# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE INFRAESTRUCTURA TECNOLÓGICA, DE ALFAGRES S.A BASADO EN LA NORMA ISO/IEC 27001:2013

**JOSE HARBEY CAICEDO CARRILLO**
**JHON JAIRO ROJAS SUAREZ**

**UNIVERSIDAD PILOTO DE COLOMBIA**
**DIRECCIÓN DE POSTGRADOS**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**BOGOTÁ**
**2017**

# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE INFRAESTRUCTURA TECNOLÓGICA, DE ALFAGRES S.A BASADO EN LA NORMA ISO/IEC 27001:2013

**JOSE HARBEY CAICEDO CARRILLO**
**JHON JAIRO ROJAS SUAREZ**

**Proyecto de grado para optar por el título de Especialista en Seguridad Informática**

**Asesor:**
**Lorena Ocampo Correa**
**Ingeniera de Sistemas**

**UNIVERSIDAD PILOTO DE COLOMBIA**
**DIRECCIÓN DE POSTGRADOS**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**BOGOTÁ**
**2017**

Nota de Aceptación:

_____
_____
_____
_____

_____
Firma del presidente del jurado:

_____
Firma primer jurado

_____
Firma segundo jurado

Bogotá, octubre del 2017

## DEDICATORIA

Este trabajo está dedicado a nuestros familiares y amigos, quienes han sido un apoyo y motivación constante en nuestro proceso de formación como profesionales, y especialistas en seguridad de la información.

A la universidad piloto de Colombia, administrativos, docentes y compañeros que brindaron un gran aporte en la formación profesional e institucional.

José, Jhón

## AGRADECIMIENTOS

Agradecemos a la universidad piloto de Colombia, por su compromiso con la formación de profesionales en seguridad de la información, a nuestros familiares y amigos, por el apoyo incondicional, y finalmente a nuestros docentes, quienes con su arduo trabajo han aportado a nuestra vida como profesionales, y aún más, como personas integras.

**CONTENIDO**

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE CUADROS

pág.

## GLOSARIO

**ACTIVO DE INFORMACIÓN: "**es un recurso de información que posee importancia para la materialización de los objetivos en una compañía, como los sistemas de telecomunicaciones, las bases de datos, el personal, manuales"[1.]

**AMENAZAS DE SEGURIDAD: "**son aquellas situaciones que pueden aprovechar o explotar una vulnerabilidad, generando daño total o parcial a la operación de un sistema u organización"[2]

**ANÁLISIS DE RIESGOS: "**es un proceso que permite identificar las amenazas a las que se encuentran expuestos todos los activos de información, se estima la frecuencia en la que se materializan todas las amenazas y valora el impacto que causarían al materializarse en nuestra organización"[3]

**CONTRAMEDIDAS:** son "los mecanismos que se utilizan para defender ataque, existen dos la preventivas con el fin de evitar el ataque o reducir sus consecuencias y paliativas para reducir el daño del ataque"[4]
**CONTROL:** son "todos los procedimientos, políticas establecidas, con el fin de mantener los riesgos por un nivel más bajo del asumido"[5]

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: "**un único evento o una cantidad de eventos de seguridad de la información que se pueden presentar de forma inesperada que poseen una gran probabilidad de comprometer las operaciones del negoció"[6].

**POLÍTICA DE SEGURIDAD: "**declaración de alto nivel que describe la posición de la entidad sobre un tema específico"[7]

---

[1] ISOTOOLS EXCELLENCE. ISO 27001: Los activos de información. [en línea]. Bogotá: PMG, 2015 [fecha de consulta 3 junio de 2017]. Disponible en: www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-información/

[2] PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo en "texto claro". [en línea]. Bogotá: MAGAZCITUM, 2013 [fecha de consulta 3 de junio de 2017]. Disponible en: www.magazcitum.com.mx/?p=2193#.WWKCUoQ1_IU

[3] ISOTOOLS. ISO 27005: Análisis de Riesgos. [en línea]. Bogotá: ISotools, 2015 [fecha de consulta 3 de junio de 2017]. Disponible en: www.isotools.pe/iso-27005-analisis-de-riesgos/

[4] CARRILLO, Aldair. Contramedidas contra ataques informáticos. [en línea]. Bogotá: Blogspot, 2013 [fecha de consulta 3 de junio de 2017]. Disponible en: http://aldair-11b.blogspot.com.co/2013/04/contramedidas-para-ataques-informaticos.html

[5] EL PORTAL DE LA ISO 27001. Glosario. [en línea]. Bogotá: ISO, 2012 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/glosario.html

[6] EL PORTAL DE LA ISO 27001. Glosario. [en línea]. Bogotá: ISO, 2012 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/glosario.html

[7] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Seguridad y privacidad de la información. [en línea]. Bogotá: MinTic, 2016 [fecha de consulta 3 de junio de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

**RIESGO:** es “una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia”[8]

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** es el “concepto central sobre el que se construye la norma ISO/IEC 27001:2013, es un proceso sistemático, documentado y conocido por toda la organización, puede considerarse, como el sistema de calidad para la seguridad de la información”[9]

**VULNERABILIDAD:** una vulnerabilidad es “una debilidad de un bien o de un control, es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento”[10]

[8] ISOTOOLS EXCELLENCE. ISO 27001: Los activos de información. [en línea]. Bogotá: Issotools, 2015 [fecha de consulta 3 de junio del 2017]. Disponible en: www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-información/

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Information Security Risk Management. Geneva: ISO, 2008. p. 24.

[10] PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo en “texto claro”. [en línea]. Bogotá: MAGAZCITUM, 2013 [fecha de consulta 3 de junio de 2017]. Disponible en: www.magazcitum.com.mx/?p=2193#.WWKCUoQ1_IU

# INTRODUCCIÓN

Actualmente la información se ha posicionado como uno de los activos más valiosos para las compañías, permitiendo realizar análisis y tomas de decisiones para el mejoramiento continuo del negocio, por lo cual la protección de este activo se ha convertido en un punto vital para las organizaciones, que por medio de las mejores prácticas, normas y estándares, se han interesado en la gestión de los riesgos e implementación de controles con el fin de evitar accesos no autorizados a la información, y minimizando los eventos que puedan afectar su disponibilidad, integridad o confidencialidad.

Para ALFAGRES S.A la información es muy importante, sin embargo, presenta un alto grado de riesgo, al no contar con políticas claras y procedimientos adecuados para la gestión de dicho recurso, y los activos que la procesan, almacenan y transportan. El área de infraestructura tecnológica gestiona los sistemas informáticos de toda la compañía, para tratar adecuadamente los riesgos de la información, se propone el diseño del sistema de gestión de seguridad de la información (SGSI), para esta área, brindando un nivel de conocimiento adecuado de los activos actuales y un proceso claro de identificación y valoración de riesgos que permita enfocar los recursos destinados por la organización, en la implementación de controles, para disminuir el nivel de los riesgos que mayor impacto puedan causar a la organización.

En el diseño del Sistema de Gestión de Seguridad de la Información (SGSI), para el área de infraestructura tecnológica de ALFAGRES S.A se planteará un sistema de análisis de riesgos, definiendo el nivel que puede aceptar la organización, para esto se tienen presente la norma estándar ISO/IEC 27001:2013, como fundamento.

# 1. PLANTEAMIENTO DEL PROBLEMA

ALFAGRES S.A es una empresa con 45 años de presencia en el sector industrial, dedicada a la producción, comercialización, distribución, importación, exportación y mercadeo de todo tipo de pisos y revestimientos para vivienda, oficinas y construcción en general, cuenta con un total de 72 sedes distribuidas a lo largo del territorio nacional, lo que la constituye como una de las empresas líderes en la industria de la cerámica.

Debido a la exigencia del mercado, ALFAGRES S.A ha venido adoptando en los últimos años, nuevas tecnologías de la información, que permiten incrementar la productividad en el desarrollo de sus procesos, garantizando una comunicación efectiva entre las diferentes sedes, y aportando al crecimiento de la compañía y bienestar de sus colaboradores.

El área de Infraestructura tecnológica es la encargada de gestionar y asegurar el buen funcionamiento de la infraestructura de TI, teniendo en cuenta la importancia que esta representa, para la operación de la compañía. Por esta razón se propone realizar una investigación mediante la cual, se identifiquen las necesidades de protección para dicha infraestructura, evaluando su estado actual de seguridad, identificando posibles amenazas y realizando una estimación de riesgos, que conlleven a la definición de una política general de seguridad, para los procesos del área.

## 1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo identificar y valorar los riesgos asociados a los procesos del área de infraestructura tecnológica de ALFAGRES S.A.?

## 2. JUSTIFICACIÓN

En la última década, se ha presentado una evolución asombrosa por parte de la tecnología, convirtiéndose en una herramienta fundamental para la operación diaria de cualquier tipo de empresa, sin embargo, este acelerado ritmo de crecimiento ha dejado diferentes falencias a su paso, generando riesgos para las diferentes áreas de las organizaciones, especialmente las encargadas de administrar los sistemas informáticos que soportan la operación diaria de una compañía, por este motivo cobra gran importancia la seguridad de la información, como el área encargada de proteger la infraestructura de tecnología y las comunicaciones, identificando las amenazas y gestionando apropiadamente los riesgos.

