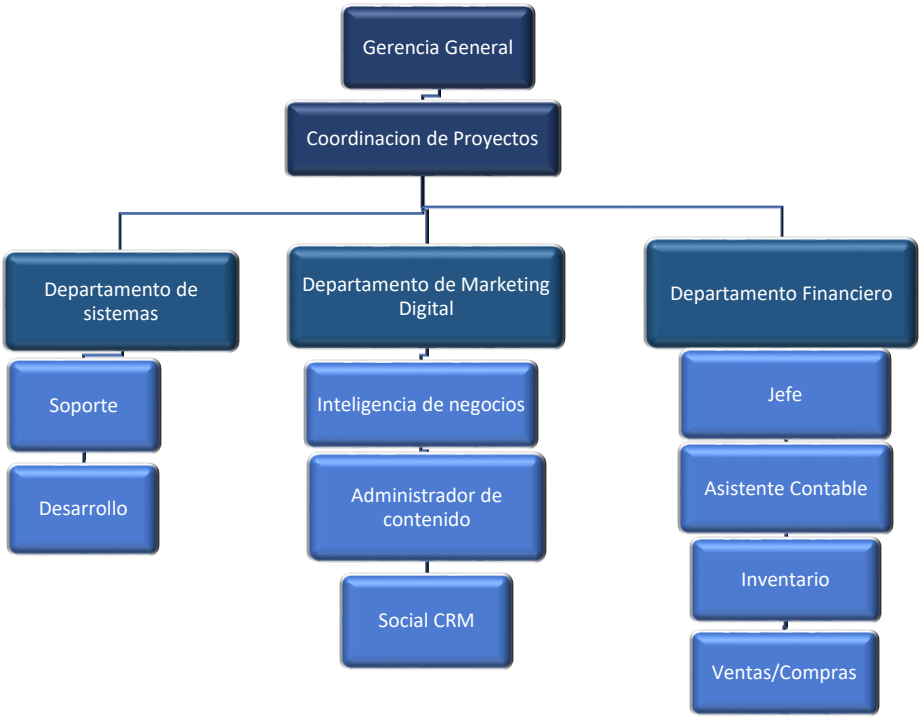



**Figura 3.1: Organigrama empresa de mensajería masiva**

**Fuente:** Los autores

Actualmente el Departamento de Sistemas cuenta con dos roles: el desarrollador, que es el encargado de implementar nuevos proyectos de software y actualizar los ya existentes según sea necesario y el segundo rol

que es el jefe de sistemas encargado de brindar soporte al cliente, de brindar mantenimiento a los servidores y de realizar cronogramas de entrega de los proyectos en desarrollo y de realizar los respectivos informes.

El Departamento de Marketing Digital se encarga de promover la marca de la organización, de lanzar marcas publicitarias para nuestros clientes y para la organización, en este departamento se encuentran definidos tres roles, las cuales son: Analista de inteligencia, Administrador de contenido y el social CRM.

Existe una página web la cual es administrada por el administrador de contenido y el social CRM que también es diseñador gráfico, esa página web está alojada en un servidor local dentro de la organización.

El Departamento Financiero está encargado de la contabilidad, conciliaciones bancarias, ventas, compras y todo lo que esté relacionado con asuntos legales, en este departamento existen cuatro roles definidos, las cuales son: venta/compra, asistente contable, inventario y el contador.

En este departamento cuenta con un sistema contable la cual está alojado en la nube, este es un servicio brindado por terceros. El sistema contable posee bancos, cuentas por pagar y cobrar, manejo de inventarios y por supuesto la contabilización de lo mismo.

La empresa posee oficinas en Guayaquil y Quito. En Quito se encuentra la mayor parte del personal, sin embargo, se suele viajar entre ambas ciudades para realizar reuniones con clientes potenciales o soporte para clientes actuales. En Guayaquil se encuentra todo el personal del departamento de sistemas, mismo que entre sus actividades se encarga de la administración de los servidores de forma presencial o remota.

## 3.2 INFRAESTRUCTURA DE LA EMPRESA

### 3.2.1 REDES

Actualmente la empresa cuenta con un servidor en la oficina de Guayaquil, tres servidores en la oficina de Quito y un servidor HiV en la nube. Tanto el servidor de Guayaquil como el servidor HiV tienen instalada la plataforma Kannel, la cual opera como puerta de enlace, con las operadoras de celular.

Cada servidor de Quito tiene una tarea distinta, el primero maneja exclusivamente la virtualización de un servidor para el servicio de botón de pánico, esto es manejado para clientes externos.

El segundo servidor virtualiza un servidor con el sistema contable de la empresa SACI, sistema contable de terceros y la cual también tienen un soporte activo.

El tercero tiene alojado Splunk, como aplicación web de inteligencia de negocio, esta aplicación web es usada por el departamento de Marketing Digital.

Para los clientes externos, la prioridad yace en el servidor de botón de pánico en Quito, el servidor de Guayaquil y el servidor de la nube. Los registros de los envíos masivos son alojados en bases de datos MySQL presentes en cada servidor. Los clientes de la empresa, según la magnitud de carga y envío de mensajes de texto, son repartidos entre los servidores. Todos los servidores brindan el servicio de aplicativo web para envío o reportes, así como conexiones para recibir peticiones de envío vía REST o SOAP.

La empresa, también tiene contratado un servicio de internet, de este servicio brindado no se ha tenido ningún tipo de quejas.

Actualmente la empresa no cuenta con ningún tipo de cortador de fuegos para bloquear conexiones o accesos indeseados, las computadoras del personal de la empresa cuentan con antivirus instalado, pero no hay ninguna garantía de que estén actualizadas ya que no existe una política o protocolo que lleve a cabo la actualización de antivirus. Todos los servicios a los que se ingresa cuentan con usuario y contraseña para

corroborar que sea un usuario autorizado el que este indagando en el sistema.

La distribución lógica de la red consta de una sola dirección de red:

| Red | Mascara | Puerta de salida |
|---|---|---|
| 192.168.1.0 | 255.255.248.0 | 192.168.1.1 |

En la siguiente figura se muestra la infraestructura de la empresa.

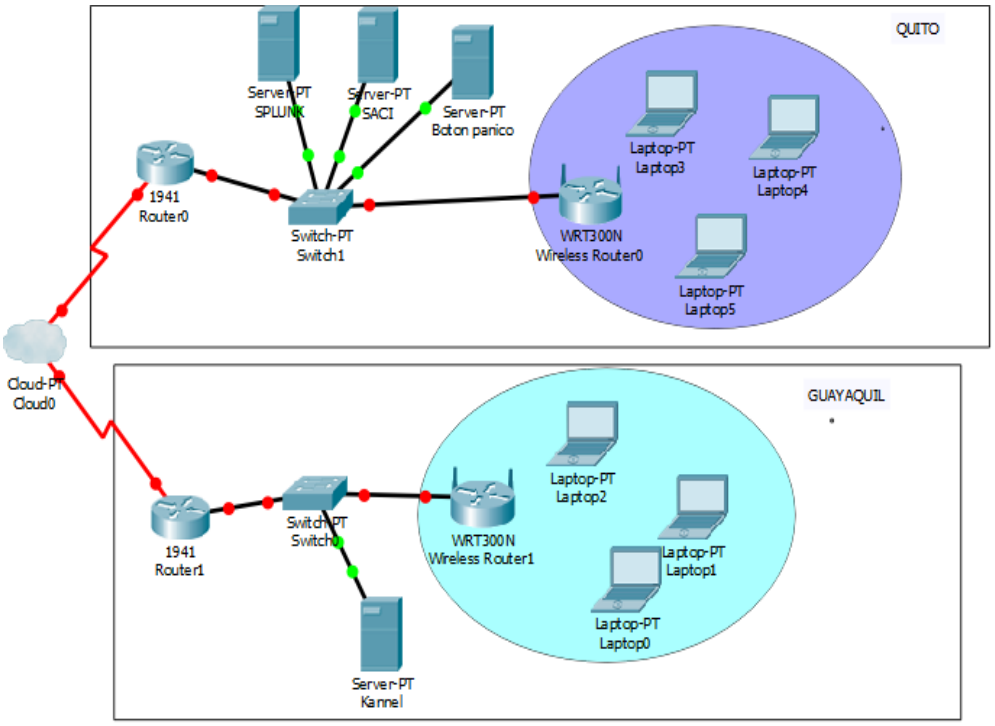



**Figura 3.2: Infraestructura de red de empresa de mensajería masiva**

**Fuente:** Los autores

### 3.2.2 SISTEMAS INFORMÁTICOS

Los servidores que cuenta la empresa tienen instalado Windows Server 2000 como sistema operativo, a estos servidores se les da un mantenimiento semanal. Este mantenimiento incluye: actualizaciones de antivirus, parches lanzados por Microsoft, liberación de memoria, desfragmentación del disco duro.

Aunque a los servidores se les da un mantenimiento regular, no se cuenta con un esquema o una política definido para realizar un mantenimiento adecuado a los servidores.

En las computadoras y laptops que usan los empleados existen diferentes tipos de sistemas operativos: dos computadoras cuentan con sistema Linux Ubuntu 14.04, 5 laptops tienen instalado Windows 8 y los 10 restantes tienen instalado Windows 10.

Los computadores que usan los empleados no se les da mantenimiento regular, por lo que son proclives a llenarse de virus y presentar comportamientos irregulares ocasionalmente.

### 3.2.3 ACTIVOS DE LA EMPRESA

La empresa posee los siguientes activos en su poder, las cuales no están debidamente registradas:

- 4 servidores locales:
  - 1 servidor donde se aloja el servicio de botón de pánico.
  - 1 servidor donde se aloja el sistema contable SACI.
  - 1 servidor donde se aloja Splunk.
  - 1 servidor que tiene instalado la plataforma Kannel.
- 1 servidor en la nube donde también se encuentra instalado la plataforma Kannel.
- 2 conmutadores de marca CISCO.
- 10 laptops.
- 5 computadores personales.
- Licencia de Sistema operativo Windows 2000.
- 5 licencias de Windows 8,
- 10 licencias de Windows 10.
- 1 router marca CISCO.
- Inmuebles:
  - 2 mesas.
  - 2 archivadores.
  - 2 sillones.
  - 10 teléfonos.

- 4 tachos de basura.
- 12 sillas.
- 5 muebles para computadores.
- 2 televisores de 40” marca LG.

## 3.3 PROCESOS DE LA EMPRESA

Los procesos principales de la empresa, como se señala en la Figura 4, se categorizan según la gestión correspondiente. Teniendo como involucrados o parte de interés a más de un miembro de distintos departamentos, los cuales pueden participar como responsable, aprobador, consultado o informado.

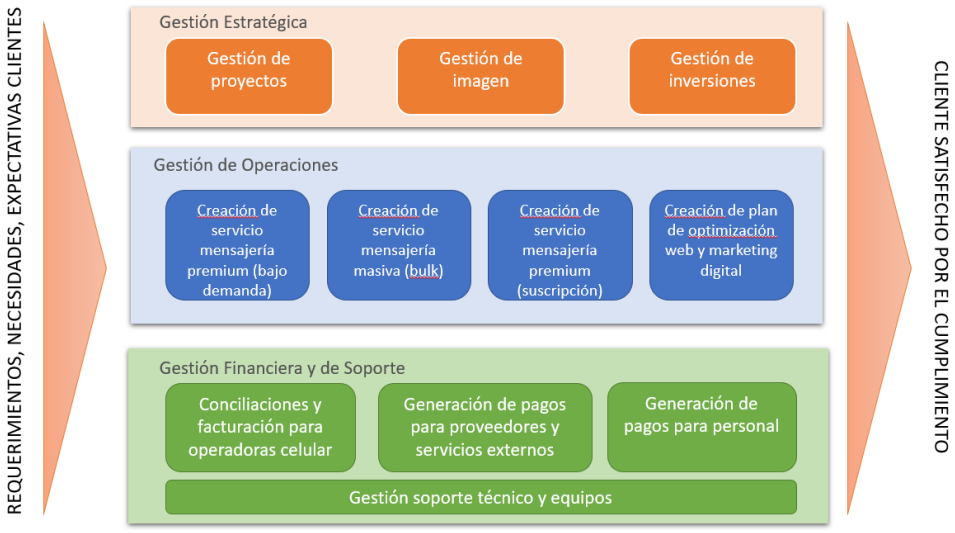



**Figura 3.3: Mapa de Procesos**

**Fuente:** Los autores

En la siguiente Tabla 2 se expone una matriz de asignación de responsabilidades tipo RACI, donde se muestra la participación de los miembros de los departamentos de la empresa con los procesos principales.

Para el objetivo de este esquema de seguridad, nos enfocaremos en analizar el proceso relacionado al envío de mensajería masiva, la cual se encuentra en la Gestión de Operaciones. Además de considerar controles para activos tecnológicos de los demás procesos operativos y financieros.

**Tabla 2: Matriz RACI de procesos principales**

| RACI | Gerente General | Asistente Gerencial | Coordinador de Proyectos | Jefe de Sistemas | Jefe Desarrollo | Jefe de Financiero | Asistente Financiero | Jefe de Digital | Asistente Digital |
|---|---|---|---|---|---|---|---|---|---|
| Gestión de proyectos | A | I | R | C | C | C | | C | C |
| Gestión de imagen | A | I | I | I | | I | | R | R |
| Gestión de inversiones | A | I | | C | | R | R | C | |
| Creación de servicio mensajería premium (bajo demanda) | A | I | C | R | R | | | | |
| Creación de servicio mensajería masiva (bulk) | A | I | C | R | R | | | | |
| Creación de servicio mensajería premium (suscripción) | A | I | C | R | R | | | | |
| Creación de plan de optimización web y marketing digital | A | I | C | C | C | | | R | R |
| Generación de conciliaciones para socios y proveedores | A | I | | C | | R | C | | |
| Conciliaciones y facturación para operadoras celular | A | I | | | | R | R | | |
| Generación de pagos para personal | A | I | | | | R | C | | |
| Gestión soporte técnico y equipos | A | R | | C | C | C | I | | |

**Fuente:** Los autores

## 3.4 INVENTARIO DE ACTIVOS

La empresa cuenta con activos que se usan en cada proceso indicado anteriormente, en la Tabla 3 se muestra los inventarios con la que cuenta cada proceso.

**Tabla 3: Activos por proceso**

| Proceso | Activo | Tipo de Activo |
|---|---|---|
| **Gestión de proyectos** | Personal de cuentas y proyectos | Persona |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras / Laptops | Hardware |
| | Sistemas operativos | Software |
| | Aplicación web para coordinación de proyectos | Servicio |
| **Gestión de imagen** | Personal de marketing digital | Persona |
| | Aplicación web para marketing digital | Software |
| | Computadoras / Laptops | Hardware |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Sistemas operativos | Software |
| | Router | Hardware |
| | Servidor Local | Hardware |
| **Gestión de inversiones** | Líderes de Departamentos | Persona |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Aplicación de contabilidad | Software |
| | Computadoras / Laptops | Hardware |
| | Sistemas operativos | Software |
| | Servidor Local | Hardware |
| **Creación de servicio mensajería premium (bajo demanda)** | Servidor Local | Hardware |
| | Routers | Hardware |
| | Personal de sistemas y digital | Persona |
| | Aplicación web marketing digital | Software |
| | Motor base de datos | Software |

| Proceso | Activo | Tipo de Activo |
|---|---|---|
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |
| | Aplicación web de reportes internos y externos | Software |
| | Aplicación web para coordinación de proyectos | Servicio |
| | Servidor en la nube | Servicio |
| | Sistema mensajería premium | Software |
| | Impresoras térmicas | Hardware |
| **Creación de servicio mensajería masiva (bulk)** | Servidor Local | Hardware |
| | Sistema mensajería masiva | Software |
| | Routers | Hardware |
| | Personal de sistemas y digital | Persona |
| | Aplicación web marketing digital | Software |
| | Motor base de datos | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |
| | Aplicación web de reportes internos | Software |
| | Aplicación web para coordinación de proyectos | Servicio |
| | Servidor en la nube | Servicio |
| **Creación de servicio mensajería premium (suscripción)** | Servidor Local | Hardware |
| | Routers | Hardware |
| | Personal de sistemas y digital | Persona |
| | Aplicación web marketing digital | Software |
| | Motor base de datos | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |

| Proceso | Activo | Tipo de Activo |
|---|---|---|
| | Aplicación web de reportes internos | Software |
| | Aplicación web para coordinación de proyectos | Servicio |
| | Servidor en la nube | Servicio |
| | Sistema mensajería premium | Software |
| | Impresoras térmicas | Hardware |
| **Creación de plan de optimización web y marketing digital** | Personal de marketing digital | Persona |
| | Servidor Local | Software |
| | Routers | Hardware |
| | Aplicación web marketing digital | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |
| | Aplicación web para coordinación de proyectos | Servicio |
| **Generación de conciliaciones para socios y proveedores** | Aplicación web de reportes internos y externos | Software |
| | Personal de financiero | Persona |
| | Servidor Local | Software |
| | Routers | Hardware |
| | Aplicación para contabilidad | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |
| **Conciliaciones y facturación para operadoras celular** | Aplicación web de reportes internos | Software |
| | Personal de financiero | Persona |
| | Servidor Local | Software |
| | Routers | Hardware |
| | Aplicación para contabilidad | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |

| Proceso | Activo | Tipo de Activo |
|---|---|---|
| | Sistema Operativo | Software |
| **Generación de pagos para personal** | Personal de financiero | Persona |
| | Servidor Local | Software |
| | Routers | Hardware |
| | Aplicación para contabilidad | Software |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Computadoras/Laptops | Hardware |
| | Sistema Operativo | Software |
| **Gestión soporte técnico y equipos** | Personal sistemas | Persona |
| | Documentos físicos y digitales | Datos/Soporte de información |
| | Asistencia técnica proveedores | Servicio |

**Fuente:** Los autores

Cada activo inventariado tiene un responsable que por lo general es el jefe del departamento, en la Tabla 4 se muestra los responsables de cada activo por departamento.

**Tabla 4: Responsables de los activos por proceso**

| Responsable | Activo |
|---|---|
| Gerente General | Líderes de Departamentos |
| Jefe de Coordinación de Proyectos | Personal de cuentas |
| | Aplicación web para coordinación de proyectos |
| Personal a cargo | Documentos físicos y digitales |
| | Computadoras / Laptops |
| Jefe de Dpto. Digital | Personal de marketing digital |
| | Aplicación web para marketing digital |
| Jefe de Dpto. de Sistemas | Sistemas operativos |
| | Router |
| | Servidor Local |

| Responsable | Activo |
|---|---|
| | Aplicación de contabilidad |
| | Personal de sistemas |
| | Motor base de datos |
| | Servidor en la nube |
| | Sistema mensajería premium |
| | Impresoras térmicas |
| | Sistema mensajería masiva |
| | Aplicación web de reportes internos |
| | Sistema mensajería premium |
| | Aplicación web de reportes internos y externos |
| Jefe de Dpto. Financiero | Personal de financiero |
| | Aplicación para contabilidad |
| | Asistencia técnica proveedores |

**Fuente:** Los autores

## 3.5 POLITICAS IMPLEMENTADAS

Actualmente la empresa no cuenta con políticas de seguridad informática implementadas, sin embargo, existen responsabilidades asignadas a cada departamento y sus miembros en relación a los sistemas de información.

Los miembros del departamento de sistemas son los responsables de cumplir las cláusulas de soporte con los clientes externos. Son quienes administran remotamente a todos los servidores, y de manera presencial, únicamente al servidor de Guayaquil. Ellos se comunican con el coordinador de proyectos e incluso con el Gerente General, para aprobar los cambios en los distintos desarrollos de productos y servicios.

Los ejecutivos de cuenta se encargan de mantener la buena relación con los clientes asignados a ellos. Tienen como responsabilidad, notificar observaciones o inconvenientes con la interacción del cliente y el servicio contratado. De esta forma los departamentos digital y sistemas se ajustan a los requerimientos señalados, los cuales son informados a Gerencia para mantenerse informados.

El jefe del departamento financiero, se comunica directamente al Gerente General y requiere de la información brindada por los sistemas internos de reportes. De esta manera, se logran cumplir con los objetivos de los procesos correspondientes a esta área. Si el sistema contable llegase a tener algún fallo, se comunica con el jefe de TI para soporte básico remoto con la opción de escalar a un tercero, como es el proveedor del sistema contable.