Un sistema de seguridad de la información comprende un conjunto de medios administrativos, técnicos y de personal, que garanticen un nivel de seguridad adecuado, teniendo en cuenta los riesgos estimados para un sistema informático.

El objetivo de este proyecto es diseñar un sistema de seguridad de la información para el área de infraestructura tecnológica de la empresa ALFAGRES S.A, de tal modo que permita la caracterización de los sistemas informáticos gestionados por esta área, un análisis para identificar las amenazas y gestionar los riesgos, y la definición de las políticas de seguridad de acuerdo con la regulación vigente y las características de la organización.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, para el área de infraestructura tecnológica de la empresa ALFAGRES S.A

## 3.2 OBJETIVOS ESPECÍFICOS

- Determinar el estado actual de la seguridad de la información en el área de infraestructura tecnológica de ALFAGRES S. A.

- Identificar y realizar el inventario de activos para el área de infraestructura tecnológica de ALFAGRES S. A.

- Realizar el análisis de riesgos, para los activos identificados, de acuerdo a la norma ISO/IEC 27005:2011

- Proponer el tratamiento de los riesgos identificados de cuerdo a la norma ISO/IEC 27001:2013.

- Plantear la política de seguridad de la información para el área de infraestructura tecnológica de ALFAGRES S. A.

# 4. MARCO TEÓRICO

El rápido avance que se ha presentado en las tecnologías durante los últimos años, ha proyectado la información como un activo de gran relevancia para las organizaciones, despertando interés en los niveles gerenciales para asegurar su protección, e impulsar la implementación de sistemas que permitan gestionar la disponibilidad, integridad y confidencialidad de la información, ante posibles amenazas, que puedan aprovechar las vulnerabilidades existentes, y someterla a diferentes formas de fraude, espionaje, sabotaje o vandalismo.

El departamento de infraestructura tecnológica en ALFAGRES SA, tiene la función de apoyar los procesos de la compañía, poniendo a su disposición tecnologías de la información, que permitan el cumplimiento eficiente en las funciones de sus colaboradores, aportando lineamientos que garanticen la protección de datos y garantizando un alto nivel de disponibilidad.

## 4.1 SEGURIDAD DE LA INFORMACIÓN

La información puede ser definida como un conjunto de datos organizados, y estructurados que transmiten un mensaje, dichos datos pueden almacenarse y transmitirse de diferentes maneras, "la seguridad de la información abarca todos aquellos mecanismos de prevención y corrección que utilizan las personas y las empresas para proteger todos los activos relacionados a estos procesos, velando por la disponibilidad, integridad y confidencialidad de la información, dichas propiedades se definen a continuación"[11].

- Confidencialidad: se encarga de garantizar que la información solo sea accedida por personas o sistemas autorizados según su cargo o función.

- Integridad: garantiza la información exacta, completa y coherente, manteniendo sus datos tal como fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

- Disponibilidad: garantiza que la información pueda ser accedida por parte de los individuos, entidades y procesos autorizados en el momento que sea requerida.

La Figura 1 muestra los pilares de la seguridad de la información; confidencialidad, integridad, y disponibilidad, aunque dependiendo del tipo de compañía, alguna de estas propiedades reviste mayor importancia que las otras dos, se deben considerar como un trípode, para lograr equilibrio en la gestión de la información de una manera segura.

[11] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES. Política general. [en línea]. Bogotá: MinTIC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

**Figura 1. Pilares de la seguridad información**


Fuente. Los Autores

## 4.2 GESTIÓN DE RIESGO

La gestión de riesgo en la seguridad de la información es "un método para manejar las incertidumbres que se encuentran, analizando y clasificando el riesgo asociados a un sistema o proceso, e identificando mecanismos para evitarlo, mitigarlo, asumirlo o transferirlo, de tal manera que sea aceptable"[12]. Para ello deben realizar el análisis, clasificación, reducción y llevar el respectivo control.

➢Análisis: Se determinan los componentes para un sistema que requiere protección, identificando las vulnerabilidades y amenazas que lo ponen en peligro.

➢Clasificación: Se determinan los riesgos encontrados y se catalogan de acuerdo con su ocurrencia e impacto.

➢Reducción: se definen o se aplican medidas necesarias de protección, que reduzcan el nivel de riesgo.

➢Control: Se evalúa la efectividad de los controles aplicados y las medidas aplicadas en la fase de reducción.

[12] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES. Gestión de riesgo. [en línea]. Bogotá: MinTC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Para realizar el análisis de los riesgos que pueden afectar la organización, se debe realizar el establecimiento del contexto con el fin de identificar el funcionamiento interno y externo a que se afrenta y así del establecimiento del contexto, poder identificar las amenazas que pueden realizar afectaciones a los activos de la organización.

Después de realizar el respectivo análisis y valoración de los riesgos de acuerdo con los criterios establecidos por la organización, se procede con el tratamiento de ellos, con el fin de reducir la probabilidad de ocurrencia y puedan generar daños de diferentes formas como económicos, reputacionales etc.

Los riesgos aceptados y tratados o reducidos, se les debe realizar el respectivo seguimiento, identificando su comportamiento asociado a su disminución, estabilidad o crecimiento. En caso de crecer el riesgo y la compañía no está establecida para mitigarlo, lo debe trasferir a un tercero con el fin de que sea tratado y no se pueda materializar.

## 4.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, (SGSI)

Un sistema de gestión de seguridad de la información es “el conjunto de procesos, que incluyen políticas, normas y procedimientos, para la protección de la información, mediante la apropiada gestión de los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la misma”[13].

El sistema de gestión de seguridad de la información (SGSI), hace posible evaluar y tratar el riesgo referente a la multitud de amenazas originadas por personas, organizaciones, gobiernos, tecnología y el medioambiente, implantando controles necesarios para mitigar, evadir, transmitir o aceptar, según el posible impacto y los recursos con los que cuenta la organización.

En el desarrollo del proceso de un SGSI, se debe contar principalmente con la aprobación y apoyo de la alta gerencia de la organización, teniendo en cuenta que la seguridad de la información no es solamente del área tecnológica o de los niveles inferiores de la empresa, la gerencia debe tener la responsabilidad de gestionar los riesgos y los impactos del negocio. Comprometiéndose con la implementación, operación, monitorización, mantenimiento, revisión y mejora continua del SGSI, tomando iniciativas como el desarrollo de la política de seguridad, garantizar el cumplimento de planes y objetivos, construir roles y responsabilidades, designar los recursos necesarios y suficientes para llevar a cabo el ciclo de vida del SGSI, determinar los criterios de aceptación del riesgo y sus correspondientes niveles, garantizar que se realicen todas las auditorías internas y llevar acabo las revisiones periódicas del SGSI.

[13] PORTAL DE ISO 27001 EN ESPAÑOL. ¿Qué es un SGSI? [en línea]. Bogotá: ISO, 2016 [fecha de consulta 7 de marzo de 2017]. Disponible en: http://www.iso27000.es/sgsi.html

Para garantizar el éxito del sistema de gestión de seguridad de la información, la alta dirección debe como parte fundamental realizar la formación y concienciación en seguridad de la información a los colaboradores, garantizando y asignando las responsabilidades para cada uno de los individuos, de acuerdo a las funciones desempeñadas dentro de la compañía, y manteniendo una cultura de seguridad, por parte de la totalidad de la organización.

### 4.4 NORMA -ISO/IEC 27001:2013

La norma ISO/IEC 27001:2013, es un estándar para la seguridad de la información, que permite el establecimiento y gestión del sistemas de gestión de seguridad de la información, utilizando el ciclo Deming o ciclo PHVA (planificar, hacer, verificar y actuar), que supone la implementación de un sistema de gestión que se centra en la mejora continua requiriendo una constante evolución para adaptarse a los cambios que se producen en la organización, e intentar conseguir el nivel más alto de eficacia operativa, las actividades que se realizan en el ciclo Deming (PHVA) son las siguientes:

- Plan (Planificar): Diseñar el sistema de gestión de seguridad de la información (SGSI), con la definición del alcance y la política de seguridad, realizando un análisis de riesgo que refleje la situación actual de la entidad. Teniendo el resultado del análisis, se definirá el plan de tratamiento de los riesgos y controles de seguridad para gestionar aquellos que pueden causar daño a la organización.

- Do (Hacer): Implantar y operar el sistema de gestión de seguridad de la información, centrándose en el plan de tratamiento de los riesgos.

- Check (Verificar): Monitorizar y revisar el sistema de gestión de seguridad de la información, realizando auditorías internas independientes y objetivas, además de realizar una revisión global del sistema de gestión de seguridad de la información por parte de la alta dirección de la organización, con el fin de enfocarse en nuevas metas a cumplir durante el próximo ciclo del SGSI.

- Act (Actuar): Mantener y mejorar el sistema de gestión de seguridad de la información[14].

[14] GLOBAL ASSOCIATION ISACA. Implementación efectiva de un SGSI ISO 27001. [en línea]. Bogotá: ISACA, 2014 [fecha de consulta 3 de junio de 2017]. Disponible en: www.isaca.org/ chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CI GRAS%20ISO%2027001 %20-%20 rbq.pdf

## 5. ESTADO ACTUAL

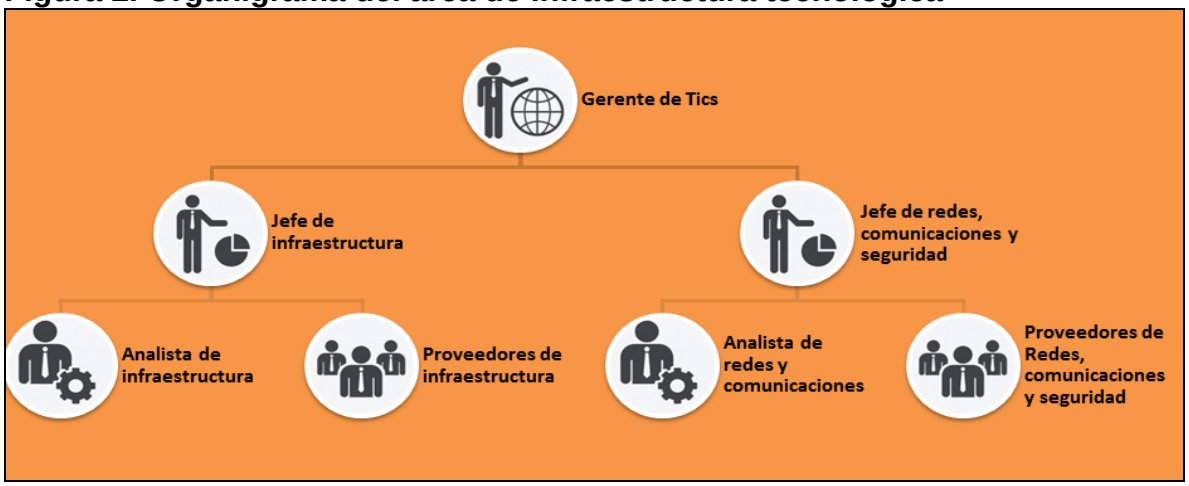
ALFAGRES S.A es una empresa experta en la producción, comercialización, distribución, importación, exportación y mercadeo de todo tipo de pisos y revestimientos para vivienda, y construcción en general. Cuenta con presencia en 18 ciudades de Colombia y actualmente exporta a países americanos, europeos y asiáticos, obteniendo reconocimiento mundial.

La misión de ALFAGRES S.A se define en diseñar y construir bienestar para la sociedad, renovando la vida de las personas a través de espacios inspiradores

La visión de ALFAGRES S.A se define en; para el 2020 ser una empresa consolidada y líder del mercado colombiano, siendo reconocida como un icono de diseño e innovación en construcción y remodelación, con un 30 % de sus ventas provenientes del mercado internacional y logrando un margen EBITDA del 12 %.

ALFAGRES S.A esta compuesta por aproximadamente tres mil colaboradores, organizados a su vez en las vicepresidencias de mercadeo, abastecimiento, manufactura, financiera y administrativa. La gerencia de Tics, se encuentra bajo el mando de la Vicepresidencia Financiera, y está encargada de las áreas de proyectos, infraestructura tecnológica (IT), mesa de servicios, datos maestros, y plataformas véase la Figura 2.

**Figura 2. Organigrama del área de Infraestructura tecnológica**




Fuente. Los Autores

El área de infraestructura tecnológica está dividida en dos jefaturas, la jefatura de redes y comunicaciones, y la jefatura de infraestructura, como su nombre lo indica, la jefatura de redes y comunicaciones se encarga de la administración de los servicios de red usados por la compañía. Por su parte el área de infraestructura administra los servicios de infraestructura de la organización, El área de infraestructura tecnológica, cuenta con una importante cantidad de proveedores,

en los cuales se apoya, para el cumplimiento de su objetivo, y centrando sus funciones en la administración de dichos proveedores.

## 5.1 PROCESOS DEL ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

El área de infraestructura tecnológica dentro de ALFAGRES S.A, es un área habilitadora, que presta servicios, para apoyar y mejorar los procesos de la organización. Sus objetivos se centran en la administración de seguridad y continuidad, soporte, operación, y apoyo a proyectos, para los servicios de la infraestructura de tecnología en la organización, con el fin de apalancar las operaciones de las unidades de negocio. En la Figura 3, se pueden observar los procesos que son responsabilidad del área.

**Figura 3. Procesos del área infraestructura tecnológica**


Fuente. Los Autores

La dirección de Infraestructura tecnológica interviene en 4 de los procesos de la gerencia de Tics, los cuales se describen a continuación:

➢Administración de servicios de soporte: brindar soporte y gestión al usuario final sobre la infraestructura y sistemas de información que apalancan las operaciones de las unidades de negocio.

➢Administración de servicios de operación: asegurar la total disponibilidad de la infraestructura de tecnología para garantizar la continuidad de las operaciones en las unidades de negocio.

➢Administración de soporte de proyectos: proponer y liderar técnicamente proyectos de mejora e innovación que permitan potenciar el conocimiento y el uso de los sistemas de información en las unidades de negocio del grupo empresarial Alfa.

➢Administración de seguridad y continuidad: mantener un conjunto de planes de continuidad, mantenimiento y seguridad informática de los servicios de Tics del grupo empresarial Alfa.

## 5.2 IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES

En las organizaciones es de vital importancia establecer contramedidas o controles para proteger los activos de las amenazas que lo pueden afectar de diferente forma. Para la identificación de la existencia o planificación de controles en la organización se puede verificar la documentación existente acerca de controles, verificación con el personal encargado de los controles implementados, si existen controles implementados, se debe realizar una revisión en el lugar donde se efectúa el control y verificar el respectivo cumplimiento. Se debe realizar un seguimiento a los controles existentes validando la eficacia del control, si no se realiza este proceso y algún control no funciona correctamente este puede causar vulnerabilidades, para ello se deben tener controles complementarios, que realicen el tratamiento del riesgo identificado de manera eficaz.

Teniendo en cuenta que actualmente no se encuentra establecido un SGSI en el área de infraestructura tecnológica de ALFAGRES S.A, se hace necesario evaluar el estado actual de la seguridad de la información, y validar como se encuentra con respecto a la normativa.

En el Cuadro 1, se puede observar los resultados de la validación de controles en ALFAGRES S.A, obteniendo el estado actual de seguridad con respecto a la norma ISO/IEC 27001:2013. Se marcó con color verde, rojo o amarillo, la casilla correspondiente, que señala si el control se encuentra implementado, no implementado, o parcialmente implementado.

**Cuadro 1. Estado actual de la seguridad**

| | | | | | |
|---|---|---|---|---|---|
| A.5 Políticas de seguridad de la información | | | | | |
| A.5.1 Orientación de la dirección para la gestión de la seguridad de la información | | | | | |
| Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. | | | | | |
| A.5.1.1 | Políticas para la seguridad de la información. | Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | La Compañía no cuenta con una política de seguridad publicada y comunicada a los empleados y partes interesadas, que permita conocer las directrices de la alta dirección con respecto a la seguridad de la información. | | |
| A.5.1.2 | Revisión de la política de seguridad de la información. | Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | La Compañía no cuenta con una política de seguridad publicada y comunicada a los empleados y partes interesadas, que permita conocer las directrices de la alta dirección con respecto a la seguridad de la información, por lo tanto no se revisan. | | |
| A.6 Organización de la seguridad de la información | | | | | |
| 6.1 Organización interna | | | | | |
| Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. | | | | | |
| A.6.1.1 | Roles y responsabilidades para la seguridad de información. | Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se tienen asignadas las responsabilidades de seguridad física, y seguridad de la información, existe una dirección de seguridad física, y la gerencia de Tics, se encarga de la seguridad perimetral y de host. | | |