# CAPÍTULO 4

# ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD

## 4.1 IDENTIFICACIÓN DEL PROCESO A ANALIZAR

Para la identificación del proceso central o el proceso a la cual es de alta importancia la implementación del esquema de seguridad se realizó una pequeña reunión con los miembros de la Gerencia General, la cual nos informaron que el proceso central de la empresa, es el de envío de mensajería masiva ya que ese es el negocio de ellos y debido a que no tienen implementadas adecuadamente políticas de seguridad, han presentado varios problemas con el servicio brindado al cliente.

El análisis y diseño del esquema de seguridad será enfocado al proceso de envío de mensajería masiva, si este proceso presenta problemas estarían

dando una mala imagen como empresa e incumpliendo con su objetivo y se verían afectado gravemente a nivel económico.

## 4.2 ANÁLISIS DE BRECHA

Es necesario conocer el estado y el desempeño actual de la empresa frente a la seguridad para luego comparar el estado de la organización una vez que el esquema de seguridad sea implementado.

Se obtuvo la información requerida para realizar correctamente el análisis de brecha. La matriz de análisis de brecha, junto con todos los controles, se lo puede encontrar en el Anexo B.

La Tabla 6 muestra el nivel de cumplimiento de la organización con respecto a los controles definidos en la norma ISO 27001:2013, resultado dado por la matriz de análisis de brecha.

El porcentaje de cumplimiento se lo calculo con el nivel de cumplimiento en cada control de cada dominio de la norma y sacando un promedio entre los porcentajes dados en cada dominio.

La Tabla 5 especifica la ponderación que se le puede dar a cada control.

**Tabla 5: Rubrica de nivel de cumplimiento**

| Porcentaje | Definición |
|---|---|
| 0% | No existe implementado el control. |
| 1% - 20% | No existen procesos estandarizados, es decir una política en la cual basarse sino que cada caso independiente se aplica un procedimiento particular, es decir la implementación de un control depende de cada individuo. |
| 21% - 40% | Existen procedimientos dependientes de las personas y otras la siguen. No existe comunicación formal sobre los procedimientos que se deben seguir. |
| 41% - 75% | Los procedimientos se definen y se comunican mediante un entrenamiento formal. No existen mediciones ni monitoreo sobre el cumplimiento de los procedimientos |
| 76% - 99% | Los controles implementados se comunican mediante un entrenamiento formal. Existen mediciones y monitoreo sobre el cumplimiento del procedimiento. No existe evidencias sobre incidentes para aplicar mejora continua |
| 100% | Cumple totalmente con la descripción del control, existen políticas implementadas y se sigue acorde a ellas. Se recoge evidencia numérica sobre los incidentes y se aplica mejoras al control |

**Fuente:** Los autores

**Tabla 6: Nivel de cumplimiento de la organización**

| No. Dominio | Dominio de la Norma | % de cumplimiento |
|---|---|---|
| 5 | Políticas de seguridad de la información | 0% |
| 6 | Organización de la seguridad de la información | 6% |
| 7 | Seguridad de los recursos humanos | 43.33% |
| 8 | Gestión de activos | 21% |
| 9 | Control de acceso | 23% |
| 10 | Criptografía | 0% |
| 11 | Seguridad física y del entorno | 68% |
| 12 | Seguridad de las operaciones | 42.8% |
| 13 | Seguridad de las comunicaciones | 42.8% |
| 14 | Adquisición, desarrollo y mantenimiento de sistema | 26.9% |
| 15 | Relaciones con los proveedores | 0% |
| 16 | Gestión de incidentes de la seguridad de la información | 31.4% |
| 17 | Aspectos de la seguridad de la información de la gestión de la continuidad de la información | 0% |
| 18 | Cumplimiento | 75% |

**Fuente:** Los autores

Debido a que la organización no cuenta con políticas de seguridad claramente definidas o los procedimientos para realizar alguna acción, respaldo, soporte o comunicación con el cliente/proveedor no está documentado, el resultado del análisis de brecha de la empresa con respecto a la seguridad de la información es muy baja, es de 27.16%.

Nuestro objetivo es que el nivel de cumplimiento de la empresa con respecto a la seguridad de la información incremente aplicando el esquema de seguridad sobre el proceso central de la organización.

## 4.3 ANÁLISIS DE RIESGO

Para el análisis de riesgo se usó la metodología Magerit, se definió el alcance la evaluación de riesgo, se identificaron los activos que intervienen en el proceso de mensajería masiva, se identificaron las amenazas y luego se realizó la clasificación de los activos de acuerdo a las amenazas.

### 4.3.1 ALCANCE DE LA EVALUACIÓN DE RIESGO

La evaluación de riesgo será sobre el proceso de creación y envío de mensajería masiva, por lo cual esto involucra a todos los activos que se encuentran en el proceso, así como a los departamentos involucrados, los cuales son: personal dentro del Departamento de Sistemas y el personal dentro del Departamento de Marketing Digital.

### 4.3.2 DEFINICION DE LOS TIPOS DE RIESGOS

En la siguiente tabla se muestran los tipos de riesgos existentes para el proceso de creación y envió de mensajería masiva.

**Tabla 7: Definición de los tipos riesgos**

| Identificación | Nombre |
|---|---|
| R1 | Riesgo tecnológico |
| R2 | Riesgo operativo |
| R3 | Riesgo de imagen |
| R4 | Riesgo de cumplimiento |

**Fuente:** Los autores

### 4.3.3 IDENTIFICACIÓN DE LOS ACTIVOS

Los activos que están asociados a este proceso se los muestra en la Tabla 8.

Dentro del proceso de mensajería masiva se encuentran trece categorías de activos y sobre estos se realiza la identificación de las amenazas.

Los activos son clasificados en función a su importancia o grado de criticidad, para llevar a cabo dicha clasificación nos basamos en la Tabla 9.

**Tabla 8: Activos dentro del proceso de mensajería masiva**

| No. | Activo | Tipo de Activo |
|---|---|---|
| 1 | Servidores | Hardware |
| 2 | Routers | Hardware |
| 3 | Personal de sistemas y digital | Persona |
| 4 | Sistema de mensajería masiva | Software |
| 5 | Aplicación web marketing digital | Software |
| 6 | Motor base de datos | Software |

| No. | Activo | Tipo de Activo |
|---|---|---|
| 7 | Documentos físicos | Datos/Soporte de información |
| 8 | Computadoras/Laptops | Hardware |
| 9 | Sistema Operativo | Software |
| 10 | Aplicación web de reportes internos y externos | Software |
| 11 | Sistema mensajería premium | Software |
| 12 | Impresoras térmicas | Hardware |
| 13 | Aplicación web para coordinación de proyectos | Software |

**Fuente:** Los autores

**Tabla 9: Valoración**

| Valor | Confidencialidad | Disponibilidad | Integridad | Importancia |
|---|---|---|---|---|
| 1 | No aplica | No aplica | No aplica | No aplica |
| 2 | Pública | Muy bajo | Muy bajo | Muy bajo |
| 3 | Uso interno | Bajo | Bajo | Bajo |
| 4 | Uso restringido | Medio | Medio | Medio |
| 5 | Confidencial | Alto | Alto | Alto |
| 6 | Secreto | Crítico | Crítico | Crítico |

**Fuente:** Los autores

En la Tabla 10 se clasifican estos activos en función de su criticidad.

**Tabla 10: Importancia de los activos**

| Activo | Confidencialidad | Disp. | Integridad | Media | Importancia |
|---|---|---|---|---|---|
| Servidores | 5 | 6 | 6 | 5 | Alto |
| Routers | 5 | 6 | 6 | 5 | Alto |
| Sistema de mensajería masiva | 2 | 6 | 6 | 4 | Medio |

| Activo | Confidencialidad | Disp. | Integridad | Media | Importancia |
|---|---|---|---|---|---|
| Aplicación web marketing digital | 2 | 5 | 1 | 2 | Muy bajo |
| Motor base de datos | 5 | 6 | 6 | 5 | Alto |
| Documentos físicos | 3 | 2 | 6 | 3 | Bajo |
| Computadoras/Laptops | 3 | 5 | 1 | 3 | Bajo |
| Sistema operativo | 6 | 6 | 1 | 4 | Medio |
| Aplicación web de reportes internos y externos | 5 | 5 | 5 | 5 | Alto |
| Sistema mensajería premium | 5 | 6 | 6 | 6 | Crítico |
| Impresoras térmicas | 3 | 4 | 1 | 3 | Bajo |
| Aplicación web para coordinación de proyectos | 5 | 4 | 3 | 4 | Medio |

**Fuente:** Los autores

### 4.3.4 IDENTIFICACIÓN DE LAS AMENAZAS

Para la identificación de las amenazas sobre el proceso de envío de mensajería masiva, se indagó sobre los problemas e incidentes que han tenido, no nos proveyeron de un documento sobre los incidentes ocurridos, ya que no cuentan con un registro de incidentes, todo esto fue de manera verbal.

Las amenazas están clasificadas de la siguiente manera:

- De origen natural.
- Del entorno.
- Defecto de las aplicaciones.
- Causadas por las personas de forma accidental.

- Causadas por las personas de forma deliberada.

La Tabla 11 muestra cuales son las amenazas que residen sobre los activos.

**Tabla 11: Amenazas sobre los activos**

| Activo | Tipo de riesgo | Amenaza |
|---|---|---|
| **Aplicación web para coordinación de proyectos** | Defecto de las aplicaciones | Mantenimiento inadecuado |
| | | Huecos de seguridad |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Aplicación web de reportes internos y externos** | Defecto de las aplicaciones | Mantenimiento inadecuado |
| | | Huecos de seguridad |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Sistema mensajería premium** | Defecto de las aplicaciones | Mantenimiento inadecuado |
| | | Huecos de seguridad |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Impresoras térmicas** | De origen natural | Terremoto |
| | | Inundación |
| | Del entorno | Incendio |
| | | Suciedad |
| | | Desgaste de partes |
| | | Corte de suministro de luz |
| | Defectos de las aplicaciones | Mantenimiento inadecuado |
| **Servidores** | De origen natural | Terremoto |
| | | Inundación |
| | Del entorno | Incendio |

| Activo | Tipo de riesgo | Amenaza |
|---|---|---|
| | | Suciedad |
| | | Desgaste de partes |
| | | Corte de suministro de luz |
| | Defectos de las aplicaciones | Mantenimiento inadecuado |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| | Causada por las personas de forma accidental/deliberada | Denegación de servicio por error |
| **Routers** | De origen natural | Terremoto |
| | | Inundación |
| | Del entorno | Incendio |
| | | Suciedad |
| | | Desgaste de partes |
| | | Corte de suministro de luz |
| **Sistema de mensajería masiva** | Defectos de las aplicaciones | Subir código con fallas a producción |
| | | Huecos de seguridad |
| | | No tener control de versiones |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Aplicación web marketing digital** | Defectos de las aplicaciones | Subir código con fallas a producción |
| | | Huecos de seguridad |
| | | No tener control de versiones |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Motor base de datos** | Defectos de las aplicaciones | No tener respaldo de información |
| | | Mantenimiento inadecuado |
| | | No tener integridad en los datos |

| Activo | Tipo de riesgo | Amenaza |
|---|---|---|
| | Causada por las personas de forma accidental | Eliminación errónea de registros |
| **Documentos físicos** | De origen natural | Inundación |
| | Del entorno | Incendio |
| | | Suciedad |
| | | Desgaste de hojas |
| | Causada por las personas de forma accidental/deliberada | Destrucción de la información |
| | | Robo |
| **Computadoras/Laptops** | De origen natural | Terremoto |
| | | Inundación |
| | Del entorno | Incendio |
| | | Suciedad |
| | | Desgaste de partes |
| | | Corte de suministro de luz |
| | Defectos de las aplicaciones | Mantenimiento inadecuado |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| **Sistema operativo** | Defectos de las aplicaciones | Mantenimiento inadecuado |
| | Causada por las personas de forma deliberada | Acceso no autorizado |
| | Causada por las personas de forma accidental/deliberada | Virus |
| | | Eliminación de registros para el correcto funcionamiento del SO |

**Fuente:** Los autores

### 4.3.5 VALORACIÓN DE LAS AMENAZAS

Las amenazas se valorizan de acuerdo a la probabilidad de ocurrencia y al impacto sobre el proceso afectado. La Tabla 12 muestra la escala de valorización entre probabilidad de ocurrencia e impacto.

**Tabla 12: Escala de valoración de probabilidad/impacto**

| Probabilidad | Impacto-Consecuencia | | | | |
|---|---|---|---|---|---|
| | Insignificante | Menor | Moderado | Mayor | Catastrófi_co |
| Raro | Bajo | Bajo | Moderado | Alto | Alto |
| Improbable | Bajo | Bajo | Moderado | Alto | Extremo |
| Posible | Bajo | Moderado | Alto | Extremo | Extremo |
| Probable | Moderado | Alto | Alto | Extremo | Extremo |
| Casi seguro | Alto | Alto | Extremo | Extremo | Extremo |

**Fuente:** Los autores

La Tabla 13 muestra la valoración de amenazas de los activos del proceso de mensajería masiva.

**Tabla 13: Valoración de las amenazas**

| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto |
|---|---|---|---|---|
| Aplicación web para coordinación de proyectos | Defecto de las aplicaciones | Mantenimiento inadecuado | Probable | Menor |
| | | Huecos de seguridad | Probable | Menor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Posible | Menor |
| Aplicación web de reportes internos y externos | Defecto de las aplicaciones | Mantenimiento inadecuado | Probable | Mayor |
| | | Huecos de seguridad | Probable | Mayor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Posible | Menor |

| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto |
|---|---|---|---|---|
| Sistema de mensajería premium | Defecto de las aplicaciones | Mantenimiento inadecuado | Probable | Mayor |
| | | Huecos de seguridad | Probable | Mayor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Probable | Catastrófico |
| Impresoras térmicas | De origen natural | Daño por terremoto | Improbable | Menor |
| | | Daño por inundación | Improbable | Menor |
| | Del entorno | Daño por incendio | Posible | Menor |
| | | Daño por suciedad | Posible | Menor |
| | | Desgaste de partes | Posible | Menor |
| | | Corte de suministro de luz | Posible | Menor |
| | Defectos de las aplicaciones | Mantenimiento inadecuado | Probable | Menor |
| Servidores | De origen natural | Terremoto | Improbable | Catastrófico |
| | | Inundación | Improbable | Catastrófico |
| | Del entorno | Incendio | Posible | Catastrófico |
| | | Suciedad | Probable | Catastrófico |
| | | Desgaste de partes | Probable | Moderado |
| | | Corte de suministro de luz | Posible | Mayor |
| | Defectos de las aplicaciones | Mantenimiento inadecuado | Probable | Menor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Posible | Mayor |

| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto |
|---|---|---|---|---|
| | Causada por las personas de forma accidental/deliberada | Denegación de servicio por error | Probable | Mayor |
| Routers | De origen natural | Daño por terremoto | Improbable | Moderado |
| | | Daño por inundación | Improbable | Moderado |
| | Del entorno | Daño por incendio | Posible | Moderado |
| | | Daño por suciedad | Probable | Moderado |
| | | Desgaste de partes | Probable | Moderado |
| | | Corte de suministro de luz | Posible | Moderado |
| Sistema de mensajería masiva | Defectos de las aplicaciones | Subir código con fallas a producción | Casi seguro | Moderado |
| | | Huecos de seguridad | Casi seguro | Moderado |
| | | No tener control de versiones | Posible | Menor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Probable | Menor |
| Aplicación web marketing digital | Defectos de las aplicaciones | Subir código con fallas a producción | Casi seguro | Moderado |
| | | Huecos de seguridad | Casi seguro | Moderado |
| | | No tener control de versiones | Posible | Menor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Posible | Menor |
| Motor base de datos | Defectos de las aplicaciones | No tener respaldo de información | Posible | Moderado |
| | | Mantenimiento inadecuado | Improbable | Menor |

| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto |
|---|---|---|---|---|
| | | No tener integridad en los datos | Posible | Mayor |
| | Causada por las personas de forma accidental | Eliminación errónea de registros | Probable | Catastrófico |
| Documentos físicos | De origen natural | Daño por inundación | Improbable | Menor |
| | Del entorno | Daño por incendio | Improbable | Menor |
| | | Daño por suciedad | Posible | Menor |
| | | Desgaste de hojas | Casi seguro | Menor |
| | Causada por las personas de forma accidental/deliberada | Destrucción de la información | Probable | Menor |
| | | Robo | Posible | Menor |
| Computadoras/Laptops | De origen natural | Daño por Terremoto | Improbable | Moderado |
| | | Daño por inundación | Improbable | Moderado |
| | Del entorno | Daño por incendio | Posible | Menor |
| | | Daño por suciedad | Posible | Menor |
| | | Desgaste de partes | Posible | Menor |
| | | Corte de suministro de luz | Posible | Menor |
| | Defectos de las aplicaciones | Mantenimiento inadecuado | Probable | Menor |
| | Causada por las personas de forma deliberada | Acceso no autorizado | Probable | Menor |
| Sistema operativo | Defectos de las aplicaciones | Mantenimiento inadecuado | Probable | Moderado |

| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto |
|---|---|---|---|---|
| | Causada por las personas de forma deliberada | Acceso no autorizado | Probable | Moderado |
| | Causada por las personas de forma accidental/deliberada | Virus | Probable | Mayor |
| | | Eliminación de registros para el correcto funcionamiento del SO | Posible | Mayor |

**Fuente**: Los autores

### 4.3.6 MATRIZ DE ANÁLISIS DE RIESGOS

Con la valoración de los inventarios y la valoración de las amenazas detectadas sobre los activos, se procede a realizar la matriz de análisis de riesgos, ver Anexo B.

Las amenazas a la cual se les aplicará el esquema de seguridad para la mitigación, son los que tiene una clasificación ‘Alto’ y ‘Extremo’.

### 4.3.7 IDENTIFICACION DE LOS RIESGOS CON MAYOR INCIDENCIA

No se cuenta con una bitácora a algún registro formal sobre las amenazas y el número de incidencias, por lo que los valores que se ponen en la Tabla 14 fueron indicados verbalmente por el jefe de sistemas y se nos indicó que pueden ser menor o mayor a lo real.

**Tabla 14: Incidencias de las amenazas**

| Tipo de amenaza | Amenaza | No. Incidencias | Porcentaje |
|---|---|---|---|
| Deliberadas (D) | Acceso no autorizado | 20 | 11.56% |
| Accidentales (A) | Eliminación errónea de registros | 5 | 2.89% |
| Accidentales (A) | Denegación de servicio por error | 8 | 4.62% |
| Accidentales (A) | Subir códigos con fallas a producción | 38 | 21.97% |
| Deliberadas (D) | Mantenimiento inadecuado | 28 | 16.18% |
| Accidentales (A) | Virus | 40 | 23.12% |
| Accidentales(A) | Eliminación de registros para el correcto funcionamiento del SO | 3 | 1.73% |
| Entorno (E) | Daño por suciedad | 15 | 8.67% |
| Entorno (E) | Desgaste de partes | 10 | 5.78% |
| Accidentales (A) | Destrucción de la información | 5 | 2.89% |
| Entorno (E) | Daño por inundación | 1 | 0.58% |
| Total amenazas | | 173 | 100% |

**Fuente:** Los autores

En el siguiente gráfico de pastel se puede apreciar cuales son las incidencias con mayor probabilidad de ocurrencia.