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| A.6.1.2 | Separación de deberes. | Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | La compañía cuenta con una distribuciones roles en el área de Tecnología, para evitar posibilidades de modificación no autorizadas, de igual manera existe un área independiente que realiza auditoría a la gerencia de Tics, para identificar posibles abuso de permisos por parte de los administradores de tecnología. | | |
| A.6.1.3 | Contacto con las autoridades. | Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Existen estructuras a nivel organizacional, que permiten la toma de decisiones y acciones pertinentes en caso de ser necesarias, para garantizar la seguridad de la información. | | |
| A.6 Organización de la seguridad de la información | | | | | |
| 6.1 Organización interna | | | | | |
| Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. | | | | | |
| A.6.1.4 | Contacto con grupos de interés especial. | Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Existe vínculo con varios proveedores de servicios, especializados en seguridad, que retroalimentan a la gerencia de Tics, sobre información de interés, en cuanto a seguridad informática. | | |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos. | Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se incluye la seguridad de la información, en la gestión de proyectos realizados dentro del área. | | |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="5">6.2 Dispositivos móviles y teletrabajo</td></tr>
<tr><td colspan="5">Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.</td></tr>
<tr><td rowspan="3">A.6.2.1</td><td rowspan="3">Política para dispositivos móviles.</td><td rowspan="3">Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI NO</td><td>PARCIALMENTE</td></tr>
<tr><td colspan="2">Existe una normativa, publicada y aprobada por la gerencia de Tics, que regula el uso de dispositivos móviles corporativos.</td></tr>
<tr><td colspan="5">6.2 Dispositivos móviles y teletrabajo</td></tr>
<tr><td colspan="5">Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.</td></tr>
<tr><td rowspan="3">A.6.2.2</td><td rowspan="3">Teletrabajo.</td><td rowspan="3">Control: Se deberían 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.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI NO</td><td>PARCIALMENTE</td></tr>
<tr><td colspan="2">No existe una política de seguridad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.</td></tr>
<tr><td colspan="5">A.7 Seguridad de los recursos humanos</td></tr>
<tr><td colspan="5">7.1 Antes de asumir el empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</td></tr>
<tr><td rowspan="3">A.7.1.1</td><td rowspan="3">Selección</td><td rowspan="3">La verificación 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.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI NO</td><td>PARCIALMENTE</td></tr>
<tr><td colspan="2">Actualmente se realiza un proceso de selección por parte le área de recursos humanos, sin embargo, no hay ninguna aprobación o verificación por parte del área de seguridad de la información.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="5">A.7 Seguridad de los recursos humanos</td></tr>
<tr><td colspan="5">7.1 Antes de asumir el empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</td></tr>
<tr><td rowspan="3">A.7.1.2</td><td rowspan="3">Términos y condiciones del empleo.</td><td rowspan="3">Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI NO</td><td>PARCIALMENTE</td></tr>
<tr><td colspan="2">Los contratos realizados con proveedores, del área, incluyen algunas cláusulas en cuanto al tratamiento de información confidencial sensible, de la compañía, sin embargo, no existe un modelo que permite validar los requerimientos mínimos de seguridad, que se requieren por parte del proveedor, según los servicios ofrecidos a la compañía.</td></tr>
<tr><td colspan="5">7.2 Durante la ejecución del empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td rowspan="3">A.7.2.1</td><td rowspan="3">Responsabilidades de la dirección.</td><td rowspan="3">Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI</td><td>NO PARCIALMENTE</td></tr>
<tr><td colspan="2">No existen políticas de seguridad de la información, que indiquen los requerimientos mínimos que deben cumplir los empleados y proveedores, o demás personal relacionado con el área de IT.</td></tr>
<tr><td colspan="5">7.2 Durante la ejecución del empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td rowspan="3">A.7.2.2</td><td rowspan="3">Toma de conciencia, educación y formación en la seguridad de la información.</td><td rowspan="3">Control: Todos los empleados de la organización, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes.</td><td colspan="2">Implementado</td></tr>
<tr><td>SI</td><td>NO PARCIALMENTE</td></tr>
<tr><td colspan="2">No existen políticas de seguridad de la información, y no hay programas de concientización, educación o formación, en el área, o la organización que aporten conocimientos de seguridad de la información a los empleados proveedores, y personas involucradas en el tratamiento, almacenamiento y transporte de la información en al área de IT.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.7.2.3 | Proceso disciplinario | Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | Implementado<br>SI / NO / PARCIALMENTE<br>No existen procesos disciplinarios formales, para emprender acciones contra empleados, proveedores, o terceros que hayan cometido una violación a la seguridad de la información, de igual manera, no existe la política de seguridad, que defina lo que puede ser considerado como una violación de seguridad de la información. |
| 7.3 Terminación o cambio de empleo | | | |
| Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato. | | | |
| A.7.3.1 | 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 de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir. | Implementado<br>SI / NO / PARCIALMENTE<br>No existen cláusulas que obliguen a los empleados o proveedores del área, cumplir con las responsabilidades y deberes de seguridad de la información, en caso de terminación o cambio de contrato. |
| A.8 Gestión de activos | | | |
| 8.1 Responsabilidad por los activos | | | |
| Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. | | | |
| A.8.1.1 | Inventario de activos. | Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de activos. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe inventario, ni proceso de identificación de activos de información. |
| A.8.1.2 | Propiedad de los activos. | Control: Los activos mantenidos en el inventario deberían tener un propietario. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe inventario, ni proceso de identificación de activos de información, por lo tanto no hay claridad, con respecto a los responsables de los activos de información en el área de IT. |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.8 Gestión de activos | | | |
| 8.1 Responsabilidad por los activos | | | |
| Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. | | | |
| A.8.1.3 | Uso aceptable de los activos. | Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | Implementado<br>SI / NO / PARCIALMENTE<br>No existen reglas para el uso de información y de activos asociados con la instalación y procesamiento de la misma. |
| A.8.1.4 | Devolución de activos. | Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. | Implementado<br>SI / NO / PARCIALMENTE<br>Existe un proceso de paz y salvo mediante el cual se valida que los empleados y usuarios del área entreguen los activos entregados por la organización, al terminar su vínculo laboral. |
| 8.2 Clasificación de la información | | | |
| Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. | | | |
| A.8.2.1 | Clasificación de la información. | Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un proceso de clasificación de la información, para evaluar su criticidad, y determinar el valor que tiene para el área de IT, o la organización. |
| 8.2 Clasificación de la información | | | |
| Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. | | | |
| A.8.2.2 | Etiquetado de la información. | Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado por la organización. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un esquema de clasificación de información, para un adecuado etiquetado de la información. |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.8.2.3 | Manejo de activos. | Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema adoptado por la organización. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un esquema de clasificación de información, o procedimientos para el manejo de activos. |
| 8.3 Manejo de medios<br>Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. | | | |
| A.8.3.1 | Gestión de medios removibles. | Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema adoptado por la organización. | Implementado<br>SI / NO / PARCIALMENTE<br>No existen procedimientos para la gestión de medios removibles. |
| A.8.3.2 | Disposición de los medios. | Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | Implementado<br>SI / NO / PARCIALMENTE<br>Existe un área que apoya el proceso de reciclaje de medios tecnológicos, sin embargo no existe un procedimiento formal en el área que regule este proceso. |
| 8.3 Manejo de medios<br>Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. | | | |
| A.8.3.3 | Transferencia de medios físicos. | Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un procedimiento que permita proteger los medios que contienen información contra acceso no autorizado, o controles que permitan restringir el acceso no autorizado a la información contenida en los medios físicos. |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.9 Control de acceso | | | |
| 9.1 Requisitos del negocio para control de acceso | | | |
| Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información. | | | |
| A.9.1.1 | Política de control de acceso. | Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe una política de control de acceso que defina la visión de la seguridad de la información, por parte de la compañía, y que establezca los lineamientos para los accesos a los sistemas de información administrados por el área de IT. |
| A.9.1.2 | Política sobre el uso de los servicios de red. | Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. | Implementado<br>SI / NO / PARCIALMENTE<br>Existen controles para el uso de recursos de red, sin embargo, no existe una política definida y documentada, que indique los lineamientos con respecto al personal que debería contar con accesos a los servicios de red. |
| 9.2 Gestión de acceso de usuarios | | | |
| Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. | | | |
| A.9.2.1 | Registro y cancelación del registro de usuarios. | Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | Implementado<br>SI / NO / PARCIALMENTE<br>Existe un procedimiento claro de registro y cancelación de registro de usuarios para posibilitar la asignación de los derechos de acceso. |
| A.9.2.2 | Suministro de acceso de usuarios. | Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas. | Implementado<br>SI / NO / PARCIALMENTE<br>Existe un proceso mediante el cual se asignan o revocan derechos de accesos a los usuarios para todos los sistemas y servicios que presta el área. |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.9.2.3 | Gestión de derechos de acceso privilegiado. | Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. | Implementado<br>SI / NO / PARCIALMENTE<br>Se restringe y controla la asignación y uso de derechos de acceso privilegiado, teniendo en cuenta el perfilamiento del cargo para cada uno de los usuarios. |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios. | Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un proceso de gestión formal para la asignación de información secreta, de igual manera no existe un proceso de etiquetado de información que indique para qué información se debe cumplir este control. |
| 9.2 Gestión de acceso de usuarios | | | |
| Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. | | | |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios. | Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe un inventario de activos, y por lo tanto no hay una documentación formal de los propietarios de los mismos. |
| A.9.2.6 | 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 deberían retirar al terminar su empleo, o se deberían ajustar cuando se hagan cambios. | Implementado<br>SI / NO / PARCIALMENTE<br>Existe un proceso de retiro de accesos, cuando un usuario termina su empleo o contrato, sin embargo no existe un control, para ajustar dichos accesos, cuando se realizan cambios. |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">9.3 Responsabilidades de los usuarios</td></tr>
<tr><td colspan="4">Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.</td></tr>
<tr><td rowspan="3">A.9.3.1</td><td rowspan="3">Uso de la información de autenticación secreta.</td><td rowspan="3">Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Existen controles implementados por medio de herramientas tecnológicas, que obligan a los usuarios a autenticarse en los diferentes sistemas de información, sin embargo no existe una política formal en el área que establezca los lineamientos para el uso de información secreta.</td></tr>
<tr><td colspan="4">9.4 Control de acceso a sistemas y aplicaciones</td></tr>
<tr><td colspan="4">Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones</td></tr>
<tr><td rowspan="3">A.9.4.1</td><td rowspan="3">Restricción de acceso Información.</td><td rowspan="3">Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Existen controles para restringir los derechos de acceso, sin embargo no existe política de control de acceso que defina los lineamientos para restringir el acceso a los sistemas de información.</td></tr>
<tr><td rowspan="3">A.9.4.2</td><td rowspan="3">Procedimiento de ingreso seguro.</td><td rowspan="3">Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No existe política de control de accesos, que indique los lineamientos para determinar cuándo se requiere un proceso de ingreso seguro.</td></tr>
<tr><td rowspan="3">A.9.4.3</td><td rowspan="3">Sistema de gestión de contraseñas.</td><td rowspan="3">Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se encuentran implementados requisitos de seguridad mínimos para las contraseñas, para asegurar la calidad de estas, de igual manera se encuentra configurado en los sistemas de información del área un tiempo de vencimiento de las contraseñas, forzando a los usuarios a cambiarlas de manera periódica.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">9.4 Control de acceso a sistemas y aplicaciones</td></tr>
<tr><td colspan="4">Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones</td></tr>
<tr><td rowspan="3">A.9.4.4</td><td rowspan="3">Uso de programas utilitarios privilegiados</td><td rowspan="3">Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se encuentran definidos y aplicados controles para evitar que los usuarios puedan instalar herramientas que puedan afectar el funcionamiento de los sistemas de información.</td></tr>
<tr><td rowspan="3">A.9.4.5</td><td rowspan="3">Control de acceso a códigos fuente de programas.</td><td rowspan="3">Control: Se debería restringir el acceso a los códigos fuente de los programas.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>El código fuente de las aplicaciones corporativas es restringido y solo tienen acceso quienes por sus labores lo requieren.</td></tr>
<tr><td colspan="4">A.10 Criptografía</td></tr>
<tr><td colspan="4">10.1 Controles criptográficos</td></tr>
<tr><td colspan="4">Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.</td></tr>
<tr><td rowspan="3">A.10.1.1</td><td rowspan="3">Política sobre el uso de controles criptográficos.</td><td rowspan="3">Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No existe política sobre el uso de controles criptográficos para la protección de la información.</td></tr>
<tr><td rowspan="3">A.10.1.2</td><td rowspan="3">Gestión de llaves.</td><td rowspan="3">Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No existe política sobre el uso, protección y tiempo de vida de las llaves criptográfica.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">A.11 Seguridad física y del entorno</td></tr>
<tr><td colspan="4">11.1 Áreas seguras</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.</td></tr>
<tr><td>A.11.1.1</td><td>Perímetro de seguridad física.</td><td>Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Las redes que contienen información sensible, se encuentran segmentadas, y filtradas por corta fuegos, que supervisan el tráfico generado hacia ellas, de igual manera se cuenta con protección en todas las zonas de frontera.</td></tr>
<tr><td>A.11.1.2</td><td>Controles físicos de entrada.</td><td>Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Se encuentran implementados controles de acceso biométricos y controles físicos de seguridad para la protección de los centros de datos que manejan información sensible, permitiendo el acceso únicamente a personal autorizado, y disminuyendo el riesgo de daños o hurto.</td></tr>
<tr><td>A.11.1.3</td><td>Seguridad de oficinas, recintos e instalaciones.</td><td>Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Se encuentran implementados controles físicos de acceso a las oficinas del área, para garantizar la seguridad tanto física como lógica de la información y los sistemas que la procesan.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">A.11 Seguridad física y del entorno</td></tr>
<tr><td colspan="4">11.1 Áreas seguras</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.</td></tr>
<tr><td rowspan="3">A.11.1.4</td><td rowspan="3">Protección contra amenazas externas y ambientales.</td><td rowspan="3">Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Se encuentran implementadas medidas de contingencia para garantizar la continuidad del negocio, en caso de desastres naturales, u ataques maliciosos, que puedan afectar la infraestructura tecnológica del área, con sistemas redundantes para los activos más importantes en la operación del área de IT.</td></tr>
<tr><td rowspan="3">A.11.1.5</td><td rowspan="3">Trabajo en áreas seguras.</td><td rowspan="3">Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>No existe un procedimiento que defina los requisitos para el trabajo en áreas seguras.</td></tr>
<tr><td rowspan="3">A.11.1.6</td><td rowspan="3">Áreas de despacho y carga.</td><td rowspan="3">Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Se encuentran implementados controles físicos, que impiden el acceso al área, de personal no autorizado.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| 11.2 Equipos | | | | | |
| Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. | | | | | |
| A.11.2.1 | Ubicación y protección de los equipos | Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Los equipos se encuentran ubicados dentro de zonas protegidas por controles de acceso, temperatura e incendios, lo que reducen el riesgo de amenazas y peligros del entorno. | | |
| A.11.2.2 | Servicios de suministro. | Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se encuentra implementado un sistema de potencia ininterrumpida, que garantiza el flujo eléctrico a los equipos que son vitales para la operación, durante un periodo de 40 minutos, no se encuentra definido un procedimiento para cortes de energía de más de 40 min. | | |
| A.11.2.3 | Seguridad del cableado. | Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se siguen las buenas prácticas de cableado estructurado, para las instalaciones de puntos de datos, sin embargo no existe una política que exija requerimientos mínimos que se deben cumplir para realizar la instalación de puntos de datos nuevos. | | |
| 11.2 Equipos | | | | | |
| Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. | | | | | |
| A.11.2.4 | Mantenimiento de equipos. | Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se realizan mantenimientos, sin embargo no existe una política que indique los periodos en los cuales deben ser realizados los mantenimientos preventivos, sobre los equipos que contienen información crítica para la operación del área. | | |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.11.2.5 | Retiro de activos. | Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa. | Implementado<br>SI / NO / PARCIALMENTE<br>Se realiza inspección al realizar mantenimientos sobre equipos, y se controla el retiro de los mismos mediante formatos definidos por la compañía, sin embargo no existe un procedimiento formal para garantizar la mitigación de riesgos de seguridad, al retirar equipos de las instalaciones. |
| A.11.2.6 | Seguridad de equipos y activos fuera de las instalaciones. | Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de, teniendo en cuenta los diferentes riesgos de trabajar fuera las mismas. | Implementado<br>SI / NO / PARCIALMENTE<br>Se encuentran aplicados controles de seguridad, contra programas maliciosos, y control de acceso a internet, sin embargo no existen métodos de protección contra fuga de información. |
| 11.2 Equipos | | | |
| Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. | | | |
| A.11.2.7 | Disposición segura o reutilización de equipos. | Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización. | Implementado<br>SI / NO / PARCIALMENTE<br>Se realiza un proceso de restauración a valores de fábrica, para verificar que cualquier dato sensible o software con licencia es retirado o sobrescrito en forma segura, sin embargo no existe un procedimiento formal para este proceso. |
| A.11.2.8 | Equipos de usuario desatendidos. | Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada. | Implementado<br>SI / NO / PARCIALMENTE<br>No se cuenta con procedimiento para asegurar que los equipos desatendidos se les de protección apropiada, o un proceso de capacitación, para los usuarios, que indique las mejores prácticas que deben tener en cuenta. |

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| A.11.2.9 | Política de escritorio limpio y pantalla limpia. | Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No existe política de escritorio limpio y pantalla limpia, o un proceso de capacitación, para los usuarios, que indique las mejores prácticas que deben tener en cuenta. | | |
| A.12 Seguridad de las operaciones | | | | | |
| 12.1 Procedimientos operacionales y responsabilidades | | | | | |
| Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. | | | | | |
| A.12.1.1 | Procedimientos de operación documentados | Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se encuentran documentados y puestos a disposición de los usuarios los procedimientos de operación existentes en el área, para facilitar el flujo de los procesos. | | |
| A.12.1.2 | Gestión de cambios | Control: Se deberían 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. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No existe un proceso de gestión controle los cambios en los procesos, las instalaciones y los sistemas de procesamiento de información, en el área. | | |
| A.12.1.3 | Gestión de capacidad | Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | En el área se realizan el seguimiento al uso de recursos, y control de los mismos, con el fin de identificar cuando es necesario realizar ajustes para cumplir con los requisitos de capacidad futura, y optimizar los recursos del área. | | |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">12.1 Procedimientos operacionales y responsabilidades</td></tr>
<tr><td colspan="4">Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.</td></tr>
<tr><td rowspan="3">A.12.1.4</td><td rowspan="3">Separación de los ambientes de desarrollo, pruebas y operación</td><td rowspan="3">Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se cuenta con separación de ambientes en los sistemas de información core para el negocio, administrados por el área.</td></tr>
<tr><td colspan="4">12.2 Protección contra códigos maliciosos</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</td></tr>
<tr><td rowspan="3">A.12.2.1</td><td rowspan="3">Controles contra códigos maliciosos.</td><td rowspan="3">Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se cuenta con un servicio de antivirus contratado para los computadores corporativos, mediante el cual se logra identificar y bloquear códigos maliciosos, sin embargo no existe un plan de educación para los usuarios.</td></tr>
<tr><td colspan="4">12.3 Copias de respaldo</td></tr>
<tr><td colspan="4">Objetivo: Proteger contra la perdida de datos</td></tr>
<tr><td rowspan="3">A.12.3.1</td><td rowspan="3">Respaldo de información.</td><td rowspan="3">Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de respaldo.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se realizan periódicamente copias de seguridad de los sistemas y aplicaciones más importantes para la continuidad del negocio, sin embargo no se realizan pruebas periódicas de los mismos.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| 12.4 Registro y seguimiento | | | |
| Objetivo: Registrar eventos y generar evidencia | | | |
| A.12.4.1 | 1 Registro de eventos. | Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | Implementado<br>SI \| NO \| PARCIALMENTE<br>Se realiza la conservación de logs para eventos críticos, en los sistemas de información críticos para el negocio, sin embargo la revisión se realiza por demanda |
| A.12.4.2 | Protección de la información de registro. | Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado. | Implementado<br>SI \| NO \| PARCIALMENTE<br>Se cuenta con controles de autenticación en los sistemas de información críticos para el negocio, con la finalidad de evitar accesos no autorizados |
| A.12.4.3 | Registros del administrador y del operador. | Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad. | Implementado<br>SI \| NO \| PARCIALMENTE<br>No se registran las actividades de los administradores de los sistemas de información. |
| A.12.4.4 | Sincronización de relojes. | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo. | Implementado<br>SI \| NO \| PARCIALMENTE<br>Los relojes de los sistemas de información críticos, se encuentran sincronizados de acuerdo con el servidor de hora legal Colombia, sin embargo no hay una política que exija esto. |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">12.5 Control de software operacional</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la integridad de los sistemas operacionales.</td></tr>
<tr><td rowspan="3">A.12.5.1</td><td rowspan="3">Instalación de software en sistemas operativos.</td><td rowspan="3">Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>La instalación de software en los sistemas operativos está limitada al personal de soporte de la organización, los usuarios no cuentan con los permisos necesarios para la instalación de ningún software, y para cualquier instalación se debe solicitar autorización de los administradores de acuerdo a los procedimientos instaurados por la gerencia de tics.</td></tr>
<tr><td colspan="4">12.6 Gestión de la vulnerabilidad técnica</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas</td></tr>
<tr><td rowspan="3">A.12.6.1</td><td rowspan="3">Gestión de las vulnerabilidades técnicas.</td><td rowspan="3">Control: Se debería 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.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se realizan evaluaciones oportunamente con respecto a las vulnerabilidades técnicas de los sistemas de información usados.</td></tr>
<tr><td colspan="4">12.6 Gestión de la vulnerabilidad técnica</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas</td></tr>
<tr><td rowspan="3">A.12.6.2</td><td rowspan="3">Restricciones sobre la instalación de software.</td><td rowspan="3">Control: Restricciones sobre la instalación de software.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>La instalación de software en los sistemas operativos está limitada al personal de soporte de la organización, de acuerdo a los lineamientos estipulados por la gerencia de tics. Los usuarios no cuentan con los permisos necesarios para la instalación de ningún software, y para cualquier instalación se debe solicitar autorización de los administradores, por medio de la mesa de servicios.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">12.7 Consideraciones sobre auditorías de sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.</td></tr>
<tr><td rowspan="3">A.12.7.1</td><td rowspan="3">Información controles de auditoría de sistemas</td><td rowspan="3">Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Existe un área de auditoría dentro de la organización, que verifica los diferentes procesos del área, sin embargo no se realizan verificaciones técnicas sobre los sistemas de información, que puedan identificar las vulnerabilidad de los mismos, para realizar el respectivo análisis, mediante el cual se tomen las acciones necesarias para la disminución del riesgo.</td></tr>
<tr><td colspan="4">13. Seguridad de las comunicaciones</td></tr>
<tr><td colspan="4">13.1 Gestión de la seguridad de las redes</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte</td></tr>
<tr><td rowspan="3">A.13.1.1</td><td rowspan="3">Controles de redes.</td><td rowspan="3">Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se realiza control de la infraestructura de redes de la compañía, con apoyo de varios proveedores, especializados, que operan bajo la supervisión de la jefatura de redes y comunicaciones, teniendo en cuenta los acuerdos de servicios establecidos para garantizar la operación.</td></tr>
<tr><td rowspan="3">A.13.1.2</td><td rowspan="3">Seguridad de los servicios de red.</td><td rowspan="3">Control: Se deberían 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 servicios de red, ya sea propios o contratados.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se encuentran identificados mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red, y se encuentran estipulados dentro de los contratos con los diferentes proveedores.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.13.1.3 | Separación en las redes. | Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes. | Implementado<br>SI / NO / PARCIALMENTE<br>Se encuentran segmentadas las redes de usuarios, servicios y sistemas, y filtradas por FW, para restringir el tráfico en cada una de las zonas, y evitar accesos no autorizados a los sistemas de información. |
| 13.2 Transferencia de información | | | |
| Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa | | | |
| A.13.2.1 | Políticas y procedimientos de transferencia de información. | Control: Se debería contar con políticas, procedimientos y controles para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. | Implementado<br>SI / NO / PARCIALMENTE<br>En el área no se cuenta con una política o procedimientos de transferencia de información. |
| A.13.2.2 | Acuerdos sobre transferencia de información | Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio. | Implementado<br>SI / NO / PARCIALMENTE<br>Se incluyen cláusulas en los contratos con proveedores del área, para exigir controles que permitan garantizar la transferencia segura de información del negocio. |
| A.13.2.3 | Mensajería electrónica | Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica. | Implementado<br>SI / NO / PARCIALMENTE<br>No se cuenta con procesos que permitan proteger la información enviada por medio del correo electrónico. |
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación. | Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad que reflejen las necesidades de la organización para la protección de la información. | Implementado<br>SI / NO / PARCIALMENTE<br>No se tienen identificados, revisados o documentados los requisitos para los acuerdos de confidencialidad. |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">14 Adquisición, desarrollo y mantenimientos de sistemas</td></tr>
<tr><td colspan="4">14.1 Requisitos de seguridad de los sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.</td></tr>
<tr><td rowspan="3">A.14.1.1</td><td rowspan="3">Análisis y especificación de requisitos de seguridad de la información</td><td rowspan="3">Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se incluyen requisitos de seguridad de la información en los requisitos de nuevos sistemas de información, o mejoras de los sistemas existentes, sin embargo no existe un procedimiento estipulado.</td></tr>
<tr><td rowspan="3">A.14.1.2</td><td rowspan="3">Seguridad de servicios de las aplicaciones en redes publicas</td><td rowspan="3">Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, divulgación y modificación no autorizadas.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se cuenta con un control para garantizar la protección de los servicios de aplicaciones que pasan sobre redes públicas.</td></tr>
<tr><td rowspan="3">A.14.1.3</td><td rowspan="3">Protección de transacciones de los servicios de las aplicaciones.</td><td rowspan="3">Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación de mensajes no autorizada.</td><td>Implementado</td></tr>
<tr><td>NO APLICA</td></tr>
<tr><td>El área de IT no realiza labores de desarrollo.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">14.2 Seguridad en los procesos de desarrollo y soporte</td></tr>
<tr><td colspan="4">Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</td></tr>
<tr><td rowspan="3">A.14.2.1</td><td rowspan="3">Política de desarrollo seguro.</td><td rowspan="3">Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>No se realizan desarrollos de software en el área.</td></tr>
<tr><td rowspan="3">A.14.2.2</td><td rowspan="3">Procedimientos de control de cambios en sistemas.</td><td rowspan="3">Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Existe un proceso de control de cambios para los sistemas core de la compañía.</td></tr>
<tr><td rowspan="3">A.14.2.3</td><td rowspan="3">Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.</td><td rowspan="3">Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>Se realizan pruebas al ejecutar cambios sobre los sistemas de información de los cuales es responsable el área.</td></tr>
<tr><td rowspan="3">A.14.2.4</td><td rowspan="3">Restricciones en los cambios a los paquetes de software.</td><td rowspan="3">Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.</td><td>Implementado<br>SI | NO | PARCIALMENTE<br>El área no realiza modificaciones sobre paquetes de software.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| 14.2 Seguridad en los procesos de desarrollo y soporte | | | | | |
| Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. | | | | | |
| A.14.2.5 | Principios de construcción de sistemas seguros. | Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | El área no realiza tareas de construcción de sistemas. | | |
| A.14.2.6 | Ambiente de desarrollo seguro. | Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se realizan desarrollos de software en el área. | | |
| A.14.2.7 | Desarrollo contratado externamente | Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externa mente. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se realizan desarrollos de software en el área. | | |
| A.14.2.8 | Pruebas de seguridad de sistemas | Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se realizan desarrollos de software en el área. | | |
| A.14.2.9 | Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, y actualizaciones se deben establecer pruebas y criterios de aceptación relacionados. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se establecen pruebas y criterios de aceptación, antes de iniciar el proceso de compra. | | |