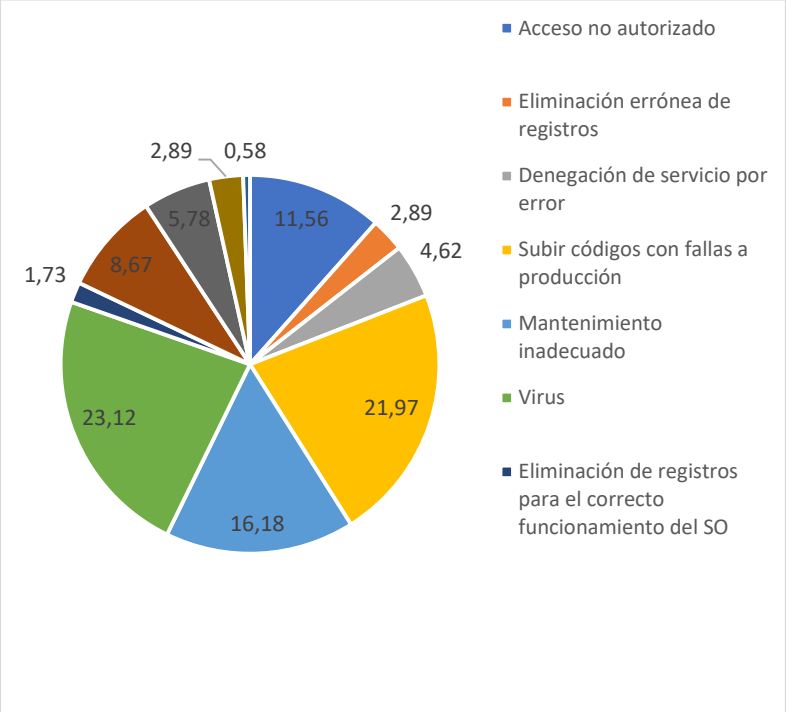



**Figura 4.1: Incidencias de las amenazas**

**Fuente:** Los autores

### 4.3.8 EVALUACIÓN DE RIESGOS

Basados en el porcentaje de incidencias que ha tenido cada amenaza se muestran los riesgos inherentes y los riesgos residuales.

Para el cálculo de riesgos inherentes y riesgos residuales se debe valorizar el impacto del riesgo y la probabilidad del riesgo, gracias a la matriz de análisis de riesgos ya conocemos cuales son los riesgos que tienen una clasificación “Extremo”, “Alto”, “Moderado” y “Bajo”. La Tabla 15 muestra la valorización.

**Tabla 15: Valoración del riesgo**

| Nivel de riesgo inherente | Calificación |
|---|---|
| Extremo | 60 |
| Alto | 30 - 40 |
| Moderado | 15 – 20 |
| Bajo | 5 - 10 |

**Fuente:** Los autores

En la Tabla 16 muestra la calificación de los riesgos inherentes

**Tabla 16: Calificación de riesgos**

| Activo | Amenaza | Clasificación | Calificación |
|---|---|---|---|
| Aplicación web para coordinación de proyectos | Mantenimiento inadecuado | Alto | 35 |
| Aplicación web para coordinación de proyectos | Huecos de seguridad | Alto | 35 |
| Aplicación web para coordinación de proyectos | Acceso no autorizado | Moderado | 20 |
| Aplicación web de reportes internos y externos | Mantenimiento inadecuado | Extremo | 60 |
| Aplicación web de reportes internos y externos | Huecos de seguridad | Extremo | 60 |
| Aplicación web de reportes internos y externos | Acceso no autorizado | Moderado | 20 |
| Sistema de mensajería premium | Mantenimiento inadecuado | Extremo | 60 |
| Sistema de mensajería premium | Huecos de seguridad | Extremo | 60 |
| Sistema de mensajería premium | Acceso no autorizado | Extremo | 60 |
| Impresoras térmicas | Terremoto | Bajo | 5 |

| Activo | Amenaza | Clasificación | Calificación |
|---|---|---|---|
| Impresoras térmicas | Inundación | Bajo | 5 |
| Impresoras térmicas | Incendio | Moderado | 15 |
| Impresoras térmicas | Suciedad | Moderado | 18 |
| Impresoras térmicas | Desgaste de partes | Moderado | 18 |
| Impresoras térmicas | Corte de suministro de luz | Moderado | 15 |
| Impresoras térmicas | Mantenimiento inadecuado | Moderado | 15 |
| Servidores | Terremoto | Extremo | 60 |
| Servidores | Inundación | Extremo | 60 |
| Servidores | Incendio | Extremo | 60 |
| Servidores | Suciedad | Extremo | 60 |
| Servidores | Desgaste de partes | Alto | 35 |
| Servidores | Corte de suministro de luz | Extremo | 60 |
| Servidores | Mantenimiento inadecuado | Alto | 38 |
| Servidores | Acceso no autorizado | Extremo | 60 |
| Servidores | Denegación de servicio por error | Extremo | 60 |
| Routers | Terremoto | Moderado | 15 |
| Routers | Inundación | Moderado | 15 |
| Routers | Incendio | Alto | 30 |
| Routers | Suciedad | Alto | 30 |
| Routers | Desgaste de partes | Alto | 30 |
| Routers | Corte de suministro de luz | Alto | 30 |
| Sistema de mensajería masiva | Subir código con fallas a producción | Extremo | 60 |
| Sistema de mensajería masiva | Huecos de seguridad | Extremo | 60 |
| Sistema de mensajería masiva | No tener control de versiones | Moderado | 15 |
| Sistema de mensajería masiva | Acceso no autorizado | Alto | 30 |

| Activo | Amenaza | Clasificación | Calificación |
|---|---|---|---|
| Aplicación web marketing digital | Subir código con fallas a producción | Extremo | 60 |
| Aplicación web marketing digital | Huecos de seguridad | Extremo | 60 |
| Aplicación web marketing digital | No tener control de versiones | Moderado | 15 |
| Aplicación web marketing digital | Acceso no autorizado | Moderado | 20 |
| Motor base de datos | No tener respaldo de información | Alto | 35 |
| Motor base de datos | Mantenimiento inadecuado | Bajo | 5 |
| Motor base de datos | No tener integridad en los datos | Extremo | 60 |
| Motor base de datos | Eliminación errónea de registros | Extremo | 60 |
| Documentos físicos | Inundación | Bajo | 5 |
| Documentos físicos | Incendio | Bajo | 5 |
| Documentos físicos | Suciedad | Moderado | 20 |
| Documentos físicos | Desgaste de hojas | Alto | 35 |
| Documentos físicos | Destrucción de la información | Alto | 35 |
| Documentos físicos | Robo | Moderado | 15 |
| Computadoras/Laptops | Terremoto | Moderado | 15 |
| Computadoras/Laptops | Inundación | Moderado | 15 |
| Computadoras/Laptops | Incendio | Moderado | 15 |
| Computadoras/Laptops | Suciedad | Moderado | 15 |
| Computadoras/Laptops | Desgaste de partes | Moderado | 15 |
| Computadoras/Laptops | Corte de suministro de luz | Moderado | 15 |
| Computadoras/Laptops | Mantenimiento inadecuado | Alto | 35 |
| Computadoras/Laptops | Acceso no autorizado | Alto | 35 |
| Sistema operativo | Mantenimiento inadecuado | Alto | 35 |

| Activo | Amenaza | Clasificación | Calificación |
|---|---|---|---|
| Sistema operativo | Acceso no autorizado | Alto | 35 |
| Sistema operativo | Virus | Extremo | 60 |
| Sistema operativo | Eliminación de registros para el correcto funcionamiento del SO | Extremo | 60 |

**Fuente:** Los autores

El riesgo inherente suma un total de 2019, esto debe ser reducido cuando se le apliquen los tratamientos a cada riesgo y ese cálculo será el riesgo residual.

### 4.3.9 MATRIZ DE RIESGOS

Se realizó la matriz de riesgos para determinar cuáles son los riesgos más relevantes para poder aplicar el esquema de seguridad, en el anexo E se muestra la matriz de riesgos.

De la matriz de riesgo se procedió a realizar los respectivos mapas de calor de los valores de criticidad actual y un mapa de calor con los valores de criticidad propuestos, en la Figura 6 muestra el mapa de calor de los riesgos actuales.

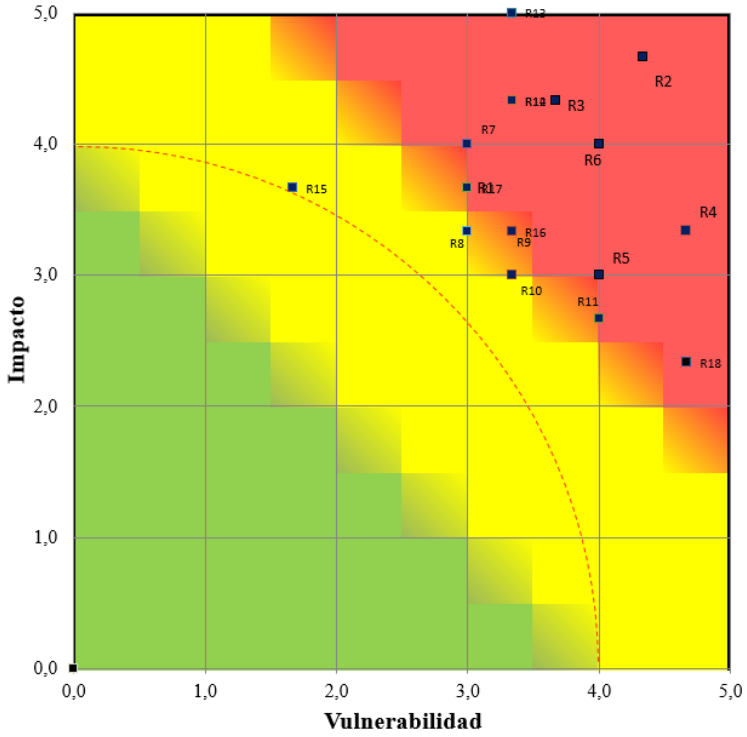



**Figura 4.2: Mapa de calor con valores de criticidad de riesgos actuales**

**Fuente:** Los autores

Posterior a la implementación de los controles seleccionados para mitigar las amenazas y conociendo el porcentaje esperado de cumplimiento, se repite la evaluación de las amenazas tanto en vulnerabilidad como en impacto, resultando en una criticidad representada en el mapa de calor de la Figura 6.

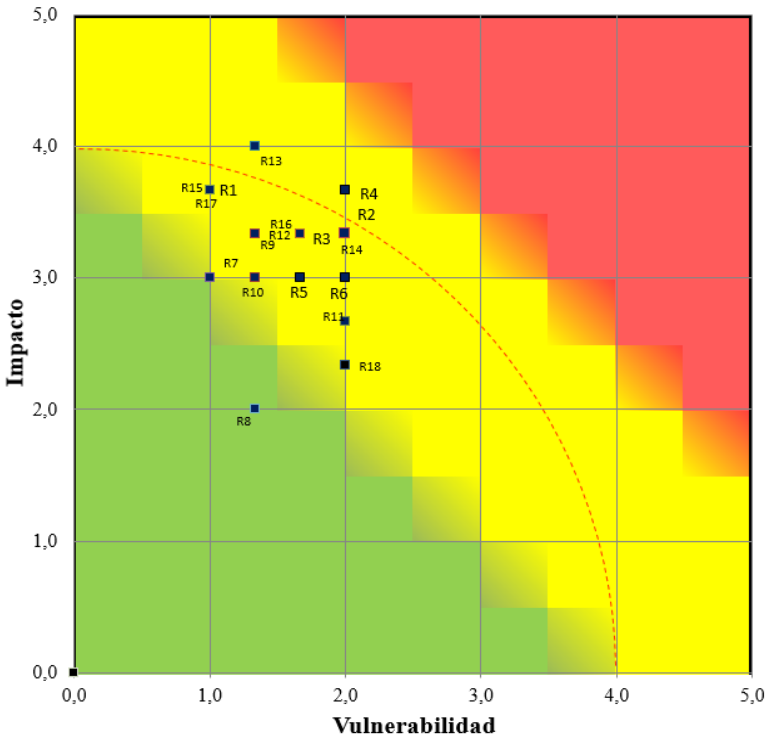



**Figura 4.3: Mapa de calor con valores de criticidad después de implementar los controles**

**Fuente:** Los autores

# CAPÍTULO 5

# IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD BASADO EN LA NORMA ISO 27001:2013

## 5.1 DECLARACIÓN DE APLICABILIDAD

Con la información previamente analizada, se procede a diseñar el tratamiento de riesgos, esto es analizar que controles se pueden aplicar al proceso de mensajería masiva para mitigar el impacto de incidencias sobre los activos**.**

En la Tabla 17 se muestran los controles que se implementarán en el proceso de mensajería masiva, esta información es sacada de la declaración de aplicabilidad que se encuentra en el Anexo B.

**Tabla 17: Políticas aplicables al proceso de mensajería masiva**

| Control | Descripción |
|---|---|
| **A5** | **POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN** |
| **A5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** |
| A5.1.1 | Políticas para la seguridad de la información |
| A5.1.2 | Revisión de las políticas para la seguridad de la información. |
| **A6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** |
| **A6.1** | **Organización interna** |
| A6.1.1 | Roles y responsabilidades para la seguridad de la información |
| **A8** | **GESTIÓN DE ACTIVOS** |
| **A8.1** | **Responsabilidad por los activos** |
| A8.1.1 | Inventario de activos |
| A8.1.2 | Propiedad de los activos |
| A8.1.3 | Uso aceptable de los activos |
| **A8.2** | **Clasificación de la información** |
| A8.2.1 | Clasificación de la información |
| A8.2.3 | Manejo de activos |
| **A9** | **CONTROL DE ACCESO** |
| **A9.1** | **Requisitos del negocio para el control de acceso** |
| A9.1.1 | Política de control de acceso |
| A9.1.2 | Acceso a redes y a servicios en red |
| **A9.2** | **Gestión de acceso de usuarios** |
| A9.2.1 | Registro y cancelación del registro de usuarios |

| Control | Descripción |
|---|---|
| A9.2.2 | Suministro de acceso de usuarios |
| A9.2.3 | Gestión de derechos de acceso privilegiado |
| A9.2.4 | Gestión de información de autenticación secreta de usuarios |
| A9.2.5 | Revisión de los derechos de acceso de usuarios |
| A9.2.6 | Retiro o ajuste de los derechos de acceso |
| **A9.4** | **Control de acceso a sistemas y aplicaciones** |
| A9.4.1 | Restricción de acceso a la información |
| A9.4.2 | Procedimiento de ingreso seguro |
| A9.4.3 | Sistema de gestión de contraseñas |
| A9.4.5 | Control de acceso a códigos fuente de programas |
| **A11** | **SEGURIDAD FÍSICA Y DEL ENTORNO** |
| **A11.1** | **Áreas seguras** |
| A11.1.2 | Controles de acceso físicos |
| **A11.2** | **Equipos** |
| A11.2.1 | Ubicación y protección de los equipos |
| A11.2.4 | Mantenimiento de los equipos. |
| A11.2.5 | Retiro de activos |
| **A12** | **SEGURIDAD DE LAS OPERACIONES** |
| **A12.1** | **Procedimientos operacionales y responsabilidades** |
| A12.1.1 | Gestión de cambios |
| A12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación |

| Control | Descripción |
|---|---|
| **A12.2** | **Protección contra códigos maliciosos** |
| A12.2.1 | Controles contra códigos maliciosos |
| **A12.3** | **Copias de respaldo** |
| A12.3.1 | Respaldo de la información |
| **A12.4** | **Registro y seguimiento** |
| A12.4.1 | Registro de eventos |
| A12.4.2 | Protección de la información de registro |
| A12.4.3 | Registros del administrador y del operador |
| **A12.5** | **Control de software operacional** |
| A12.5.1 | Instalación de software en sistemas operativos |
| **A12.7** | **Consideraciones sobre auditorias de sistemas de información** |
| A12.7.1 | Controles de auditorias de sistemas de información |
| **A13** | **SEGURIDAD DE LAS COMUNICACIONES** |
| **A13.1** | **Gestión de la seguridad de las redes** |
| A13.1.1 | Controles de redes |
| A13.1.2 | Seguridad de los servicios de red |
| A13.1.3 | Separación en las redes |
| **A13.2** | **Transferencia de información** |
| A13.2.4 | Acuerdos de confidencialidad o de no divulgación |
| **A14.2** | **Seguridad en los procesos de Desarrollo y de Soporte** |
| A.14.2.1 | Política de desarrollo seguro |

| Control | Descripción |
|---|---|
| A.14.2.2 | Procedimientos de control de cambios en sistemas |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software |
| A.14.2.5 | Principio de Construcción de los Sistemas Seguros. |
| A.14.2.6 | Ambiente de desarrollo seguro |
| A.14.2.8 | Pruebas de seguridad de sistemas |
| **A16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** |
| **A16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** |
| A16.1.2 | Reporte de eventos de seguridad de la información |
| A16.1.3 | Reporte de debilidades de seguridad de la información |
| A16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos |
| A16.1.5 | Respuesta a incidentes de seguridad de la información |
| A16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información |
| A16.1.7 | Recolección de evidencia |
| **A17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO** |
| **A17.1** | **Continuidad de Seguridad de la información** |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información |
| A17.1.2 | Implementación de la continuidad de la seguridad de la información |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información |
| **A17.2** | **Redundancias** |
| A17.2.1 | Disponibilidad de instalaciones de procesamiento de información |

| Control | Descripción |
|---|---|
| A18.2 | Revisiones de seguridad de la información |
| A18.2.1 | Revisión independiente de la seguridad de la información |
| A18.2.2 | Cumplimiento con las políticas y normas de seguridad |
| A18.2.3 | Revisión del cumplimiento técnico |

**Fuente:** Los autores

## 5.2 TRATAMIENTO DE RIESGOS

Para el tratamiento de riesgos existen cuatro opciones. Aplicar los controles de seguridad para disminuir el riesgo, transferir el riesgo, evitar el riesgo y aceptar el riesgo. Al proceso de mensajería masiva se les aplicó los controles a los riesgos para poder mitigarlos, por decisión de la alta gerencia no se optó por transferir el riesgo.

Con los controles aplicables, seleccionados por medio de la evaluación de riesgos, se procede a documentar su implementación. En esta sección del documento, se traslada lo analizado de la teoría a la práctica. Para esto, se describen políticas de seguridad con el procedimiento, los responsables y los recursos necesarios para lograrlo. Posteriormente se agruparán lo controles con las amenazas a las que corresponde, y finalmente se analizarán los resultados de la implementación y el cumplimiento de los objetivos.

### 5.2.1 PLAN DE TRATAMIENTO DE RIESGOS

En la Tabla 18 se muestra el plan de tratamiento de riesgos que se usó para el proceso de mensajería masiva.