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">14.3 Datos de Prueba</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los datos usados para pruebas.</td></tr>
<tr><td rowspan="3">A.14.3.1</td><td rowspan="3">Protección de datos de prueba.</td><td rowspan="3">Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se realizan desarrollos de software en el área de IT.</td></tr>
<tr><td colspan="4">15. Relación con los proveedores</td></tr>
<tr><td colspan="4">15.1 Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</td></tr>
<tr><td rowspan="3">A.15.1.1</td><td rowspan="3">Política de seguridad de la información para las relaciones con proveedores.</td><td rowspan="3">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 deberían acordar con estos y se deberían documentar.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se tienen definida una política por parte de la organización, que indique que lineamientos de seguridad deben ser de cumplimiento obligatorio para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.</td></tr>
<tr><td rowspan="3">A.15.1.2</td><td rowspan="3">Tratamiento de la seguridad dentro de los acuerdos con proveedores.</td><td rowspan="3">Control: Se deberían 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.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se tienen claros los requisitos de seguridad de la información que deben cumplir los proveedores.</td></tr>
<tr><td colspan="4">15. Relación con los proveedores</td></tr>
<tr><td colspan="4">15.1 Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</td></tr>
<tr><td rowspan="3">A.15.1.3</td><td rowspan="3">Cadena de suministro de tecnología de información y comunicación.</td><td rowspan="3">Control: Los acuerdos con proveedores deberían 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.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se incluyen requisitos para el tratamiento de riesgos de seguridad de la información, asociada con la cadena de suministro de productos y servicios de tecnología de información y comunicaciones.</td></tr>
</table>

**Cuadro 1. (Continuación)**

<table>
<tr><td colspan="4">15.2 Gestión de la prestación de servicios con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.</td></tr>
<tr><td rowspan="3">A.15.2.1</td><td rowspan="3">Seguimiento y revisión de los servicios de los proveedores.</td><td rowspan="3">Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se realiza supervisión y seguimiento periódico a la prestación de servicios de los proveedores, sin embargo no se encuentra definido un procedimiento formal.</td></tr>
<tr><td rowspan="3">A.15.2.2</td><td rowspan="3">Gestión de cambios en los servicios de proveedores.</td><td rowspan="3">Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>Se realiza un proceso de gestión de cambios en los servicios prestados por los proveedores.</td></tr>
<tr><td colspan="4">16. Gestión de incidentes de seguridad de la información</td></tr>
<tr><td colspan="4">16.1 Gestión de incidentes y mejoras en la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información.</td></tr>
<tr><td rowspan="3">A.16.1.1</td><td rowspan="3">Responsabilidad y procedimientos.</td><td rowspan="3">Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se encuentran establecidos los procedimientos de respuesta a incidentes de seguridad de la información, que permitan una respuesta oportuna para disminuir el impacto del negocio.</td></tr>
<tr><td rowspan="3">A.16.1.2</td><td rowspan="3">Reporte de eventos de seguridad de la información.</td><td rowspan="3">Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.</td><td>Implementado</td></tr>
<tr><td>SI | NO | PARCIALMENTE</td></tr>
<tr><td>No se cuenta con la capacitación y concientización suficiente o procedimientos que permitan la identificación y notificación de incidentes de seguridad de la información, por parte de los usuarios.</td></tr>
</table>

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| A.16.1.3 | Reporte de debilidades de seguridad de la información. | Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se cuenta con procedimientos de notificación de incidentes de seguridad de la información. | | |
| 16. Gestión de incidentes de seguridad de la información | | | | | |
| 16.1 Gestión de incidentes y mejoras en la seguridad de la información | | | | | |
| Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades | | | | | |
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se cuenta con un proceso de evaluación de eventos que permita clasificarlos como incidentes de seguridad de la información. | | |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información. | Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se cuenta con procedimientos de respuesta a incidentes de seguridad de la información. | | |
| A.16.1.6 | 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 debería usar para reducir la posibilidad o el impacto de incidentes futuros. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se cuenta con procedimientos de respuesta a incidentes de seguridad de la información. | | |

**Cuadro 1. (Continuación)**

| | | | |
|---|---|---|---|
| A.16.1.7 | Recolección de evidencia. | Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. | Implementado<br>SI / NO / PARCIALMENTE<br>No se cuenta con procedimientos de respuesta a incidentes de seguridad de la información. |
| 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio | | | |
| 17.1 Continuidad de seguridad de la información | | | |
| Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización | | | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información. | Control: La organización debería 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. | Implementado<br>SI / NO / PARCIALMENTE<br>No se encuentran definidos los requisitos para la seguridad de la información y la continuidad de la seguridad de la información en situaciones adversas. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información. | Control: La organización debería 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. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe planificación para la seguridad de la información durante situaciones adversas. |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | Control: La organización debería 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. | Implementado<br>SI / NO / PARCIALMENTE<br>No existe planificación para la seguridad de la información durante situaciones adversas. |

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| 17.2 Redundancias | | | | | |
| Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información. | | | | | |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se cuenta con sistemas redundantes ubicados en diferentes posiciones geográficas, garantizando la continuidad de los servicios y más importantes para el área de IT, y la operación del negocio. | | |
| 18. Cumplimiento | | | | | |
| 18.1 Cumplimiento de requisitos legales y contractuales | | | | | |
| Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad. | | | | | |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales. | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Este proceso es realizado por el área jurídica de la, quien garantiza el cumplimiento de los reglamentos legales aplicables a la compañía. | | |
| 18. Cumplimiento | | | | | |
| 18.1 Cumplimiento de requisitos legales y contractuales | | | | | |
| Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad. | | | | | |
| A.18.1.2 | Derechos de propiedad intelectual. | Control: Se deberían 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. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Este proceso es realizado por el área jurídica de la compañía. | | |

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| A.18.1.3 | Protección de registros. | Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación contractuales. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se realiza protección de registros. | | |
| A.18.1.4 | Privacidad y protección de información de datos personales | Se debe asegurar la privacidad y la protección de la información de datos personales como se exige en la legislación. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No se encuentra definida las medidas de protección de datos personales. | | |
| A.18.1.5 | Reglamentación de controles criptográficos. | Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | Se usan los controles necesarios de acuerdo con el tipo de empresa | | |
| 18.2 Revisiones de seguridad de la información | | | | | |
| Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales. | | | | | |
| A.18.2.1 | 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 deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | Implementado | | |
| | | | SI | NO | |
| | | | No existen objetivos de control, controles, políticas, procesos y procedimientos documentados para la seguridad de la información. | | |

**Cuadro 1. (Continuación)**

| | | | | | |
|---|---|---|---|---|---|
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad. | Control: Los directores deberían 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. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No existen objetivos de control, controles, políticas, procesos y procedimientos documentados para la seguridad de la información. | | |
| A.18.2.3 | Revisión del cumplimiento técnico. | Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | Implementado | | |
| | | | SI | NO | PARCIALMENTE |
| | | | No existen objetivos de control, controles, políticas, procesos y procedimientos documentados para la seguridad. | | |

Fuente. Los Autores

En el Cuadro 2 se puede observar el consolidado con los porcentajes de cumplimiento, el total de controles implementados es de un 34.7%, existiendo dominios para los cuales no hay controles, lo que representa grandes riesgos de seguridad para la información manejada por el área de IT en ALFAGRES S.A.

**Cuadro 2. Cumplimiento en seguridad de la información**

| Dominio de control | Cumplimiento por dominio | Número de controles | Total Porcentaje de Cumplimiento |
|---|---|---|---|
| A5. Políticas de la seguridad de la información | 0 | 2 | 0 |
| A6. Organización de la seguridad de la información | 35,7 | 7 | 2,2 |
| A7. Seguridad de los recursos humanos | 16,7 | 6 | 0,9 |
| A8. Gestión de activos | 10 | 10 | 0,9 |
| A9. Control de acceso | 53,6 | 14 | 6,6 |
| A10. Criptografía | 0 | 2 | 0 |
| A11. Seguridad física y del entorno | 56,7 | 15 | 7,5 |
| A12. Seguridad de las operaciones | 67,9 | 14 | 8,3 |
| A13. Seguridad de las comunicaciones | 50 | 7 | 3,1 |
| A14. Adquisición, desarrollo y mantenimiento de sistemas | 26,9 | 13 | 3,1 |
| A15. Relación con los proveedores | 30 | 5 | 1,3 |
| A16. gestión de incidentes de seguridad de información | 0 | 7 | 0 |
| A17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio | 25 | 4 | 0,9 |
| A18. Revisión de seguridad de la información | 0,4 | 8 | 0 |
| **Totales** | | **114** | **34,7** |

Fuente. Los Autores

# 6. ACTIVOS DE INFORMACIÓN

Los activos de información son de alta importancia para la organización ya que tienen un valor alto y que por lo tanto requiere de la protección necesaria y adecuada evitando consecuencias negativas que pueden ser generadas por parte de personas mal intencionadas. El inventario de activos de información es una parte fundamental del diseño de un SGSI, permitiendo clasificar los activos a los que se debe brindar una mayor protección de acuerdo con las características del mismo, y el rol al interior de un proceso.