**Tabla 18: Plan de tratamiento de riesgos.**

| Activos | Responsable | Amenazas | Vulnerabilidades | Controles |
|---|---|---|---|---|
| Servidores | Jefe de TI | Terremoto | *Ausencia de diseño antisísmico en el edificio | A11.1.2.<br>A11.2.1.<br>A17.2.1.<br>A11.2.4.<br>A11.2.5.<br>A9.1.1.<br>A12.4.1.<br>A8.2.3.<br>A8.1.3. |
| | | Inundación | *Fallo en las bombas de agua. | |
| | | Incendio | *No contar con extintores.<br>*Personas que fumen dentro de las instalaciones | |
| | | Suciedad | *No realizar la limpieza adecuada a los servidores.<br>*No realizar la limpieza adecuada en el cuarto donde se encuentran los servidores. | |
| | | Corte de suministro de luz | *No contar con fuentes de energías alternas. | |
| | | Acceso no autorizado | *No contar con panel de seguridad para el acceso al cuarto.<br>*No tener definidos permisos de acceso por usuario. | |

| Activos | Responsable | Amenazas | Vulnerabilidades | Controles |
|---|---|---|---|---|
| | | Denegación de servicio por error | *No mantener actualizado el sistema operativo.<br><br>*No contar con cortafuegos adecuados.<br><br>*Permitir el acceso a usuarios no autorizados. | |
| | | Desgaste de partes | *No poseer repuestos adecuados.<br><br>*No mantener el servidor en un lugar adecuado. | |
| Aplicación web para aplicación de proyectos | Jefe de TI | Mantenimiento inadecuado | *Subir errores al código en producción.<br><br>*Subir con fallos de seguridad alguna actualización. | A14.2.1.<br><br>A14.2.2.<br><br>A14.2.6.<br><br>A14.2.8. |
| | | Huecos de seguridad | *No realizar las pruebas necesarias. | A12.1.4. |
| Aplicación web de reportes internos y externos | Jefe de TI | Mantenimiento inadecuado | *Subir errores al código en producción.<br><br>*Subir con fallos de seguridad alguna actualización. | A14.2.1.<br><br>A14.2.2.<br><br>A14.2.6.<br><br>A14.2.8. |
| | | Huecos de seguridad | *No realizar las pruebas necesarias. | A12.1.4. |
| Sistema de mensajería premium | Jefe de TI | Mantenimiento inadecuado | *Subir errores al código en producción.<br><br>*Subir con fallos de seguridad alguna actualización. | A14.2.1.<br><br>A14.2.2.<br><br>A14.2.6.<br><br>A14.2.8. |
| | | Huecos de seguridad | *No realizar las pruebas necesarias. | |

| Activos | Responsable | Amenazas | Vulnerabilidades | Controles |
|---|---|---|---|---|
| | | Acceso no autorizado | * No tener definidos permisos de acceso por usuario. | A9.1.1.<br>A9.1.2.<br>A9.2.1.<br>A9.2.2.<br>A.9.2.6.<br>A12.1.4. |
| Routers | Jefe de TI | Incendio | *No contar con extintores.<br>*Personas que fumen dentro de las instalaciones | A11.1.2.<br>A11.2.1.<br>A17.2.1. |
| | | Suciedad | *No realizar la limpieza adecuada a los servidores.<br>*No realizar la limpieza adecuada en el cuarto donde se encuentran los servidores. | A11.2.4.<br>A11.2.5.<br>A9.1.1.<br>A12.4.1. |
| | | Corte de suministro de luz | *No contar con fuentes de energías alternas. | A8.2.3<br>A8.1.3. |
| Sistema de mensajería masiva | Jefe de TI | Subir códigos con fallas a producción | *No haber pasado por un ambiente de pruebas.<br>*No hacer las pruebas necesarias para encontrar errores o bugs. | A14.2.1.<br>A14.2.2.<br>A14.2.6.<br>A14.2.8.<br>A9.1.1. |
| | | Huecos de seguridad | *No realizar las pruebas necesarias. | A9.1.2. |
| | | Acceso no autorizado | * No tener definidos permisos de acceso por usuario. | A9.2.1.<br>A9.2.2. |

| Activos | Responsable | Amenazas | Vulnerabilidades | Controles |
|---|---|---|---|---|
| | | | | A.9.2.6.<br>A12.1.4. |
| Aplicación web marketing digital | Jefe de TI | Subir códigos con fallas a producción | *No haber pasado por un ambiente de pruebas.<br>*No hacer las pruebas necesarias para encontrar errores o bugs. | A14.2.1.<br>A14.2.2.<br>A14.2.6.<br>A14.2.8. |
| | | Huecos de seguridad | *No realizar las pruebas necesarias. | A12.1.4. |
| Motor de base de datos | Jefe de TI | No tener respaldo de la información | *Los respaldos automáticos no están funcionando.<br>*No probar los respaldos generados. | A12.3.1<br>A9.1.2.<br>A9.2.1.<br>A9.2.2. |
| | | Eliminación errónea de registros | *Dar acceso a usuario no autorizado.<br>*Falla en la interfaz middleware que se comunica con la base de datos. | A.9.2.6.<br>A12.4.1<br>A12.4.2.<br>A12.4.3 |
| Documentos físicos | Jefe de TI | Desgastes de hojas | *No tener copia del documento. | A12.3.1 |
| | | Destrucción de la información | *Los documentos sean accesibles por cualquier persona. | A11.1.2. |
| Computadoras/Laptops | Jefe de TI | Mantenimiento inadecuado | *No realizar limpieza periódicamente. | A11.1.2. |
| | | Acceso no autorizado | *Sea accesible para cualquier personal | A8.1.1<br>A8.1.2<br>A8.1.3 |
| Sistema operativo | Jefe de TI | Mantenimiento inadecuado | *No realizar las actualizaciones necesarias. | A12.2.1 |

| Activos | Responsable | Amenazas | Vulnerabilidades | Controles |
|---|---|---|---|---|
| | | Acceso no autorizado | *No contar con cuentas de usuarios. | A12.3.1.<br>A12.4.1<br>A12.4.2.<br>A9.2.2.<br>A9.2.3.<br>A9.2.4.<br>A9.2.5.<br>A9.2.6. |
| | | Virus | *No actualizar los antivirus. | |
| | | Eliminación de registros para el correcto funcionamiento del S.O. | *No asignar correctamente los privilegios a las cuentas de usuarios. | |

**Fuente:** Los autores

### 5.2.2 IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD

De acuerdo a los controles aplicables para cada riesgo, se ha implementado la debida política de seguridad, agregando las políticas de seguridad que deben ser generales para toda la empresa.

La Tabla 20 muestra las políticas de seguridad que fueron implementadas para el proceso de mensajería masiva.

**Tabla 19: Políticas de seguridad**

| Sección | Control | Política |
|---|---|---|
| A5.1.1 | Políticas para la seguridad de la información | El siguiente grupo de políticas se han definido para la seguridad de la información de la empresa, en contexto al proceso de |

| Sección | Control | Política |
|---|---|---|
| | | mensajería masiva. El departamento de Gerencia será el que apruebe las políticas y posteriormente, asigne a los demás jefes de departamentos, su debida publicación y comunicación. Con la finalidad de alcanzar tanto al personal interno, como a los clientes externos pertinentes. |
| A5.1.2 | Revisión de las políticas para la seguridad de la información. | El grupo de políticas definidas, tendrá un período de revisión anual, con la finalidad de calificar el cumplimiento y eficacia de las mismas de manera continua. Además, se establecen condiciones para modificaciones bajo circunstancias de cambios en infraestructura tecnológica o de cambios significativos en el flujo u otros detalles del proceso de mensajería masiva. |
| A6.1.1 | Roles y responsabilidades para la seguridad de la información | - Los jefes de departamento serán los encargados de informar el estado de los activos correspondientes a su área y del cumplimiento de las políticas por parte del personal a su cargo.<br><br>- Cada empleado tendrá la responsabilidad de informar cualquier novedad a su jefe inmediato acerca de los activos asignados y de cumplir las políticas de seguridad de la información.<br><br>- El gerente general aprobará modificaciones en los responsables de activos según considere pertinente, |

| Sección | Control | Política |
|---|---|---|
| | | incluyendo sugerencias de los jefes de departamento. |
| A8.1.1 | Inventario de activos | - El inventario de activos del proceso de mensajería masiva de la Tabla 6, debe estar disponible y será revisado anualmente y actualizado para los eventos de compra de nuevo hardware, de actualizaciones de software y la infraestructura tecnológica, y de cambios del proceso en cuestión.<br><br>- El acceso al inventario será restringido únicamente para el departamento de ventas en Quito, el departamento de sistemas en Guayaquil y la Gerencia General. |
| A8.1.2 | Propiedad de los activos | - El documento para el inventario de activos, tendrá una sección en donde se indique el historial de personas responsables de la seguridad del mismo, así como la persona encargada actualmente.<br><br>- Si el activo no tiene una persona asignada, dado que es nuevo o ha sido dado de baja, se le asignará al jefe del departamento de sistemas como responsable si el activo se encuentra en Guayaquil o en la nube, y se le asignará al jefe del departamento financiero si el activo se encuentra en Quito. |
| A8.1.3 | Uso aceptable de los activos | - El documento para el inventario de activos, tendrá un detalle indicando la ubicación física del mismo, con historial de traslado |

| Sección | Control | Política |
|---|---|---|
| | | entre Guayaquil, Quito u otra ciudad.<br><br>- La información en custodio, sea esta física o lógica que la empresa proporcione o reciba del responsable a cargo, deberá ser utilizada únicamente para fines del negocio de la organización y de su integridad se hará responsable la persona designada, siendo supervisado cualquier cambio por el inmediato superior.<br><br>- El responsable a cargo de la administración de aplicativos o servicios tecnológicos de la empresa, deberá garantizar disponibilidad para brindar asistencia siempre que se necesite y únicamente para los clientes (internos o externos) autorizados a su acceso.<br><br>- Los activos de hardware que son elementos de la infraestructura, participarán de mantenimientos frecuentes por parte del responsable, así como la verificación del uso conforme con el plan de negocio por parte del inmediato superior. |
| A8.2.1 | Clasificación de la información | - La información debe ser clasificada en función de su valor y criticidad con el motivo de conocer la importancia de la información. |

| Sección | Control | Política |
|---|---|---|
| | | - La información que contiene a los clientes y el sistema de mensajería masiva debe estar clasificado con un valor máximo y una criticidad máxima. |
| A8.2.3 | Manejo de activos | - Los activos con mayor valor y criticidad deben tener un responsable la cual deberá garantizar que el uso de los activos sea el correcto, el activo no debe ser dañado, modificado o eliminado. Este activo deberá contar con algún respaldo que garantice la no perdida de la información.<br><br>- Los activos con menor valor y criticidad deben tener un responsable la cual deberá garantizar que el uso de los activos sea el correcto, el activo no debe ser dañado, modificado o eliminado. |
| A9.1.1 | Política de control de acceso | - Todos los sistemas deben ser accedidos por medio de un usuario y contraseña que autentique únicamente a los clientes interno o externos que correspondan.<br><br>- Las contraseñas serán otorgadas a cada usuario, bajo estatutos de generación de contraseñas seguras.<br><br>- Las contraseñas seguras otorgadas por la empresa, tendrán vigencia por 1 año, antes de ser renovadas. |

| Sección | Control | Política |
|---|---|---|
| | | - Los usuarios con acceso autorizado a los distintos sistemas de la empresa, serán responsable del usuario y contraseña asignados y deberán velar por su confidencialidad. |
| A9.1.2 | Acceso a redes y a servicios en red | - Los servicios web configurados con los clientes externos, serán puestos en producción una vez se realicen pruebas de comunicación y autenticación por medio de una red virtual privada (VPN).<br><br>- Los clientes internos y externos, tendrán acceso únicamente bajo autenticación a los servicios de reportería.<br><br>- Sobre el servicio de reportería interna, los puntos de acceso serán exclusivos a terminales en las redes internas de la empresa. |
| A9.2.1 | Registro y cancelación del registro de usuarios | - Los usuarios deben ser registrados a un sistema de registro de usuarios donde se cuente con toda la información de dicho usuario, tal como el nombre, correo electrónico, privilegios, ultima hora de conexión.<br><br>- La cancelación del registro de usuario se debe dar cuando el usuario ya no trabaja en la empresa, la información debe quedar intacta para fines de histórico pero el acceso ya no debe ser permitido. |

| Sección | Control | Política |
|---|---|---|
| A9.2.2 | Suministro de acceso de usuarios | Todo usuario debe tener bien definido los privilegios dependiendo del cargo a lo que se encuentra.<br><br>- Los usuarios de contabilidad solo deben tener acceso a ventas, compras, inventarios y recursos humanos.<br><br>- Los de marketing digital solo deben tener acceso al sistema de marketing digital.<br><br>- Los desarrolladores de software solo deben tener acceso a los ambientes de pruebas y de producción del sistema de mensajería masiva y sistema de marketing digital. |
| A9.2.3 | Gestión de derechos de acceso privilegiado | Administrar los usuarios que cuenten con acceso privilegiado, se debe poner un registro de acceso al sistema y de cuando se realizó el proceso de autenticación. |
| A9.2.4 | Gestión de información de autenticación secreta de usuarios | Todos los usuarios deben tener, usuario y contraseña para el acceso a los sistemas de información, la contraseña que el usuario genero debe ser guardado como Hash con método MD5 y con un salteo para evitar el acceso no autorizado por fuerza bruta |
| A9.2.5 | Revisión de los derechos de acceso de usuarios | Todas las cuentas de los usuarios deberá ser revisada una vez por semana para evitar una escala de privilegios no autorizada. |

| Sección | Control | Política |
|---|---|---|
| A9.2.6 | Retiro o ajuste de los derechos de acceso | - Se retira el privilegio al usuario una vez que termine sus funciones en la empresa y esto deberá ser total.<br><br>- Para dar más privilegios al usuario debe ser reportado de manera formal por el jefe inmediato de este usuario, así mismo si se le debe dar menos acceso al sistema a la cual ingresan. |
| A9.4.1 | Restricción de acceso a la información | Cada privilegio debe estar bien definido los permisos que tienen y aquellos que no cuentan con permisos no deben ser accedidos por los usuarios con esos privilegios. |
| A9.4.2 | Procedimiento de ingreso seguro | Todo usuario debe autenticarse antes de ingresar el sistema, este medio por el cual se autentican deberá enviar la información ingresada por el usuario de manera encriptada hacia el servidor. |
| A9.4.3 | Sistema de gestión de contraseñas | - Las contraseñas deben tener una longitud mínima de 6 caracteres.<br><br>- La contraseña debe tener mayúsculas, minúsculas, números y mínimo un carácter especial.<br><br>- La contraseña tendrá un periodo de validez de 3 meses, |
| A9.4.5 | Control de acceso a códigos fuente de programas | - El código fuente no puede ser accedido por personal que no tenga como privilegio de desarrollador.<br><br>- Registrar el ingreso del usuario al código. |

| Sección | Control | Política |
|---|---|---|
| | | - El acceso al código fuente debe ser previamente consultado con el jefe inmediato.<br><br>- Si el jefe de sistema es quien ingresa el código fuente este no deberá realizar ningún cambio. |
| A11.1.2 | Controles de acceso físicos | Se debe contar con un sistema electrónico con reconocedor de huellas para el acceso al cuarto donde se encuentren la información o activos con una criticidad alta. |
| A11.2.1 | Ubicación y protección de los equipos | - Los servidores y los routers deben estar ubicados en un cuarto con una refrigeración adecuada, esto es alrededor de 12°C.<br><br>- El acceso a este cuarto deberá ser controlado con un sistema electrónico reconocedor de huellas.<br><br>- En la parte de externa del cuarto, cerca de la puerta deberá estar un extintor de fuego. |
| A11.2.4 | Mantenimiento de los equipos. | - Las computadoras y laptops deberán ser revisadas y actualizadas una vez al mes por el personal de sistemas, se deberá actualizar sistemas antivirus, actualizar parches del sistema operativo, eliminar registros o archivos que sean innecesarios para la labor que realiza el usuario, se debe realizar la limpieza adecuada si este lo amerita. |

| Sección | Control | Política |
|---|---|---|
| | | - Los equipos de servidores y routers se debe dar mantenimiento una vez al mes, se debe revisar conexiones, temperatura del CPU y si la temperatura en el cuarto es la adecuada, se debe realizar la limpieza adecuada si este lo amerita.<br><br>- Los mantenimientos de computadores y laptops se deben planificar con 24 horas de antelación y deberá ser fuera de horarios laborales. La fecha definida no debe ser la misma al mantenimiento de routers y servidores<br><br>- Los mantenimientos de servidores y routers se deben planificar con 24 horas de antelación y deberá ser un fin de semana fuera de horas laborables. La fecha definida no debe ser el mismo que el mantenimiento de computadores y laptops. |
| A11.2.5 | Retiro de activos | Se debe dar de baja en el inventario aquellos activos que se consideren obsoletos para continuar en el proceso de mensajería masivo y que no pueda ser usado en algún otro proceso. |
| A12.1.1 | Procedimientos operacionales y responsabilidades | - Documentar el proceso para subir código nuevo al sistema de producción.<br><br>- Documentar el proceso para asignar, quitar y aumentar permisos de acceso a los usuarios. |

| Sección | Control | Política |
|---|---|---|
| | | - Documentar el proceso de registros a los clientes. |
| A12.1.2 | Gestión de cambios | - La petición de cambio debe ser dada de manera formal y aprobada por la alta gerencia.<br><br>- Registrar la petición de cambio.<br><br>- Realizar las pruebas necesarias en un ambiente seguro sin que afecte el proceso de operación.<br><br>- Se debe planificar para la implantación del cambio en el proceso de operación.<br><br>- Se debe contar con un respaldo de la información antes de realizar dicho cambio.<br><br>- Revisar el cambio realizado y documentar los resultados. |
| A12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | - Debe existir el entorno de producción, entorno de pruebas y el entorno de desarrollo, estos tres entornos deben ser completamente independientes, esto es, un entorno no debe verse afectado por problemas de otro entorno.<br><br>- Cada entorno mencionado anteriormente debe estar en una red distinta.<br><br>- Se debe contar con perfiles de acceso distintos para acceder de un entorno a otro. |

| Sección | Control | Política |
|---|---|---|
| | | - Se debe contar con un responsable que garantice que la ejecución de un entorno no interrumpa las operaciones de otros sistemas o redes. |
| A12.2.1 | Controles contra códigos maliciosos | - Todos los sistemas operativos deberán contar con un antivirus actualizado.<br><br>- Todos los sistemas operativos deberán contar con un software de recuperación de archivos en caso de que alguno sea eliminado por un virus. |
| A12.3.1 | Respaldo de la información | - Toda información que fue clasificada con valor alto y criticidad alta deberá tener su respaldo.<br><br>- Los respaldos de información debe ser diaria.<br><br>- Todos los respaldos deben ser probados y verificados. |
| A12.4.1 | Registro de eventos | Se debe contar con un sistema de registro de eventos.<br><br>* Registrar cada acceso al sistema.<br><br>* Registrar las acciones de los usuarios.<br><br>* Registrar fallas reportadas. |
| A12.4.2 | Protección de la información de registro | - Los registros se deben almacenar en una base de datos distinta a la base de operación, esto es en la base de datos especializada para logs. |

| Sección | Control | Política |
|---|---|---|
| | | - Los registros almacenados como archivos no deben ser modificados y deben tener código de seguridad para poder leerlos.<br><br>- Los registros deben tener copias para evitar la pérdida de vital de información.<br><br>- Garantizar que el sistema donde se encuentran alojados todos los registros cuenten con la capacidad necesaria para almacenar gran cantidad de información. |
| A12.4.3 | Registros del administrador y del operador | Registrar el acceso del administrador y las acciones del mismo. |
| A12.5.1 | Instalación de software en sistemas operativos | - Los usuarios comunes no deben tener la autorización para instalar, actualizar o modificar software en el sistema operativo.<br><br>- Toda instalación de software debe tener su debida autorización y el registro del día/hora y usuario en la que se llevó acabo.<br><br>- Se debe probar en un ambiente seguro la instalación del nuevo software para evitar infiltración de algún virus que tenga oculto dicho software. |
| A12.7.1 | Controles de auditorías de sistemas de información | Todo mantenimiento, control o actualización de los sistemas de información se debe notificar con una antelación de 24 horas y |

| Sección | Control | Política |
|---|---|---|
| | | este deberá se fuera las horas laborables |
| A13.1.1 | Controles de redes | - Los dispositivos de red deben autenticarse para poder conectarse a la red.<br><br>- Se debe contar con filtrado de direcciones MAC para evitar conexiones no deseadas.<br><br>- Se debe contar con un cortafuego ubicado entre el acceso a internet y la red local.<br><br>- Se deben cerrar los puertos que no sean usados por alguna aplicación dentro de la empresa. |
| A13.1.2 | Seguridad de los servicios de red | Se debe contar con corta fuegos, con sistemas de detección de intrusos y con una zona desmilitarizada |
| A13.1.3 | Separación en las redes | - Se debe segmentar la red inalámbrica con la red física.<br><br>- Se debe tener 5 VLANs: uno para los servidores de producción, uno para desarrollo, otro para pruebas y otro para los demás usuarios dentro de la organización y el ultimo para separar la red física con la red inalámbrica.<br><br>- Monitorear la segmentación de la redes. |
| A13.2.4 | Acuerdos de confidencialidad o de no divulgación | Se debe firmar un contrato empleador-empleado indicando que este no va a divulgar sobre el trabajo que |

| Sección | Control | Política |
|---|---|---|
| | | realiza y sobre el proceso de mensajería masiva. |
| A.14.2.1 | Política de desarrollo seguro | - Se debe proporcionar un ambiente de desarrollo completamente independiente al ambiente de producción.<br><br>- Las actualizaciones que se suban en este ambiente deberá ser probada y aprobada por el usuario final.<br><br>- Cada reporte que el usuario realiza sobre el sistema deberá ser de manera formal hacia el jefe de sistemas.<br><br>- Una vez aprobada por el cliente, la nueva actualización deberá someterse a pruebas de seguridad. |
| A.14.2.2 | Procedimientos de control de cambios en sistemas | - Los cambios se deben iniciar con una solicitud formal y este debe estar registrada en el sistema de registros.<br><br>- Se debe detallar y guardar el tipo de cambio que se va a realizar ya que ese cambio puede afectar a otros procesos.<br><br>- Registrar la fecha en que se realizara el cambio, la persona encargada de realizar el cambio, que activo y que procesos afectará ese cambio. |

| Sección | Control | Política |
|---|---|---|
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | - Para realizar algún cambio en la plataforma de producción es necesario que sea autorizado por la gerencia de manera formal y esto debe quedar registrado.<br><br>- Revisar que las aplicaciones que afecten al sistema de mensajería masiva funcionen correctamente, esto es realizando pruebas automáticas a estas aplicaciones una vez se haya hecho algún cambio en la plataforma.<br><br>- Se debe registrar todo cambio que se realice en la plataforma. |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software | - No se debe realizar actualizaciones sin realizar una previa investigación sobre la actualización disponible, esta actualización puede afectar el perfecto funcionamiento del resto del sistema.<br><br>- El departamento de sistemas debe estar a cargo de esta investigación sobre la actualización disponible.<br><br>- El usuario común no debe tener permisos para actualizar o realizar un cambio a los paquetes de software. |
| A.14.2.5 | Principio de Construcción de los Sistemas Seguros. | - Todo sistema de software que se encuentre en uso debe tener una documentación técnica y una documentación general sobre el uso, procesos y construcción del mismo. |

| Sección | Control | Política |
|---|---|---|
| | | - Todo sistema de software que este en desarrollo debe tener una documentación técnica y una documentación general sobre el uso, procesos y construcción del mismo. |
| A.14.2.6 | Ambiente de desarrollo seguro | El ambiente de desarrollo seguro debe ser accedido solamente por el personal de sistemas, esto es desarrolladores y el jefe de sistemas. |
| A.14.2.8 | Pruebas de seguridad de sistemas | - Verificar la propiedad de código.<br><br>- Verificar que se cuente con un sistema con licencia válida.<br><br>- Para la realización de pruebas de seguridad se debe informar a la alta gerencia y ser aprobado por ellos, dicha prueba no deberá ser en horarios laborables.<br><br>- Realizar pruebas de explotación de vulnerabilidades y escalamiento de privilegios. |
| A16.1.2 | Reporte de eventos de seguridad de la información | Reportar el evento de manera inmediata por medio de correo electrónico cuyo asunto deberá comenzar con URG.<evento> |
| A16.1.3 | Reporte de debilidades de seguridad de la información | - Realizar reportes sobre las fallas de seguridad que se tuvieron en las pruebas realizadas.<br><br>- Todos los empleados que usen el sistema deben observar y reportar si existe |

| Sección | Control | Política |
|---|---|---|
| | | algún fallo en el sistema, esto se hara por medio de un correo cuyo asunto deberá comenzar con VULN. <vulnerabilidad o debilidad> |
| A16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Todos los eventos surgidos serán evaluados una vez al día y se debe clasificar por criticidad, considerando el daño que provoca el evento al proceso de mensajería masiva |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | - Se debe documentar el procedimiento que se realizó para solucionar o mitigar el incidente.<br><br>- Todo incidente previamente materializado debe ser solucionado siguiendo el procedimiento documentado. |
| A16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | Todo incidente reportado y mitigado debe estar documentado. |
| A16.1.7 | Recolección de evidencia | - Los LOGS generados por el sistema deben ser almacenados en una base de datos dedicados para LOGS.<br><br>- Los logs no deben ser eliminados al menos que tengan un año de antigüedad.<br><br>- Todo correo cuyo asunto comience con URG. o VULN. Debe ser almacenado en una carpeta específica para guardar este tipo de incidentes. |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | Se debe llevar a cabo cada mes y un horario que sea fuera de horas laborables, si esto no es posible, se debe |

| Sección | Control | Política |
|---|---|---|
| | | comunicar al cliente sobre el posible corte de servicio, la fecha y hora, el tiempo de inactividad del servicio y si está de acuerdo. |
| A17.1.2 | Implementación de la continuidad de la seguridad de la información | - Crear un comité de seguridad que vele por el cumplimiento y continuidad de los procesos.<br><br>- Documentar el plan y periodicidad de simulacros.<br><br>- Registrar los resultados de los simulacros establecidos.<br><br>- Crear un procedimiento que reúna todo lo relacionado a la seguridad aplicada al sistema de gestión de seguridad de la información. |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | - Se debe realizar la verificación, revisión y evaluación del plan de continuidad al menos una vez al mes.<br><br>- Se debe tener un registro de evidencias de las pruebas reales y sus resultados.<br><br>- Si en las pruebas realizadas se detecta alguna deficiencia se debe remediar inmediatamente y se debe volver a probar varias veces para asegurar que la solución es eficaz. |
| A17.2.1 | Disponibilidad de instalaciones de procesamiento de información | - Realización de diseños de infraestructura que tengan redundancias a nivel de almacenamiento. |

| Sección | Control | Política |
|---|---|---|
| | | - Realización de respaldos de la información. |
| A18.2.1 | Revisión independiente de la seguridad de la información | - Documentar los hallazgos de auditoria y los procedimientos para solventarlos.<br><br>- Verificar que las implementaciones de controles estén alineadas con los riesgos a activos de la información. |
| A18.2.2 | Cumplimiento con las políticas y normas de seguridad | Revisar y analizar que las políticas implementadas sigan las normas de seguridad aceptadas a nivel global. |
| A18.2.3 | Revisión del cumplimiento técnico | La revisión de los cumplimientos de las políticas de seguridad deberá ser de manera periódica cada 2 meses. |

**Fuente**: Los autores

### 5.2.3 PLAN DE IMPLEMENTACIÓN DE POLÍTICAS

Se realizó un cronograma que indica el tiempo de duración para la implementación de cada política de seguridad, la cual fue propuesto para la empresa de mensajería masiva, en ella se describe los días que tomara para implementar cada política de seguridad. La Tabla 21 muestra el tiempo de duración para cada política a ser implementada.

**Tabla 20: Plan de implementación de políticas**

| Nombre del proyecto | Tiempo (días) |
|---|---|
| ► **Proyecto de Implementación de Políticas de Control de Acceso** | 12 |
| Documentación sobre generación de contraseñas seguras | 0.5 |
| Implementación de alertas para vigencia de contraseñas | 1 |
| Documentación de roles y privilegios para clientes internos y externos | 2 |
| Documentación de solicitudes para elevar o disminuir niveles de privilegios | 0.5 |
| Configuración de puntos de acceso permitidos hacia las aplicaciones de la empresa | 1.5 |
| Implementación de encriptación para autenticación en las aplicaciones | 2 |
| Implementación de registros de acceso de usuarios | 2 |
| Documentación de solicitudes de acceso a código fuente | 0.5 |
| Documentación para pruebas de servicios web externos por medio de VPN | 1 |
| Capacitación de políticas de control de acceso | 1 |
| ► **Proyecto de Implementación de Políticas de Gestión de Activos** | **7** |
| Documentación de actualización y comunicación del inventario de activos | 0.5 |
| Configuración de roles y puntos de acceso al inventario | 1.5 |
| Implementación de secciones del inventario de activos | 2 |
| Documentación de secciones inventario de activos | 1 |
| Documentación de asignaciones de responsables de los activos | 0.5 |
| Documentación de confidencialidad e integridad de los activos | 0.5 |
| Capacitación de políticas de gestión de activos | 1 |
| ► **Proyecto de Implementación de Políticas de Seguridad de las operaciones** | **13** |
| Implementación de entornos de desarrollo, de pruebas y de producción | 3 |

| Nombre del proyecto | Tiempo (días) |
|---|---|
| Configuración de antivirus y restauradores para los equipos | 1 |
| Documentación de entornos de desarrollo | 1 |
| Documentación de respaldo de información | 1 |
| Documentación de solicitudes de cambio para entorno de pruebas y de producción | 1 |
| Documentación de responsables de cada entorno | 0.5 |
| Configuración de registros de acceso y acciones de usuarios | 1 |
| Configuración de base de datos para almacenar registros de usuarios | 1 |
| Documentación para almacenamiento de registros de usuarios | 1 |
| Configuración de privilegios de usuarios en el sistema operativo | 1 |
| Documentación para instalación de nuevo software | 0.5 |
| Capacitación de políticas de seguridad de las operaciones | 1 |
| **► Proyecto de Implementación de Políticas para adquisición, desarrollo y mantenimiento de sistemas** | **8.5** |
| Documentación de creación de nuevos módulos en la plataforma | 1 |
| Documentación de registros y autorizaciones de cambios en producción | 0.5 |
| Documentación sobre actualizaciones de recursos de la plataforma | 0.5 |
| Documentación de uso, procesos y construcción para actuales y nuevas aplicaciones | 4 |
| Documentación sobre autoría de códigos fuentes y licencias | 0.5 |
| Documentación de pruebas de seguridad y vulnerabilidades | 1 |
| Capacitación de políticas para adquisición, desarrollo y mantenimiento de sistemas | 1 |
| **► Proyecto de Implementación de Políticas para la Gestión de Incidentes de la Seguridad de la Información** | **7** |
| Documentación de reporte de incidentes detectados | 1 |
| Documentación de reporte para fallas en pruebas de seguridad | 1 |

| Nombre del proyecto | Tiempo (días) |
|---|---|
| Documentación de clasificación y manejo de incidentes | 1 |
| Documentación de incidentes mitigados | 0.5 |
| Configuración de base de datos para almacenamientos de reportes de incidentes | 1 |
| Documentación para almacenamiento de reportes de incidentes | 0.5 |
| Configuración de carpetas de incidentes en el software de correo | 1 |
| Capacitación de políticas para la gestión de incidentes de la seguridad de la información | 1 |
| **► Proyecto de Implementación de Políticas para la Gestión de Continuidad de Negocio** | 10.5 |
| Documentación de comunicación al cliente sobre inactividad de servicios | 0.5 |
| Crear un comité de seguridad para el cumplimiento y continuidad de los procesos | 2 |
| Documentación sobre planes y periodicidad de simulacros | 1 |
| Documentación de verificación y evaluación mensual del plan de seguridad | 1 |
| Documentación para registros de resultados de simulacros y pruebas | 1 |
| Documentación para la retroalimentación de resultados deficientes | 1 |
| Configuración de redundancias de almacenamiento de la información | 2 |
| Documentación de restauración de la información | 1 |
| Capacitación de políticas para la gestión de continuidad de negocio | 1 |
| **► Proyecto de Implementación de Políticas para el Cumplimiento Legal** | **6** |
| Documentación para registro y manejo de resultados de auditoría | 2 |
| Documentación para análisis de políticas implementadas, mitigación de riesgos y normas de seguridad | 2 |
| Documentación sobre el cumplimiento de políticas de seguridad | 1 |
| Capacitación de políticas para el cumplimiento legal | 1 |

**Fuente**: Los autores

# CAPÍTULO 6

# ANÁLISIS DE RESULTADOS

## 6.1 EVALUACIÓN DE POLÍTICAS DE SEGURIDAD IMPLEMENTADAS

### 6.1.1 POLITICAS DE SEGURIDAD IMPLEMENTADAS EN EL SERVICIO DE MENSAJERIA MASIVA

En base al plan de tratamiento de riesgos, se propuso las siguientes políticas de seguridad para la empresa de servicio de mensajes simples(SMS) y se llevó a cabo la implementación de la misma.

**Políticas de control de acceso**

- Todos los sistemas deben ser accedidos por medio de un usuario y contraseña que autentique únicamente a los clientes interno o externos que correspondan.
- Las contraseñas serán otorgadas a cada usuario, bajo estatutos de generación de contraseñas seguras.

- Las contraseñas seguras otorgadas por la empresa, tendrán vigencia por 1 año, antes de ser renovadas.
- Los usuarios con acceso autorizado a los distintos sistemas de la empresa, serán responsable del usuario y contraseña asignados y deberán velar por su confidencialidad.
- Los sistemas deberán ser accedidos únicamente por usuarios autorizados.
- No se debe acceder a redes inalámbricas inseguras cuando se esté trabajando con información sensible.
- Los servicios web configurados con los clientes externos, serán puestos en producción una vez se realicen pruebas de comunicación y autenticación por medio de una red virtual privada (VPN).
- Los clientes internos y externos, tendrán acceso únicamente bajo autenticación a los servicios de reportes.
- Sobre el servicio de reportes interna, los puntos de acceso serán exclusivos a terminales en las redes internas de la empresa.

Con referencia al registro, cancelación o asignación de permisos a usuarios:

- Todo usuario debe tener bien definido los privilegios dependiendo del cargo a lo que se encuentra.
- Los usuarios de contabilidad solo deben tener acceso a ventas, compras, inventarios y recursos humanos.

- El departamento de Marketing Digital solo debe tener acceso al sistema de marketing digital.
- Los desarrolladores de software solo deben tener acceso a los ambientes de pruebas y de producción del sistema de mensajería masiva y sistema de marketing digital.
- Administrar los usuarios que cuenten con acceso privilegiado, se debe poner un registro de acceso al sistema y de cuando se realizó el proceso de autenticación.
- Todos los usuarios deben tener, usuario y contraseña para el acceso a los sistemas de información, la contraseña que el usuario genero debe ser guardado como Hash con método MD5 y con un salteo para evitar el acceso no autorizado por fuerza bruta.
- Todas las cuentas de los usuarios deberán ser revisada una vez por semana para evitar una escala de privilegios no autorizada.
- Se retira el privilegio al usuario una vez que termine sus funciones en la empresa y esto deberá ser total.
- Para dar más privilegios al usuario debe ser reportado de manera formal por el jefe inmediato de este usuario, así mismo si se le debe dar menos acceso al sistema a la cual ingresan.

Con respecto al acceso a sistemas y aplicaciones:

- Cada privilegio debe estar bien definido los permisos que tienen y aquellos que no cuentan con permisos no deben ser accedidos por los usuarios con esos privilegios.
- Todo usuario debe autenticarse antes de ingresar el sistema, este medio por el cual se autentican deberá enviar la información ingresada por el usuario de manera encriptada hacia el servidor.
- Las contraseñas deben tener una longitud mínima de 6 caracteres.
- La contraseña debe tener mayúsculas, minúsculas, números y mínimo un carácter especial.
- La contraseña tendrá un periodo de validez de 3 meses.
- El código fuente no puede ser accedido por personal que no tenga como privilegio de desarrollador.
- Registrar el ingreso del usuario al código.
- El acceso al código fuente debe ser previamente consultado con el jefe inmediato.
- Si el jefe de sistema es quien ingresa el código fuente este no deberá realizar ningún cambio.

**Políticas para la gestión de activos**

- El inventario de activos del proceso de mensajería masiva de la Tabla 6, debe estar disponible y será revisado anualmente y actualizado para los eventos de compra de nuevo hardware, de

actualizaciones de software y la infraestructura tecnológica, y de cambios del proceso en cuestión.

- El acceso al inventario será restringido únicamente para el departamento de ventas en Quito, el departamento de sistemas en Guayaquil y la Gerencia General.
- El documento para el inventario de activos, tendrá una sección en donde se indique el historial de personas responsables de la seguridad del mismo, así como la persona encargada actualmente.
- Si el activo no tiene una persona asignada, dado que es nuevo o ha sido dado de baja, se le asignará al jefe del departamento de sistemas como responsable si el activo se encuentra en Guayaquil o en la nube, y se le asignará al jefe del departamento financiero si el activo se encuentra en Quito.
- El documento para el inventario de activos, tendrá un detalle indicando la ubicación física del mismo, con historial de traslado entre Guayaquil, Quito u otra ciudad.
- La información en custodio, sea esta física o lógica que la empresa proporcione o reciba del responsable a cargo, deberá ser utilizada únicamente para fines del negocio de la organización y de su integridad se hará responsable la persona designada, siendo supervisado cualquier cambio por el inmediato superior.

- El responsable a cargo de la administración de aplicativos o servicios tecnológicos de la empresa, deberá garantizar disponibilidad para brindar asistencia siempre que se necesite y únicamente para los clientes (internos o externos) autorizados a su acceso.
- Los activos de hardware que son elementos de la infraestructura, participarán de mantenimientos frecuentes por parte del responsable, así como la verificación del uso conforme con el plan de negocio por parte del inmediato superior.

**Políticas para la seguridad de las operaciones**

Con respecto a la gestión de cambios:

- La petición de cambio debe ser dada de manera formal y aprobada por la alta gerencia.
- Registrar la petición de cambio.
- Realizar las pruebas necesarias en un ambiente seguro sin que afecte el proceso de operación.
- Se debe planificar para la implantación del cambio en el proceso de operación.
- Se debe contar con un respaldo de la información antes de realizar dicho cambio.
- Revisar el cambio realizado y documentar los resultados.

Con respecto a la separación de ambientes de desarrollo, pruebas y operación:

- Debe existir el entorno de producción, entorno de pruebas y el entorno de desarrollo, estos tres entornos deben ser completamente independientes, esto es, un entorno no debe verse afectado por problemas de otro entorno.
- Cada entorno mencionado anteriormente debe estar en una red distinta.
- Se debe contar con perfiles de acceso distintos para acceder de un entorno a otro.
- Se debe contar con un responsable que garantice que la ejecución de un entorno no interrumpa las operaciones de otros sistemas o redes.

Con respecto a los códigos maliciosos:

- Todos los sistemas operativos deberán contar con un antivirus actualizado.
- Todos los sistemas operativos deberán contar con un software de recuperación de archivos en caso de que alguno sea eliminado por un virus.

Con respecto al respaldo de la información y registro de eventos:

- Toda información que fue clasificada con valor alto y criticidad alta deberá tener su respaldo.

- Los respaldos de la información deben ser diarias.
- Todos los respaldos deben ser probados y verificados.
- Registrar cada acceso al sistema.
- Registrar las acciones de los usuarios.
- Registrar fallas reportadas.
- Los registros se deben almacenar en una base de datos distinta a la base de operación, esto es en la base de datos especializada para logs.
- Los registros almacenados como archivos no deben ser modificados y deben tener código de seguridad para poder leerlos.
- Los registros deben tener copias para evitar la pérdida de vital de información.
- Garantizar que el sistema donde se encuentran alojados todos los registros cuenten con la capacidad necesaria para almacenar gran cantidad de información.
- Registrar el acceso del administrador y las acciones del mismo.

Con respecto a la instalación de software:

- Los usuarios comunes no deben tener la autorización para instalar, actualizar o modificar software en el sistema operativo.
- Toda instalación de software debe tener su debida autorización y el registro del día/hora y usuario en la que se llevó acabo.

- Se debe probar en un ambiente seguro la instalación del nuevo software para evitar infiltración de algún virus que tenga oculto dicho software.
- Todo mantenimiento, control o actualización de los sistemas de información se debe notificar con una antelación de 24 horas y este deberá se fuera las horas laborables.

**Política para adquisición, desarrollo y mantenimiento de sistemas**

- Se debe proporcionar un ambiente de desarrollo completamente independiente al ambiente de producción.
- Las actualizaciones que se suban en este ambiente deberá ser probada y aprobada por el usuario final.
- Cada reporte que el usuario realiza sobre el sistema deberá ser de manera formal hacia el jefe de sistemas.
- Una vez aprobada por el cliente, la nueva actualización deberá someterse a pruebas de seguridad.

Con respecto al control de cambios de sistemas:

- Los cambios se deben iniciar con una solicitud formal y este debe estar registrada en el sistema de registros.
- Se debe detallar y guardar el tipo de cambio que se va a realizar ya que ese cambio puede afectar a otros procesos.

- Registrar la fecha en que se realizará el cambio, la persona encargada de realizar el cambio, que activo y que procesos afectará ese cambio.
- Para realizar algún cambio en la plataforma de producción es necesario que sea autorizado por la gerencia de manera formal y esto debe quedar registrado.
- Revisar que las aplicaciones que afecten al sistema de mensajería masiva funcionen correctamente, esto es realizando pruebas automáticas a estas aplicaciones una vez se haya hecho algún cambio en la plataforma.
- Se debe registrar todo cambio que se realice en la plataforma.
- No se debe realizar actualizaciones sin realizar una previa investigación sobre la actualización disponible, esta actualización puede afectar el perfecto funcionamiento del resto del sistema.
- El departamento de sistemas debe estar a cargo de esta investigación sobre la actualización disponible.
- El usuario común no debe tener permisos para actualizar o realizar un cambio a los paquetes de software.

Con respecto a la construcción de sistemas seguros:

- Todo sistema de software que se encuentre en uso debe tener una documentación técnica y una documentación general sobre el uso, procesos y construcción del mismo.

- Todo sistema de software que este en desarrollo debe tener una documentación técnica y una documentación general sobre el uso, procesos y construcción del mismo.
- El ambiente de desarrollo seguro debe ser accedido solamente por el personal de sistemas, esto es desarrolladores y el jefe de sistemas.
- Verificar la propiedad de código.
- Verificar que se cuente con un sistema con licencia válida.
- Para la realización de pruebas de seguridad se debe informar a la alta gerencia y ser aprobado por ellos, dicha prueba no deberá ser en horarios laborables.
- Realizar pruebas de explotación de vulnerabilidades y escalamiento de privilegios.

**Política para la gestión de incidentes de seguridad de la información**

- Reportar el evento de manera inmediata por medio de correo electrónico cuyo asunto deberá comenzar con URG. <evento>
- Realizar reportes sobre las fallas de seguridad que se tuvieron en las pruebas realizadas.
- Todos los empleados que usen el sistema deben observar y reportar si existe algún fallo en el sistema, esto se hará por medio

de un correo cuyo asunto deberá comenzar con VULN. <vulnerabilidad o debilidad>

- Todos los eventos surgidos serán evaluados una vez al día y se debe clasificar por criticidad, considerando el daño que provoca el evento al proceso de mensajería masiva.
- Se debe documentar el procedimiento que se realizó para solucionar o mitigar el incidente.
- Todo incidente previamente materializado debe ser solucionado siguiendo el procedimiento documentado.
- Todo incidente reportado y mitigado debe estar documentado.

Con respecto a la recolección de evidencia:

- Los LOGS generados por el sistema deben ser almacenados en una base de datos dedicados para LOGS.
- Los LOGS no deben ser eliminados al menos que tengan un año de antigüedad.
- Todo correo cuyo asunto comience con URG. o VULN. Debe ser almacenado en una carpeta específica para guardar este tipo de incidentes.

**Política para la gestión de continuidad de negocio**

- Se debe llevar a cabo cada mes y un horario que sea fuera de horas laborables, si esto no es posible, se debe comunicar al

cliente sobre el posible corte de servicio, la fecha y hora, el tiempo de inactividad del servicio y si está de acuerdo.

Con respecto a la implementación de la continuidad de la seguridad de la información:

- Crear un comité de seguridad que vele por el cumplimiento y continuidad de los procesos.
- Documentar el plan y periodicidad de simulacros.
- Registrar los resultados de los simulacros establecidos.
- Crear un procedimiento que reúna todo lo relacionado a la seguridad aplicada al sistema de gestión de seguridad de la información.
- Se debe realizar la verificación, revisión y evaluación del plan de continuidad al menos una vez al mes.
- Se debe tener un registro de evidencias de las pruebas reales y sus resultados.
- Si en las pruebas realizadas se detecta alguna deficiencia se debe remediar inmediatamente y se debe volver a probar varias veces para asegurar que la solución es eficaz.
- Realización de diseños de infraestructura que tengan redundancias a nivel de almacenamiento.
- Realización de respaldos de la información.

**Políticas para el cumplimiento legal**

- Documentar los hallazgos de auditoria y los procedimientos para solventarlos.
- Verificar que las implementaciones de controles estén alineadas con los riesgos a activos de la información.
- Revisar y analizar que las políticas implementadas sigan las normas de seguridad aceptadas a nivel global.
- La revisión de los cumplimientos de las políticas de seguridad deberá ser de manera periódica cada 2 meses.

### 6.1.2 POLITICAS DE SEGURIDAD EN PROCESO DE IMPLEMENTACION EN EL SERVICIO DE MENSAJERIA MASIVA

Las siguientes políticas fueron consideradas para una segunda etapa debido al tiempo que toma implementar dichas políticas ya que interviene el presupuesto y la importación de equipos.

**Políticas para la seguridad física y del entorno**

- Se debe contar con un sistema electrónico con reconocedor de huellas para el acceso al cuarto donde se encuentren la información o activos con una criticidad alta.
- Los servidores y los routers deben estar ubicados en un cuarto con una refrigeración adecuada, esto es alrededor de 12°C.
- El acceso a este cuarto deberá ser controlado con un sistema electrónico reconocedor de huellas.

- En la parte de externa del cuarto, cerca de la puerta deberá estar un extintor de fuego.
- Las computadoras y laptops deberán ser revisadas y actualizadas una vez al mes por el personal de sistemas, se deberá actualizar sistemas antivirus, actualizar parches del sistema operativo, eliminar registros o archivos que sean innecesarios para la labor que realiza el usuario, se debe realizar la limpieza adecuada si este lo amerita.
- Los equipos de servidores y routers se debe dar mantenimiento una vez al mes, se debe revisar conexiones, temperatura del CPU y si la temperatura en el cuarto es la adecuada, se debe realizar la limpieza adecuada si este lo amerita.
- Los mantenimientos de computadores y laptops se deben planificar con 24 horas de antelación y deberá ser fuera de horarios laborales. La fecha definida no debe ser la misma al mantenimiento de routers y servidores
- Los mantenimientos de servidores y routers se deben planificar con 24 horas de antelación y deberá ser un fin de semana fuera de horas laborables. La fecha definida no debe ser el mismo que el mantenimiento de computadores y laptops.
- Se debe dar de baja en el inventario aquellos activos que se consideren obsoletos para continuar en el proceso de mensajería masivo y que no pueda ser usado en algún otro proceso.

**Política de seguridad de las comunicaciones**

- Los dispositivos de red deben autenticarse para poder conectarse a la red.
- Se debe contar con filtrado de direcciones MAC para evitar conexiones no deseadas.
- Se debe contar con un cortafuego ubicado entre el acceso a internet y la red local.
- Se deben cerrar los puertos que no sean usados por alguna aplicación dentro de la empresa.
- Se debe contar con corta fuegos, con sistemas de detección de intrusos y con una zona desmilitarizada.
- Se debe segmentar la red inalámbrica con la red física.
- Se debe tener 5 VLANs: uno para los servidores de producción, uno para desarrollo, otro para pruebas y otro para los demás usuarios dentro de la organización y el ultimo para separar la red física con la red inalámbrica.
- Monitorear la segmentación de las redes.

Con respecto a la confidencialidad:

- Se debe firmar un contrato empleador-empleado indicando que este no va a divulgar sobre el trabajo que realiza y sobre el proceso de mensajería masiva.

### 6.1.3 IMPACTO ESPERADO CON LA IMPLEMENTACIÓN DE LAS POLÍTICAS

Con la implementación de las políticas descritas en el apartado anterior, se volvió a realizar un análisis de brecha para conocer el cumplimiento que tendrá la empresa de mensajería simples (SMS).

**Tabla 21: Impacto esperado**

| No. Dominio | Dominio de la Norma | % de cumplimiento actual | % de cumplimiento esperado |
|---|---|---|---|
| 5 | Políticas de seguridad de la información | 0% | 100% |
| 6 | Organización de la seguridad de la información | 6% | 18.6% |
| 7 | Seguridad de los recursos humanos | 43.33% | 43.33% |
| 8 | Gestión de activos | 21% | 60% |
| 9 | Control de acceso | 23% | 85.7% |
| 10 | Criptografía | 0% | 0% |
| 11 | Seguridad física y del entorno | 68% | 73.33% |
| 12 | Seguridad de las operaciones | 42.8% | 78.6% |
| 13 | Seguridad de las comunicaciones | 42.8% | 57.1% |
| 14 | Adquisición, desarrollo y mantenimiento de sistema | 26.9% | 61.5% |
| 15 | Relaciones con los proveedores | 0% | 0% |
| 16 | Gestión de incidentes de la seguridad de la información | 31.4% | 100% |
| 17 | Aspectos de la seguridad de la información de la gestión de la | 0% | 100% |

| No. Dominio | Dominio de la Norma | % de cumplimiento actual | % de cumplimiento esperado |
|---|---|---|---|
| | continuidad de la información | | |
| 18 | Cumplimiento | 75% | 100% |
| **Porcentaje total de cumplimiento** | | **27.15%** | **62.7%** |

**Fuente**: Los autores

En la siguiente figura se muestra el gráfico radial del análisis de brecha previamente realizada junto con el análisis de brecha después de implementar los controles.

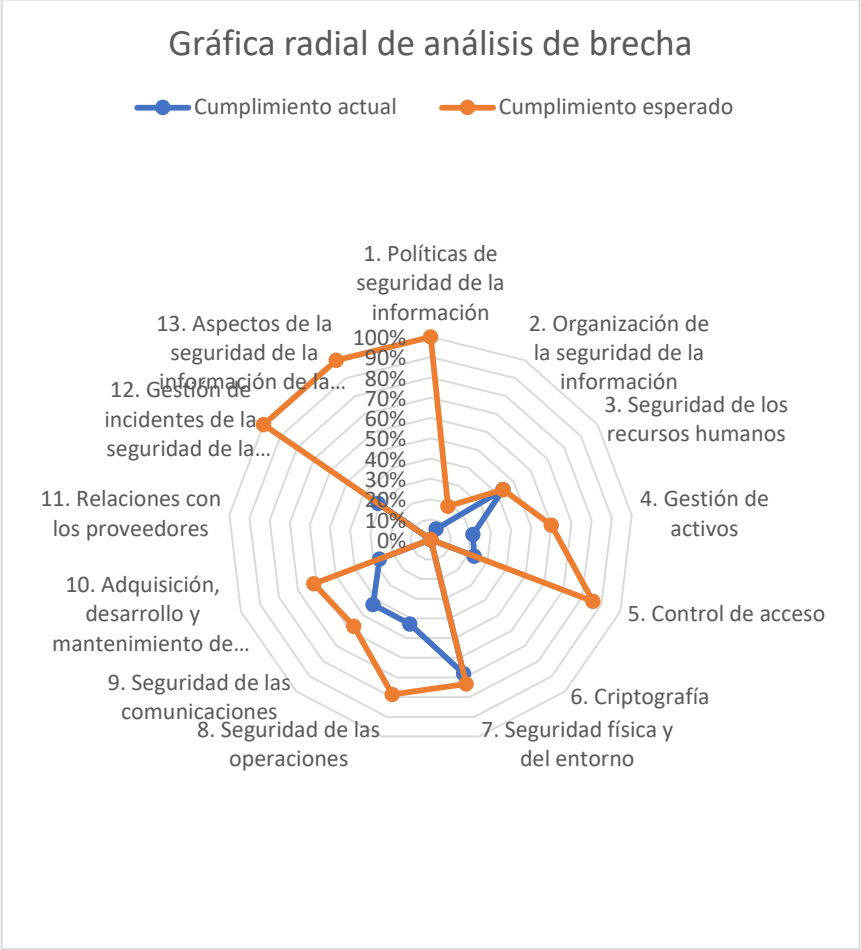



**Figura 6.1: Gráfica radial de análisis de brecha**

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

1. Se logró identificar las debilidades y las amenazas que están expuestos los inventarios que intervienen en el proceso de mensajería masiva, mediante un análisis de riesgo que permitió controlar y mitigar dichas amenazas de forma efectiva siguiendo lo establecido por la norma ISO 27001:2013.

2. Las políticas de control de acceso no poseen documentación al respecto, sin embargo, las implementaciones de ellas se agilitan dado que existen procedimientos que manejan los usuarios y sus permisos según su rol. El mismo caso ocurre con el respaldo de información, pues pese a que existen respaldos, éstos no se les realizan verificaciones de integridad de datos. La empresa no posee ni procedimientos ni políticas sobre planes de continuidad de negocio ante caída de servicios por situaciones adversas, por lo que se tuvo que empezar desde cero con este control.

3. La implementación de un esquema de seguridad es de vital importancia para la continuidad y el buen desempeño de una compañía, al no tener políticas o

controles implementados, el servicio brindado por la organización se verá comprometida dando como resultado problemas con los clientes. Se implementa el esquema por medio de las políticas de seguridad de la información definidas en el presente proyecto, y la ejecución de las mismas siguiendo el plan de aplicación de controles.

4. Toda política de seguridad debe ser revisada de forma periódica y debe ser auditado ya sea por auditores internos o externos para asegurar que estas se cumplan debidamente.

## Recomendaciones

**1.** Se debe implementar un esquema de seguridad para los otros procesos y darles mayor prioridad aquellos procesos que dependen del proceso de mensajería masiva o aquellos procesos por la cual el servicio de mensajería masiva dependa.

2. Toda política de seguridad debe ser revisada de forma periódica y debe ser auditado ya sea por auditores internos o externos para asegurar que estas se cumplan debidamente.

3. Revisar y auditar las políticas y controles implementados en el proceso de mensajería masiva, con el fin de garantizar el cumplimiento del mismo por parte de los empleados.

# BIBLIOGRAFÍA

[1] ISO2700.ES, Sistema de gestión de la seguridad de la información, http://www.iso27000.es/download/doc_sgsi_all.pdf, fecha de consulta mayo 2018.

[2] ISO.ORG, Tecnologías de la información, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, fecha de consulta mayo 2018.

[3] ISOTOOLS.ORG, Sistema de gestión de riesgos y seguridad, https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/, fecha de consulta mayo 2018.

[4] INCIBE.ES, Análisis de riesgos, https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo, fecha de consulta Agosto 2018.

[5] CCN-CERT.CNI.ES, Metodología de implementación de un esquema de seguridad, https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar/metodologia.html, fecha de consulta Agosto 2018.

[6] AUDITOOL.ORG, Riesgo inherente y riesgo residual, https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual, fecha de consulta Agosto 2018.

[7] WELIVESECURITY.COM, Metodología Magerit v3, https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/, fecha de consulta Agosto 2018

[8] ISOTOOLS.ORG, https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/, fecha de consulta mayo 2018.

[9] CRIPTORED.UPM.ES, Los controles, http://www.criptored.upm.es/guiateoria/gt_m292h.htm, fecha de consulta mayo 2018.

# ANEXOS

## ANEXO A: Glosario de términos

| Término | Significado |
|---|---|
| Hosting | Alojamiento de un servicio web por la cual todo el mundo lo pueda ver. |
| Social CRM | Sistema de relaciones de clientes basados en redes sociales. |
| Analista de inteligencia | Aquel que toma decisiones estratégicas mediante el análisis y el procesamiento de datos relevantes para el negocio. |
| Administrador de contenido | Encargado de crear, borrar, actualizar contenido en las aplicaciones de redes sociales, como Facebook, Instagram, etc. o la página web de la organización. |
| Plataforma Kannel | Es una pasarela de SMS, permite la conectividad de otras aplicaciones mediante su API. |
| Servicio HiVelocity | Proveedor de hosting y de servidores dedicados. |

| | |
|---|---|
| Virtualización | Emular un sistema operativo o un servidor bajo una plataforma anfitrión. |
| Splunk | Sistema que proporciona datos estadísticos de rendimiento y poder administrarlos. |
| MySQL | Servidor de bases de datos ligero. |
| REST | Transferencia de estado representacional. Usa el protocolo HTTP para la obtención de datos. |
| SOAP | Protocolo simple de acceso a objetos. Permite la comunicación por medio de intercambio de datos XML. |
| Análisis de brecha | Análisis que se realiza en la organización para conocer el nivel actual de cumplimiento con respecto a las normas. |
| Declaración de aplicabilidad | Documento donde se define que controles aplican para el proceso analizado. |

**ANEXO B: Matriz de Análisis de Brecha**

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A5 | POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN | | | |
| A5.1 | Orientación de la dirección para la gestión de la seguridad de la información | | | |
| A5.1.1 | Políticas para la seguridad de la información | Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. | 0,00 % | No tienen definido una política para la seguridad de la información |
| A5.1.2 | Revisión de las políticas para la seguridad de la información. | Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas. | 0,00 % | No tienen definido una política para la seguridad de la información |
| A6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION | | | |
| A6.1 | Organización interna | | | |
| A6.1.1 | Roles y responsabilidades para la seguridad de la información | Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información. | 10,00 % | En cada área hay información importante la cual debe haber una persona encargada para la planificación de la seguridad, sin embargo no existe una control establecida |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A6.1.2 | Separación de deberes | Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización | 20,00 % | El personal de la empresa conoce los deberes por la están a cargos, sin embargo no existe un control definido |
| A6.1.3 | Contacto con las autoridades | Control: Se deben mantener contactos apropiados con las autoridades pertinentes. | 0,00 % | No poseen un control, ni una manera establecida para contactar con las autoridades pertinentes |
| A6.1.4 | Contacto con grupos de interés especial | Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad | 0,00 % | No poseen un control, ni una manera establecida para contactar con los grupos de interés |
| A6.1.5 | Seguridad de la información en la gestión de proyectos. | Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | 0,00 % | No poseen un control |
| A6.2 | Dispositivos móviles y teletrabajo | | | |
| Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles | | | | |
| A6.2.1 | Política para dispositivos móviles | Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | 0,00 % | No existe política definida para el uso de dispositivos móviles |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A6.2.2 | Teletrabajo | Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | 10,00 % | Existe un procedimiento para realizar trabajo remoto, sin embargo no hay un control sobre esto |
| A7 | SEGURIDAD DE LOS RECURSOS HUMANOS | | | |
| A7.1 | Antes de asumir el empleo | | | |
| A7.1.1 | Selección | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos. | 100,00 % | Poseen un control definido para la selección del personal |
| A7.1.2 | Términos y condiciones del empleo | Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | 100,00 % | Poseen un control definido para los términos y condiciones de empleo |
| A7.2 | Durante la ejecución del empleo | | | |
| Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. | | | | |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A7.2.1 | Responsabilidades de la dirección | Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | 0,00 % | No se exige a los empleados sobre la aplicación de la seguridad de la información |
| A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | 10,00 % | Los empleados de la organización no reciben la debida educación sobre las políticas o reglas establecidas en la empresa |
| A7.2.3 | Proceso disciplinario | Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | 50,00 % | Existe un control implementado en el 2014 sobre el proceso disciplinario pero esto se ha revisado nuevamente |
| A7.3 | Terminación y cambio de empleo | | | |
| Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo | | | | |
| A7.3.1 | Terminación o cambio de responsabilidades de empleo | Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio | 0,00 % | No es de importancia para la empresa |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | | |
| A8 | GESTION DE ACTIVOS | | | |
| A8.1 | Responsabilidad por los activos | | | |
| A8.1.1 | Inventario de activos | Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | 60,00 % | Existe un control sobre los inventarios de activos la cual se debe revisar nuevamente debido a que fue implementado en el 2014 |
| A8.1.2 | Propiedad de los activos | Control: Los activos mantenidos en el inventario deben tener un propietario. | 50,00 % | Los activos tienen propietario, sin embargo no existe una política que defina esto |
| A8.1.3 | Uso aceptable de los activos | Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | 0,00 % | No existe documentación sobre el uso aceptable que se le debe dar a los activos |
| A8.1.4 | Devolución de activos | Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. | 0,00 % | No es de interés para la empresa |
| A8.2 | Clasificación de la información | | | |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. | | | | |
| A8.2.1 | Clasificación de la información | Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | 0,00 % | No existe clasificación de la información |
| A8.2.2 | Etiquetado de la información | Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. | 0,00 % | No es de interés para la empresa |
| A8.2.3 | Manejo de activos | Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. | 0,00 % | No existe un control sobre el manejo de activos |
| A8.3 | Manejo de medios | | | |
| Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios | | | | |
| A8.3.1 | Gestión de medio removibles | Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | 50,00 % | Se realiza un procedimiento definido, pero esto no está establecido en un documento o en un control |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A8.3.2 | Disposición de los medios | Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | 0,00 % | No es de importancia para la empresa |
| A8.3.3 | Transferencia de medios físicos | Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | 50,00 % | Se realiza un procedimiento definido, pero esto no está establecido en un documento o en un control |
| A9 | CONTROL DE ACCESO | | | |
| A9.1 | Requisitos del negocio para el control de acceso | | | |
| A9.1.1 | Política de control de acceso | Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información. | 50,00 % | Se realiza un procedimiento definido, pero esto no está establecido en un documento o en un control |
| A9.1.2 | Acceso a redes y a servicios en red | Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. | 50,00 % | Se realiza un procedimiento definido, pero esto no está establecido en un documento o en un control |
| A9.2 | Gestión de acceso de usuarios | | | |
| Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. | | | | |
| A9.2.1 | Registro y cancelación del registro de usuarios | Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | 10,00 % | A pesar de que si se lo realiza, no existe un proceso formal para el registro y cancelación del mismo |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A9.2.2 | Suministro de acceso de usuarios | Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | 10,00 % | A pesar de que si se lo realiza, no existe un proceso formal para el suministro de acceso |
| A9.2.3 | Gestión de derechos de acceso privilegiado | Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | 10,00 % | No existe un proceso formal para el registro y cancelación del mismo |
| A9.2.4 | Gestión de información de autenticación secreta de usuarios | Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. | 0,00 % | No existe control sobre esto |
| A9.2.5 | Revisión de los derechos de acceso de usuarios | Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | 0,00 % | No se realiza la revisión |
| A9.2.6 | Retiro o ajuste de los derechos de acceso | Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | 10,00 % | Se realiza el retiro de privilegios pero no existe un proceso definido |
| A9.3 | Responsabilidades de los usuarios | | | |
| Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación. | | | | |
| A9.3.1 | Uso de información de autenticación secreta | Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de | 0,00 % | No se exige a los empleados |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | información de autenticación secreta. | | |
| A9.4 | Control de acceso a sistemas y aplicaciones | | | |
| Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones. | | | | |
| A9.4.1 | Restricción de acceso a la información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | 20,00 % | Se restringe el acceso a personal no autorizado, pero no existe un control de acceso en la que basarse |
| A9.4.2 | Procedimiento de ingreso seguro | Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. | 0,00 % | No existe control de ingreso seguro |
| A9.4.3 | Sistema de gestión de contraseñas | Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. | 0,00 % | No son interactivos |
| A9.4.4 | Uso de programas utilitarios privilegiados | Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | 60,00 % | Existe restricción de navegación a algunas páginas, en todo caso se debe revisar e implementar una política de acceso |
| A9.4.5 | Control de acceso a códigos fuente de programas | Control: Se debe restringir el acceso a los códigos fuente de los programas. | 100,00 % | Solo los desarrolladores tienen acceso al código fuente |
| A10 | CRIPTOGRAFIA | | | |
| A10.1 | Controles criptográficos | | | |
| A10.1.1 | Política sobre el uso de controles criptográficos | Control: Se debe desarrollar e implementar una | 0,00 % | No es de importancia para la empresa |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | política sobre el uso de controles criptográficos para la protección de la información. | | |
| A10.1.2 | Gestión de llaves | Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida. | 0,00 % | No es de importancia para la empresa |
| A11 | SEGURIDAD FISICA Y DEL ENTORNO | | | |
| A11.1 | Áreas seguras | | | |
| A11.1.1 | Perímetro de seguridad física | Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. | 100,00 % | Cuenta con áreas seguras definidas |
| A11.1.2 | Controles de acceso físicos | Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado. | 100,00 % | Las áreas están aseguradas contra acceso no autorizado |
| A11.1.3 | Seguridad de oficinas, recintos e instalaciones. | Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.. | 100,00 % | Cuentan con un diseño de seguridad en las oficinas |
| A11.1.4 | Protección contra amenazas externas y ambientales. | Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | 100,00 % | Poseen extintores y llaves de agua contra incendios |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A11.1.5 | Trabajo en áreas seguras. | Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. | 100,00 % | Si cuentan con ese diseño |
| A11.1.6 | Áreas de carga, despacho y acceso público | Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | 100,00 % | Si se controla el acceso de persona no autorizadas |
| A11.2 | Equipos | | | |
| A11.2.1 | Ubicación y protección de los equipos | Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | 100,00 % | Los servidores se encuentran en un lugar adecuado para esto |
| A11.2.2 | Servicios de suministro | Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | 100,00 % | Si cuentan contra protección a fallas |
| A11.2.3 | Seguridad en el cableado. | Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño. | 0,00 % | No es de importancia para la empresa |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño. | | |
| A11.2.4 | Mantenimiento de los equipos. | Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | 20,00 % | Se realiza mantenimiento parcial, es decir se hace mantenimiento solamente en los servidores |
| A11.2.5 | Retiro de activos | Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa | 100,00 % | Si está definido |
| A11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | 0,00 % | No es de importancia para la empresa |
| A11.2.7 | Disposición segura o reutilización de equipos | Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso. | 100,00 % | Se realiza la verificación |
| A11.2.8 | Equipos de usuario desatendido | Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. | 0,00 % | No se realiza la revisión |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | limpia en las instalaciones de procesamiento de información. | | |
| A12 | SEGURIDAD DE LAS OPERACIONES | | | |
| A12.1 | Procedimientos operacionales y responsabilidades | | | |
| A12.1.1 | Procedimientos de operación documentados | Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan. | 0,00 % | No es de importancia para la empresa |
| A12.1.2 | Gestión de cambios | Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. | 100,00 % | Se realiza el control sobre cambios en la organización y se tiene documentado dicho cambio |
| A12.1.3 | Gestión de capacidad | Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | 0,00 % | No se realiza el seguimiento al uso de recursos |
| A12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | 100,00 % | Si existe ambiente de desarrollo y producción |
| A12.2 | Protección contra códigos maliciosos | | | |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A12.2.1 | Controles contra códigos maliciosos | Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | 20,00 % | Se realiza cierto control de código malicioso en los servidores, mientras que en los equipos del personal no, No existe un control definido |
| A12.3 | Copias de respaldo | | | |
| A12.3.1 | Respaldo de la información | Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | 50,00 % | Se hacen respaldo de la información, sin embargo estos no son probados |
| A12.4 | Registro y seguimiento | | | |
| A12.4.1 | Registro de eventos | Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | 0,00 % | No se registran los eventos de errores |
| A12.4.2 | Protección de la información de registro | Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. | 100,00 % | Si cuentan con esto |
| A12.4.3 | Registros del administrador y del operador | Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. | 30,00 % | Existe un registro de acceso pero de los clientes |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A12.4.4 | Sincronización de relojes | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. | 0,00 % | No tienen implementado este diseño |
| A12.5 | Control de software operacional | | | |
| A12.5.1 | Instalación de software en sistemas operativos | Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | 100,00 % | La instalación de software está restringido |
| A12.6 | Gestión de la vulnerabilidad técnica | | | |
| A12.6.1 | Gestión de las vulnerabilidades técnicas | Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | 0,00 % | No se realiza una evaluación de las vulnerabilidades |
| A12.6.2 | Restricciones sobre la instalación de software | Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. | 100,00 % | La instalación de software está restringido |
| A12.7 | Consideraciones sobre auditorías de sistemas de información | | | |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A12.7.1 | Controles de auditorías de sistemas de información | Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | 0,00 % | No se planifica la auditoria |
| A13 | SEGURIDAD DE LAS COMUNICACIONES | | | |
| A13.1 | Gestión de la seguridad de las redes | | | |
| A13.1.1 | Controles de redes | Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. | 100,00 % | Si cuentan con ese diseño |
| A13.1.2 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. | 0,00 % | No se cuenta con mecanismos de seguridad en la red de la organización |
| A13.1.3 | Separación en las redes | Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | 100,00 % | Si cuentan con ese diseño |
| A13.2 | Transferencia de información | | | |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A13.2.1 | Políticas y procedimientos de transferencia de información | Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | 0,00 % | No es de importancia para la empresa |
| A13.2.2 | Acuerdos sobre transferencia de información | Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas. | 0,00 % | No es de importancia para la empresa |
| A13.2.3 | Mensajería Electrónica | Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica. | 0,00 % | No es de importancia para la empresa |
| A13.2.4 | Acuerdos de confidencialidad o de no divulgación | Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | 100,00 % | Si está implementado |
| A14 | Adquisición, desarrollo y mantenimiento de sistemas | | | |
| A14.1 | Requisitos de seguridad de los sistemas de información | | | |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | Control: Los requisitos relacionados con seguridad de la información se deben incluir en los | 0,00 % | No se tiene como requisito |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. | | |
| A.14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas | Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. | 0,00 % | No cuentan con la protección sobre fraudes o disputas |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones. | Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. | 0,00 % | No tienen implementado este control |
| A14.2 | Seguridad en los procesos de Desarrollo y de Soporte | | | |
| A.14.2.1 | Política de desarrollo seguro | Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización. | 0,00 % | No cuentan con una política |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A.14.2.2 | Procedimientos de control de cambios en sistemas | Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | 50,00 % | No cuentan con una política definida, sin embargo usan control de cambios en la parte de software |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. | 0,00 % | No se realiza dicha revisión |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software | Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | 0,00 % | No es de importancia para la empresa |
| A.14.2.5 | Principio de Construcción de los Sistemas Seguros. | Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | 0,00 % | No cuentan con un documento para desarrollo de sistema seguro |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | sistemas de información. | | |
| A.14.2.6 | Ambiente de desarrollo seguro | Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | 100,00 % | Se tiene un ambiente de pruebas |
| A.14.2.7 | Desarrollo contratado externamente | Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. | 0,00 % | No es de importancia para la empresa |
| A.14.2.8 | Pruebas de seguridad de sistemas | Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad. | 100,00 % | Se realizan las pruebas respectivas antes de lanzarlo a producción |
| A.14.2.9 | Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados. | 100,00 % | Si se establece un programas de pruebas y esto son revisados por la gerencia |
| A14.3 | Datos de prueba | | | |
| A.14.3.1 | Protección de datos de prueba | Control: Los datos de prueba se deben seleccionar, proteger | 0,00 % | No es de importancia para la empresa |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar. | 0,00 % | No cuentan con política |
| A15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | 0,00 % | No realiza este procedimiento para la elección del proveedor |
| A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | 0,00 % | No es de importancia para la empresa |
| A15.2 | Gestión de la prestación de servicios de proveedores | | | |
| A15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | 0,00 % | No es de importancia para la empresa |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A15.2.2 | Gestión del cambio en los servicios de los proveedores | Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos. | 0,00 % | No es de importancia para la empresa |
| A16 | GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | | | |
| A16.1 | Gestión de incidentes y mejoras en la seguridad de la información | | | |
| A16.1.1 | Responsabilidades y procedimientos | Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | 100,00 % | Si cuentan con responsabilidades establecidas para responder a los problemas ocasionados |
| A16.1.2 | Reporte de eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | 0,00 % | No existe reporte de eventos de seguridad |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A16.1.3 | Reporte de debilidades de seguridad de la información | Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | 20,00 % | Se reporta de manera verbal, no hay procedimiento adecuado para esto |
| A16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | 0,00 % | No se evalúan los eventos de seguridad |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | 0,00 % | La respuesta al problema no sigue un procedimiento documentado |
| A16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros. | 100,00 % | Si cuentan con esto |
| A16.1.7 | Recolección de evidencia | Control: La organización debe definir y aplicar procedimientos para la identificación, y preservación de información que pueda servir como evidencia. | 0,00 % | No cuentan con procedimientos definidos |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO | | | |
| A17.1 | Continuidad de Seguridad de la información | | | |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. | 0,00 % | No se ha considerado esto |
| A17.1.2 | Implementación de la continuidad de la seguridad de la información | Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. | 0,00 % | No se ha considerado esto |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. | 0,00 % | No se ha considerado esto |
| A17.2 | Redundancias | | | |
| A17.2.1 | Disponibilidad de instalaciones de procesamiento de información | Control: Las instalaciones de procesamientos de información se deben | 0,00 % | No cuentan con redundancia en los servidores |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | | |
| A18 | CUMPLIMIENTO | | | |
| A18.1 | Cumplimiento de requisitos legales y contractuales | | | |
| A18.1.1 | Identificación de la legislación aplicable. | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. | 100,00 % | Si cuentan con la documentación adecuada con respecto a aspectos legales |
| A18.1.2 | Derechos propiedad intelectual (DPI) | Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. | 0,00 % | No cuentan con procedimientos definidos |
| A18.1.3 | Protección de registros | Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los | 100,00 % | Si están protegidos contra perdida, esto está alojado en un servidor en la nube |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| | | requisitos legislativos, de reglamentación, contractuales y de negocio. | | |
| A18.1.4 | Privacidad y protección de información de datos personales | Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. | 100,00 % | Si están protegidos contra privacidad |
| A18.1.5 | Reglamentación de controles criptográficos. | Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | 0,00 % | No es de importancia para la empresa |
| A18.2 | Revisiones de seguridad de la información | | | |
| A18.2.1 | Revisión independiente de la seguridad de la información | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | 0,00 % | No se ha considerado esto |

| Sección | Descripción del dominio | Domino, objetivo de control y Controles | Cumplimiento del control | Observaciones |
|---|---|---|---|---|
| A18.2.2 | Cumplimiento con las políticas y normas de seguridad | Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. | 0,00 % | No se ha considerado esto |
| A18.2.3 | Revisión del cumplimiento técnico | Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | 0,00 % | No se ha considerado esto |

**Fuente:** Los autores

**ANEXO C: Matriz de análisis de riesgos**

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo operativo | Aplicación web para coordinación de proyectos | Software | Mantenimiento inadecuado | Probable | Menor | Alto |
| Riesgo operativo | Aplicación web para coordinación de proyectos | Software | Huecos de seguridad | Probable | Menor | Alto |
| Riesgo operativo | Aplicación web para coordinación de proyectos | Software | Acceso no autorizado | Posible | Menor | Moderado |
| Riesgo operativo | Aplicación web de reportes internos y externos | Software | Mantenimiento inadecuado | Probable | Mayor | Extremo |
| Riesgo operativo | Aplicación web de reportes internos y externos | Software | Huecos de seguridad | Probable | Mayor | Extremo |
| Riesgo operativo | Aplicación web de reportes internos y externos | Software | Acceso no autorizado | Posible | Menor | Moderado |
| Riesgo operativo | Sistema de mensajería premium | Software | Mantenimiento inadecuado | Probable | Mayor | Extremo |
| Riesgo operativo | Sistema de mensajería premium | Software | Huecos de seguridad | Probable | Mayor | Extremo |

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo operativo | Sistema de mensajería premium | Software | Acceso no autorizado | Probable | Catastrófico | Extremo |
| Riesgo natural | Impresoras térmicas | Hardware | Terremoto | Improbable | Menor | Bajo |
| Riesgo natural | Impresoras térmicas | Hardware | Inundación | Improbable | Menor | Bajo |
| Riesgo operativo | Impresoras térmicas | Hardware | Incendio | Posible | Menor | Moderado |
| Riesgo operativo | Impresoras térmicas | Hardware | Suciedad | Posible | Menor | Moderado |
|  | Impresoras térmicas | Hardware | Desgaste de partes | Posible | Menor | Moderado |
| Riesgo tecnológico | Impresoras térmicas | Hardware | Corte de suministro de luz | Posible | Menor | Moderado |
| Riesgo operativo | Impresoras térmicas | Hardware | Mantenimiento inadecuado | Probable | Menor | Moderado |
| Riesgo natural | Servidores | Hardware | Terremoto | Improbable | Catastrófico | Extremo |
| Riesgo natural | Servidores | Hardware | Inundación | Improbable | Catastrófico | Extremo |
| Riesgo operativo | Servidores | Hardware | Incendio | Posible | Catastrófico | Extremo |
| Riesgo operativo | Servidores | Hardware | Suciedad | Probable | Catastrófico | Extremo |

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo tecnológico | Servidores | Hardware | Desgaste de partes | Probable | Moderado | Alto |
| Riesgo tecnológico | Servidores | Hardware | Corte de suministro de luz | Posible | Mayor | Extremo |
| Riesgo operativo | Servidores | Hardware | Mantenimiento inadecuado | Probable | Menor | Alto |
| Riesgo operativo | Servidores | Hardware | Acceso no autorizado | Posible | Mayor | Extremo |
| Riesgo operativo | Servidores | Hardware | Denegación de servicio por error | Probable | Mayor | Extremo |
| Riesgo natural | Routers | Hardware | Terremoto | Improbable | Moderado | Moderado |
| Riesgo natural | Routers | Hardware | Inundación | Improbable | Moderado | Moderado |
| Riesgo operativo | Routers | Hardware | Incendio | Posible | Moderado | Alto |
| Riesgo operativo | Routers | Hardware | Suciedad | Probable | Moderado | Alto |
| Riesgo tecnológico | Routers | Hardware | Desgaste de partes | Probable | Moderado | Alto |
| Riesgo tecnológico | Routers | Hardware | Corte de suministro de luz | Posible | Moderado | Alto |
| Riesgo operativo | Sistema de mensajería masiva | Software | Subir código con fallas a producción | Casi seguro | Moderado | Extremo |

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo operativo | Sistema de mensajería masiva | Software | Huecos de seguridad | Casi seguro | Moderado | Extremo |
| Riesgo operativo | Sistema de mensajería masiva | Software | No tener control de versiones | Posible | Menor | Moderado |
| Riesgo operativo | Sistema de mensajería masiva | Software | Acceso no autorizado | Probable | Menor | Alto |
| Riesgo operativo | Aplicación web marketing digital | Software | Subir código con fallas a producción | Casi seguro | Moderado | Extremo |
| Riesgo operativo | Aplicación web marketing digital | Software | Huecos de seguridad | Casi seguro | Moderado | Extremo |
| Riesgo operativo | Aplicación web marketing digital | Software | No tener control de versiones | Posible | Menor | Moderado |
| Riesgo operativo | Aplicación web marketing digital | Software | Acceso no autorizado | Posible | Menor | Moderado |
| Riesgo de cumplimiento | Motor base de datos | Software | No tener respaldo de información | Posible | Moderado | Alto |
| Riesgo operativo | Motor base de datos | Software | Mantenimiento inadecuado | Improbable | Menor | Bajo |
| Riesgo de cumplimiento | Motor base de datos | Software | No tener integridad en los datos | Posible | Mayor | Extremo |
| Riesgo operativo | Motor base de datos | Software | Eliminación errónea de registros | Probable | Catastrófico | Extremo |
| Riesgo natural | Documentos físicos | Información | Inundación | Improbable | Menor | Bajo |

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo operativo | Documentos físicos | | Incendio | Improbable | Menor | Bajo |
| Riesgo operativo | Documentos físicos | Información | Suciedad | Posible | Menor | Moderado |
| Riesgo tecnologico | Documentos físicos | Información | Desgaste de hojas | Casi seguro | Menor | Alto |
| Riesgo operativo | Documentos físicos | Información | Destrucción de la información | Probable | Menor | Alto |
| Riesgo de imagen | Documentos físicos | Información | Robo | Posible | Menor | Moderado |
| Riesgo natural | Computadoras/Laptops | Hardware | Terremoto | Improbable | Moderado | Moderado |
| Riesgo natural | Computadoras/Laptops | Hardware | Inundación | Improbable | Moderado | Moderado |
| Riesgo operativo | Computadoras/Laptops | Hardware | Incendio | Posible | Menor | Moderado |
| Riesgo operativo | Computadoras/Laptops | Hardware | Suciedad | Posible | Menor | Moderado |
| Riesgo tecnologico | Computadoras/Laptops | Hardware | Desgaste de partes | Posible | Menor | Moderado |
| Riesgo tecnologico | Computadoras/Laptops | Hardware | Corte de suministro de luz | Posible | Menor | Moderado |
| Riesgo operativo | Computadoras/Laptops | Hardware | Mantenimiento inadecuado | Probable | Menor | Alto |

| Tipo de riesgo | Activo | Tipo | Amenaza | Probabilidad | Impacto | Clasificación |
|---|---|---|---|---|---|---|
| Riesgo operativo | Computadoras/Laptops | Hardware | Acceso no autorizado | Probable | Menor | Alto |
| Riesgo operativo | Sistema operativo | Software | Mantenimiento inadecuado | Probable | Moderado | Alto |
| Riesgo operativo | Sistema operativo | Software | Acceso no autorizado | Probable | Moderado | Alto |
| Riesgo tecnológico | Sistema operativo | Software | Virus | Probable | Mayor | Extremo |
| Riesgo operativo | Sistema operativo | Software | Eliminación de registros para el correcto funcionamiento del SO | Posible | Mayor | Extremo |

**Fuente:** Los autores

**ANEXO D: Declaración de Aplicabilidad sobre el proceso de Mensajería Masiva**

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| **A5** | **POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION** | | |
| **A5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** | | |
| A5.1.1 | Políticas para la seguridad de la información | SI | Tiene aplicabilidad global en todo el SGSI |
| A5.1.2 | Revisión de las políticas para la seguridad de la información. | SI | Se debe realizar la revisión de las políticas de seguridad de manera periódica |
| **A6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION** | | |
| **A6.1** | **Organización inter** | | |
| A6.1.1 | Roles y responsabilidades para la seguridad de la información | SI | Se debe tener bien definido los roles y responsables de la seguridad de la información. |
| A6.1.2 | Separación de deberes | NO | Para el proceso de mensajería masiva no es necesario separación de deberes |
| A6.1.3 | Contacto con las autoridades | NO | Para el proceso de mensajería masiva no es necesario estar a contacto con las autoridades |
| A6.1.4 | Contacto con grupos de interés especial | NO | Para el proceso de mensajería masiva no es necesario estar a contacto con grupos de interés especial |
| A6.1.5 | Seguridad de la información en la gestión de proyectos. | NO | En el proceso de mensajerías masivas no hay gestión de proyectos |

| | | | |
|---|---|---|---|
| A6.2 | Dispositivos móviles y teletrabajo | | |
| Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles | | | |
| A6.2.1 | Política para dispositivos móviles | NO | No aplica para el proceso de mensajería masiva |
| A6.2.2 | Teletrabajo | NO | No aplica para el proceso de mensajería masiva |
| **A7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | | |
| **A7.1** | **Antes de asumir el empleo** | | |
| A7.1.1 | Selección | NO | No aplica para el proceso de mensajería masiva |
| A7.1.2 | Términos y condiciones del empleo | NO | No aplica para el proceso de mensajería masiva |
| **A7.2** | **Durante la ejecución del empleo** | | |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A7.2.1 | Responsabilidades de la dirección | NO | No aplica para el proceso de mensajería masiva |
| A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | NO | No aplica para el proceso de mensajería masiva |
| A7.2.3 | Proceso disciplinario | NO | No aplica para el proceso de mensajería masiva |
| **A7.3** | **Terminación y cambio de empleo** | | |
| A7.3.1 | Terminación o cambio de responsabilidades de empleo | NO | No aplica para el proceso de mensajería masiva |
| **A8** | **GESTION DE ACTIVOS** | | |
| **A8.1** | **Responsabilidad por los activos** | | |
| A8.1.1 | Inventario de activos | SI | Es necesario conocer los activos para una adecuada evaluación de riesgos |
| A8.1.2 | Propiedad de los activos | SI | Cada activo debe tener un responsable |
| A8.1.3 | Uso aceptable de los activos | SI | Se debe contar con los procedimientos adecuados para el uso de los activos y no causar algún daño sobre el mismo |
| A8.1.4 | Devolución de activos | NO | No aplica para el proceso de mensajería masiva |
| **A8.2** | **Clasificación de la información** | | |

| | | | |
|---|---|---|---|
| A8.2.1 | Clasificación de la información | SI | Es necesario para el correcto manejo de activos |
| A8.2.2 | Etiquetado de la información | NO | No aplica para el proceso de mensajería masiva |
| A8.2.3 | Manejo de activos | SI | Se debe permitir el control de elementos portátiles de la compañía |
| **A8.3** | **Manejo de medios** | | |
| A8.3.1 | Gestión de medio removibles | NO | No aplica para el proceso de mensajería masiva |
| A8.3.2 | Disposición de los medios | NO | No aplica para el proceso de mensajería masiva |
| A8.3.3 | Transferencia de medios físicos | NO | No aplica para el proceso de mensajería masiva |
| **A9** | **CONTROL DE ACCESO** | | |
| **A9.1** | **Requisitos del negocio para el control de acceso** | | |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A9.1.1 | Política de control de acceso | SI | Se debe contar con una política de control de acceso para garantizar que accesos no deseados sean bloqueados |
| A9.1.2 | Acceso a redes y a servicios en red | SI | Los usuarios no autorizados no deben poder acceder a la red o algún servicio que ofrece la empresa |
| **A9.2** | **Gestión de acceso de usuarios** | | |
| A9.2.1 | Registro y cancelación del registro de usuarios | SI | Se necesita un procedimiento adecuado para el registro o la cancelación de usuario |
| A9.2.2 | Suministro de acceso de usuarios | SI | Cada usuario debe tener permisos definidos |
| A9.2.3 | Gestión de derechos de acceso privilegiado | SI | Se debe administrar correctamente para conocer quienes tienen derecho de acceso privilegiado |
| A9.2.4 | Gestión de información de autenticación secreta de usuarios | SI | Se debe implementar y administrar un protocolo de seguridad para la autenticación de los usuarios |
| A9.2.5 | Revisión de los derechos de acceso de usuarios | SI | Se debe revisar periódicamente los permisos de usuarios |
| A9.2.6 | Retiro o ajuste de los derechos de acceso | SI | Se debe tener un procedimiento adecuado para el retiro total o algún cambio de permiso |

| | | | |
|---|---|---|---|
| **A9.3** | **Responsabilidades de los usuarios** | | |
| A9.3.1 | Uso de información de autenticación secreta | NO | No aplica para el proceso de mensajería masiva |
| **A9.4** | **Control de acceso a sistemas y aplicaciones** | | |
| A9.4.1 | Restricción de acceso a la información | SI | No debe tener acceso a información un usuario a la cual no le compete |
| A9.4.2 | Procedimiento de ingreso seguro | SI | Se debe tener un procedimiento para el ingreso seguro a los sistemas |
| A9.4.3 | Sistema de gestión de contraseñas | SI | Es necesario tener contraseñas fuertes para que estas no sean vulnerables ante un ataque de fuerza bruta |
| A9.4.4 | Uso de programas utilitarios privilegiados | NO | No existen programas utilitarios privilegiados |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A9.4.5 | Control de acceso a códigos fuente de programas | SI | No todos deben ingresar al código fuente del sistema de mensajería masiva |
| **A10** | **CRIPTOGRAFIA** | | |
| **A10.1** | **Controles criptográficos** | | |
| A10.1.1 | Política sobre el uso de controles criptográficos | NO | Según Gerencia, no es necesario implementar controles criptográficas |
| A10.1.2 | Gestión de llaves | NO | Según Gerencia, no es necesario llevar una gestión de llaves |
| **A11** | **SEGURIDAD FISICA Y DEL ENTORNO** | | |
| **A11.1** | **Áreas seguras** | | |
| A11.1.1 | Perímetro de seguridad física | NO | No aplica para el proceso de mensajería masiva |
| A11.1.2 | Controles de acceso físicos | SI | |
| A11.1.3 | Seguridad de oficinas, recintos e instalaciones. | NO | No aplica para el proceso de mensajería masiva |
| A11.1.4 | Protección contra amenazas externas y ambientales. | NO | No aplica para el proceso de mensajería masiva |
| A11.1.5 | Trabajo en áreas seguras. | NO | No aplica para el proceso de mensajería masiva |
| A11.1.6 | Áreas de carga, despacho y acceso público | NO | No aplica para el proceso de mensajería masiva |
| **A11.2** | **Equipos** | | |

| | | | |
|---|---|---|---|
| A11.2.1 | Ubicación y protección de los equipos | SI | |
| A11.2.2 | Servicios de suministro | NO | Trabajo delegado por ur tercero |
| A11.2.3 | Seguridad en el cableado. | NO | Trabajo delegado por ur tercero |
| A11.2.4 | Mantenimiento de los equipos. | SI | Se debe dar mantenimiento periódicamente a los equipos para evitar algún daño |
| A11.2.5 | Retiro de activos | SI | Se debe tener ur procedimiento adecuado para el retiro de algún activo |
| A11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | NO | No tiene equipos fuera de las instalaciones |
| A11.2.7 | Disposición segura o reutilización de equipos | NO | No aplica para el proceso de mensajería masiva |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A11.2.8 | Equipos de usuario desatendido | NO | No aplica para el proceso de mensajería masiva |
| A11.2.9 | Política de escritorio limpio y pantalla limpia | NO | No aplica para el proceso de mensajería masiva |
| **A12** | **SEGURIDAD DE LAS OPERACIONES** | | |
| **A12.1** | **Procedimientos operacionales y responsabilidades** | | |
| A12.1.1 | Procedimientos de operación documentados | NO | No aplica para el proceso de mensajería masiva |
| A12.1.2 | Gestión de cambios | SI | Se debe tener un procedimiento correcto para hacer algún cambio en el servidor, código o infraestructura del proceso de mensajería masiva |
| A12.1.3 | Gestión de capacidad | NO | No aplica para el proceso de mensajería masiva |
| A12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | SI | Se debe tener un ambiente de desarrollo, pruebas y de producción |
| **A12.2** | **Protección contra códigos maliciosos** | | |
| A12.2.1 | Controles contra códigos maliciosos | SI | Se debe controlar de manera adecuada los códigos maliciosos |
| **A12.3** | **Copias de respaldo** | | |
| A12.3.1 | Respaldo de la información | SI | Es importante respaldar la información |
| **A12.4** | **Registro y seguimiento** | | |

| | | | |
|---|---|---|---|
| A12.4.1 | Registro de eventos | SI | Es parte fundamental para el análisis de riesgos |
| A12.4.2 | Protección de la información de registro | SI | Se debe proteger los registros |
| A12.4.3 | Registros del administrador y del operador | SI | Se debe tener registros del administrador y de los operadores |
| A12.4.4 | Sincronización de relojes | NO | No aplica para el proceso de mensajería masiva |
| **A12.5** | **Control de software operacional** | | |
| A12.5.1 | Instalación de software en sistemas operativos | SI | Se deben controlar los software que los usuarios instalen |
| **A12.6** | **Gestión de la vulnerabilidad técnica** | | |
| A12.6.1 | Gestión de las vulnerabilidades técnicas | NO | No aplica para el proceso de mensajería masiva |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A12.6.2 | Restricciones sobre la instalación de software | NO | No aplica para el proceso de mensajería masiva |
| **A12.7** | **Consideraciones sobre auditorias de sistemas de información** | | |
| A12.7.1 | Controles de auditorías de sistemas de información | SI | Los logs y los registros del sistema son fundamentales para el monitoreo y control de la seguridad |
| **A13** | **SEGURIDAD DE LAS COMUNICACIONES** | | |
| **A13.1** | **Gestión de la seguridad de las redes** | | |
| A13.1.1 | Controles de redes | SI | Es necesario conocer que datos están viajando en las redes |
| A13.1.2 | Seguridad de los servicios de red | SI | Mantener seguro el servicio de mensajería masiva |
| A13.1.3 | Separación en las redes | SI | No es necesario realizar segregación de redes |
| **A13.2** | **Transferencia de información** | | |
| A13.2.1 | Políticas y procedimientos de transferencia de información | NO | No aplica para el proceso de mensajería masiva |
| A13.2.2 | Acuerdos sobre transferencia de información | NO | No aplica para el proceso de mensajería masiva |
| A13.2.3 | Mensajería electrónica | NO | No aplica para el proceso de mensajería masiva |
| A13.2.4 | Acuerdos de confidencialidad o de no divulgación | SI | El proceso debe ser confidencial |

| | | | |
|---|---|---|---|
| **A14** | **Adquisición, desarrollo y mantenimiento de sistemas** | | |
| **A14.1** | **Requisitos de seguridad de los sistemas de información** | | |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | NO | No aplica para el proceso d mensajería masiva |
| A.14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas | NO | No aplica para el proceso d mensajería masiva |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones. | NO | No aplica para el proceso d mensajería masiva |
| **A14.2** | **Seguridad en los procesos de Desarrollo y de Soporte** | | |
| A.14.2.1 | Política de desarrollo seguro | SI | Se debe proveer una polític de desarrollo seguro |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A.14.2.2 | Procedimientos de control de cambios en sistemas | SI | Se debe tener un control para realizar adecuadamente cambios en el sistema |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | SI | Es necesario monitorear e sistema después de que hubo algún cambio |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software | SI | No se debe actualizar algún paquete de software que no sea compatible con el sistema de mensajería masiva |
| A.14.2.5 | Principio de Construcción de los Sistemas Seguros. | SI | Se debe contar con procedimientos para la construcción de sistemas seguros |
| A.14.2.6 | Ambiente de desarrollo seguro | SI | Es necesario contar con un ambiente de desarrollo seguro y evitar algún tipo de fuga de confidencialidad |
| A.14.2.7 | Desarrollo contratado externamente | NO | No se contratan desarrolladores externos para este proceso |
| A.14.2.8 | Pruebas de seguridad de sistemas | SI | Se debe realizar pruebas de seguridad |
| A.14.2.9 | Prueba de aceptación de sistemas | NO | No aplica para el proceso de mensajería masiva |
| A14.3 | Datos de prueba | | |
| A.14.3.1 | Protección de datos de prueba | NO | No aplica para el proceso de mensajería masiva |

| | | | |
|---|---|---|---|
| A15 | RELACIONES CON LOS PROVEEDORES | | |
| A15.1 | Seguridad de la información en las relaciones con los proveedores. | | |
| A15.1.1 | Política de seguridad de la información para las relaciones con proveedores | NO | No aplica para el proceso de mensajería masiva |
| A15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | NO | No aplica para el proceso de mensajería masiva |
| A15.1.3 | Cadena de suministro de tecnología de información y comunicación | NO | No aplica para el proceso de mensajería masiva |
| A15.2 | Gestión de la prestación de servicios de proveedores | | |
| A15.2.1 | Seguimiento y revisión de los servicios de los proveedores | NO | No aplica para el proceso de mensajería masiva |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| A15.2.2 | Gestión del cambio en los servicios de los proveedores | NO | No aplica para el proceso d mensajería masiva |
| A16 | GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | | |
| A16.1 | Gestión de incidentes y mejoras en la seguridad de la información | | |
| A16.1.1 | Responsabilidades y procedimientos | NO | No aplica para el proceso d mensajería masiva |
| A16.1.2 | Reporte de eventos de seguridad de la información | SI | Es necesario conocer si hub algún acceso no deseado algún cliente está envianc más mensajes de lo pactado |
| A16.1.3 | Reporte de debilidades de seguridad de la información | SI | Se debe tener un reporte d las debilidades para despué solucionar estos problemas |
| A16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | SI | Evaluar los eventos d seguridad y tomar decisione para mitigarlos e indispensable para la mejor continua del sistema |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | SI | Se debe tener u procedimiento adecuado par responder correctamente ant un fallo de seguridad |
| A16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | SI | Es necesario aprender de lo incidentes ocurridos par mitigarlos a futuro |

| | | | |
|---|---|---|---|
| A16.1.7 | Recolección de evidencia | SI | Es importante tener la evidencia de estos fallos de seguridad para conocer los riesgos existentes y mitigarlos |
| **A17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO** | | |
| **A17.1** | **Continuidad de Seguridad de la información** | | |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | SI | Tiene aplicabilidad en todo SGSI |
| A17.1.2 | Implementación de la continuidad de la seguridad de la información | SI | Tiene aplicabilidad en todo SGSI |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la | SI | Se debe realizar una actualización continua de la continuidad de seguridad de la información |

| Sección | Dominio de la norma | Aplicabilidad | Justificación para exclusión |
|---|---|---|---|
| | seguridad de la información | | |
| **A17.2** | **Redundancias** | | |
| A17.2.1 | Disponibilidad de instalaciones de procesamiento de información | SI | Siendo el proceso central es necesario garantizar la alta disponibilidad |
| **A18** | **CUMPLIMIENTO** | | |
| **A18.1** | **Cumplimiento de requisitos legales y contractuales** | | |
| A18.1.1 | Identificación de la legislación aplicable. | NO | No aplica para el proceso de mensajería masiva |
| A18.1.2 | Derechos propiedad intelectual (DPI) | NO | No aplica para el proceso de mensajería masiva |
| A18.1.3 | Protección de registros | NO | No aplica para el proceso de mensajería masiva |
| A18.1.4 | Privacidad y protección de información de datos personales | NO | No aplica para el proceso de mensajería masiva |
| A18.1.5 | Reglamentación de controles criptográficos. | NO | No aplica para el proceso de mensajería masiva |
| **A18.2** | **Revisiones de seguridad de la información** | | |
| A18.2.1 | Revisión independiente de la seguridad de la información | SI | Se deben revisar las prácticas de la organización para la gestión de la seguridad de la información |
| A18.2.2 | Cumplimiento con las políticas y normas de seguridad | SI | Se debe revisar que todas las políticas de seguridad se estén cumpliendo |
| A18.2.3 | Revisión del cumplimiento técnico | SI | Revisar periódicamente que se cumplan adecuadamente todos los requerimientos de acuerdo a la política de seguridad |

**Fuente:** Los autores

**ANEXO E: Matriz de riesgos**

| Riesgo | Evaluación de riesgos | | | Respuesta al riesgo | | |
|---|---|---|---|---|---|---|
| | Impacto | Probabilidad | Nivel de riesgo | Acción | Respuesta | Actividades de control |
| Acceso no autorizado | 3.7 | Probable | Alto | Evitar | Contar con un panel de seguridad para el acceso al cuarto<br>Definir permisos de acceso a usuarios | A9.1.1. Política de control de acceso. |
| Eliminación errónea de registros | 4.7 | Probable | Alto | Evitar | Impedir el acceso a usuarios no autorizados<br>Tener respaldo de los registros con información critica<br>Probar correctamente el sistema para garantizar que no se eliminen registros indebidos | A12.3.1 Respaldo de la información, A9.1.2. Acceso a redes y a servicios en red, A12.4.1 Registro de eventos, A12.4.3 Registros del administrador y del operador. |
| Denegación de servicio por error | 4.3 | Probable | Alto | Mitigar | Impedir el acceso a usuarios no autorizados | A9.1.1. Política de control de acceso. |
| Subir código con fallas a producción | 3.3 | Probable | Alto | Evitar | Pasar por un ambiente de pruebas antes de subir a producción | A14.2.1. Política de desarrollo seguro, A14.2.2. Procedimientos de control de |

| Riesgo | Evaluación de riesgos | | | Respuesta al riesgo | | |
|---|---|---|---|---|---|---|
| | Impacto | Probabilidad | Nivel de riesgo | Acción | Respuesta | Actividades de control |
| | | | | | | cambios de sistemas, A14.2.6. Ambiente de desarrollo seguro |
| Mantenimiento Inadecuado | 3.0 | Probable | Medio | Mitigar | Se debe contar con un procedimiento claramente documentado para realizar el mantenimiento a los equipos | A11.2.4. Mantenimiento de los equipos |
| Virus | 4.0 | Probable | Alto | Mitigar | Se debe actualizar el antivirus en todos los sistemas, esto incluye laptops, PCs, servidores | A12.2.1 Controles contra códigos maliciosos |
| Eliminación de registros para el correcto funcionamiento del SO | 4.0 | Posible | Medio | Evitar | Impedir el acceso a usuarios no autorizados | A9.2.2. Suministro de acceso a usuarios, A12.4.2 Protección de la información de registro, A9.2.3. Gestión de derechos de accesos privilegiados |
| | | | | | Asignar correctamente los privilegios a las cuentas de usuarios | |

| Riesgo | Evaluación de riesgos | | | Respuesta al riesgo | | |
|---|---|---|---|---|---|---|
| | Impacto | Probabilidad | Nivel de riesgo | Acción | Respuesta | Actividades de control |
| Daño por suciedad | 2.0 | Posible | Medio | Mitigar | Realizar la limpieza y mantenimiento de equipos al menos 2 veces por semana | A11.2.1. Ubicación y protección de los equipos, A11.2.4. Mantenimiento de los equipos |
| Desgaste por partes | 3.3 | Probable | Medio | Mitigar | Mantener los activos en un ambiente adecuado para evitar el desgaste rápido de materiales | A11.2.1. Ubicación y protección de los equipos |
| Huecos de seguridad | 4.3 | Probable | Medio | Mitigar | Pasar por un ambiente de pruebas antes de subir a producción<br>Tener una documentación de los que se está subiendo y lo que se debe probar para así realizar las pruebas necesarias | A14.2.1. Política de desarrollo seguro, A14.2.2. Procedimientos de control de cambios de sistemas, A14.2.6. Ambiente de desarrollo seguro |
| Daño por inundación | 2.7 | Improbable | Bajo | Aceptar | | |
| Destrucción de la información | 3.0 | Probable | Medio | Mitigar | Tener respaldo de los registros con información critica | A12.3.1 Respaldo de la información |

| Riesgo | Evaluación de riesgos | | | Respuesta al riesgo | | |
|---|---|---|---|---|---|---|
| | Impacto | Probabilidad | Nivel de riesgo | Acción | Respuesta | Actividades de control |
| Corte de suministro de luz | 4.3 | Posible | Medio | Mitigar | Tener fuentes de energía alternas y listas para ser usadas cuando haya un corte eléctrico | A17.2.1. Disponibilidad de instalaciones de procesamiento de información |
| No existe respaldo de información | 3.3 | Probable | Medio | Evitar | Tener respaldo de los registros con información critica | A12.3.1 Respaldo de la información |
| Daño por incendio | 5.0 | Probable | Alto | Mitigar | Contar con un extintor<br>Todo objeto inflamable debe estar lejos de las áreas de cómputo y de lugares donde se trabaje con fuego | A11.2.1. Ubicación y protección de los equipos |
| Terremoto | 3.7 | Improbable | Bajo | Aceptar | | |
| Desgaste de hojas | 2.3 | Casi seguro | Medio | Mitigar | Tener un respaldo de los registros y esto debe estar localizado en algún servidor o en la nube | A12.3.1 Respaldo de la información |

**Fuente:** Los autores