De acuerdo con la normativa ISO27005 el primer paso para la elaboración del inventario de activos es la identificación de los activos primarios, y los activos de soporte ligados al alcance definido, teniendo en cuenta las siguientes definiciones:

- Activos primarios según la norma ISO27005: son los procesos y la información central de la actividad en el alcance.

- Activos de soporte: Elementos de procesamiento de información, los cuales, al ser vulnerados, pueden deteriorar los activos primarios del alcance. Los activos de soporte se pueden clasificar como: hardware, software, redes, personal, sitio, organización, entre otros[15].

## 6.1 IDENTIFICACIÓN DE ACTIVOS PRIMARIOS

La actividad de identificación de los activos primarios se centra en la información, actividades y procesos o subprocesos del negocio. Esta identificación es realizada por un grupo de trabajo mixto que representa al proceso (directores, especialistas en sistema de información y usuarios).

## 6.2 IDENTIFICACIÓN DE ACTIVOS SOPORTE

Los activos de soporte tienen vulnerabilidades que son explotables por las amenazas cuya meta es deteriorar los activos primarios del alcance (procesos e información). Entre los activos de soporte de identifica el recurso humano que son todas las personas involucradas con los sistemas de información, como usuarios que tienen ciertos tipos de accesos a los sistemas para realizar sus actividades diarias. Los directores de la organización o de un proyecto específico y los propietarios son las personas a cargo de tomar decisiones

[15] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. p. 13.

## 6.3 INVENTARIO DE ACTIVOS

La actividad de la clasificación de los activos se representa con el modelo propuesto en el Cuadro 3, y así documentar el inventario de los activos de información para el área de infraestructura tecnológica de ALFAGRES S.A, con ayuda de los líderes del área en mención, a continuación, se realiza una descripción sobre la información contenida en cada una de las columnas del Cuadro 3:

- ID: código establecido para la identificación y etiquetado de los activos de información.

- Proceso: relación del activo identificado con el proceso al que pertenece.

- Activo: nombre definido para la identificación del recurso de información.

- Responsable: persona o área encargada del activo de información.

- Tipo: clasificación de acuerdo con las características del activo, puede ser de hardware, información, organización, personal, proceso, red, sitio, software.

- Descripción y observaciones: breve reseña de las características y componentes del activo de información.

**Cuadro 3. Inventario de activos de información**

| ID | Proceso | Activo | Responsable | Tipo | Descripción y observaciones |
|---|---|---|---|---|---|
| ALFAAI1 | Operación | Teléfonos celulares | Analista de telecomunicaciones | Hardware de usuario final | Equipos celulares suministrados a los colaboradores, para garantizar la comunicación efectiva y el correcto desempeño de sus labores. |
| ALFAAI2 | Soporte / operación | Teléfonos IP | Analista de telecomunicaciones | Hardware de usuario final | Dispositivos asignados a los colaboradores para facilitar la comunicación al interior de la organización. |
| ALFAAI3 | Operación / seguridad y continuidad | Firewalls | Analista de telecomunicaciones | Hardware de infraestructura | Dispositivos adquiridos por la compañía para garantizar el acceso a internet de manera segura. |
| ALFAAI4 | Operación | Switches | Analista de telecomunicaciones | Hardware de infraestructura | Dispositivos adquiridos por la compañía para garantizar el acceso de sus colaboradores a la red corporativa. |
| ALFAAI5 | Operación | Access Point | Analista de telecomunicaciones | Hardware de infraestructura | Dispositivos adquiridos por la compañía, para garantizar el acceso inalámbrico de los colaboradores a la red corporativa. |
| ALFAAI6 | Soporte/ operación/ seguridad y continuidad | Equipos de cómputo | Analista de infraestructura | Hardware de usuario final | Todo equipo de cómputo suministrado por la organización a sus colaboradores para el desempeño de sus labores. |
| ALFAAI7 | Operación | Tabletas | Analista de infraestructura | Hardware de usuario final | Dispositivos móviles proporcionados por la compañía a los colaboradores que ejecutan labores con un alto grado de movilidad. |
| ALFAAI8 | Operación | Impresoras | Analista de infraestructura | Hardware de infraestructura | Dispositivos de impresión adquiridos por la compañía en calidad de servicio. |
| ALFAAI9 | Operación | Scanner | Analista de infraestructura | Hardware de infraestructura | Dispositivos adquiridos por la compañía para la digitalización de documentos. |
| ALFAAI10 | Operación | Servidores corporativos | Analista de infraestructura | Hardware de infraestructura | Equipos físicos necesarios para la administración de servicios de directorio activo y aplicaciones corporativas |

**Cuadro 3. (Continuación)**

| ID | Proceso | Activo | Responsable | Tipo | Descripción y observaciones |
|---|---|---|---|---|---|
| ALFAAI11 | Soporte / operación | IBM | Analista de infraestructura | Organización | Proveedor de apoyo y soporte para el servicio de SAP dentro de la empresa. |
| ALFAAI12 | Soporte / operación/ proyectos | Telefónica | Jefe de redes y comunicaciones | Organización | Proveedor de apoyo para el soporte y operación de las redes y comunicaciones de la empresa. |
| ALFAAI13 | Soporte / proyectos | Neiser comunicaciones | Analista de telecomunicaciones | Organización | Proveedor de apoyo en proyectos de redes y comunicaciones. |
| ALFAAI14 | Soporte/ seguridad y continuidad | ACG of Américas | Analista de telecomunicaciones | Organización | Proveedor de apoyo para soportar y operación del servicio de seguridad de host en la empresa. |
| ALFAAI15 | Soporte/ seguridad y continuidad/ proyectos | 360 Security group | Analista de telecomunicaciones | Organización | Proveedor de apoyo para el soporte y operación del servicio de seguridad perimetral en la empresa. |
| ALFAAI16 | Soporte / operación/ proyectos | MCO Global | Analista de telecomunicaciones | Organización | Proveedor de apoyo para el soporte y operación de las redes y comunicaciones de la empresa. |
| ALFAAI17 | Soporte / operación/ proyectos | Walter Bridge | Analista de telecomunicaciones | Organización | Proveedor de apoyo para el soporte y operación de las redes y comunicaciones de la empresa. |
| ALFAAI18 | soporte / operación/ proyectos | Prointech | Analista de infraestructura | Organización | Proveedor de apoyo para el soporte y operación del servicio de impresión en la empresa. |
| ALFAAI19 | operación | Milenio PC | Analista de infraestructura | Organización | Proveedor de apoyo para el alquiler de equipos de cómputo. |
| ALFAAI20 | Soporte/ Operación/ seguridad y continuidad | Xertical labs | Analista de infraestructura | Organización | Proveedor de apoyo y soporte para el servicio de correo electrónico en la empresa. |

**Cuadro 3. (Continuación)**

| ID | Proceso | Activo | Responsable | Tipo | Descripción y observaciones |
|---|---|---|---|---|---|
| ALFAAI21 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Soluciones .net | Analista de infraestructura | Organización | Proveedor de apoyo y soporte para la administración de servidores Windows en la empresa. |
| ALFAAI22 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Jefe de redes y comunicaciones | Gerente de Tics | Personal | Encargado de la operación de las redes de comunicaciones en la empresa. |
| ALFAAI23 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Jefe de infraestructura | Gerente de Tics | Personal | Encargado de la operación de la infraestructura de tecnología en la empresa. |
| ALFAAI24 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Analista de infraestructura | Jefe de infraestructura | Personal | Encargado del soporte de la infraestructura de Tics en la empresa. |
| ALFAAI25 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Analista de telecomunicaciones | Jefe de redes y comunicaciones | Personal | Encargado del soporte de redes y comunicaciones en la empresa. |
| ALFAAI26 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Gerente de Tics | VP financiera | Personal | Encargado de la operación y gestión de recursos para el área de Tics. |

**Cuadro 3. (Continuación)**

| ID | Proceso | Activo | Responsable | Tipo | Descripción y observaciones |
|---|---|---|---|---|---|
| ALFAAI27 | Soporte | Administración de servicios de soporte | Gerente de Tics | Proceso | Brindar soporte y gestión al usuario final sobre la infraestructura y sistemas de información que apalancan las operaciones de las unidades de negocio del grupo empresarial ALFA. |
| ALFAAI28 | Operación | Administración de servicios de operación | Gerente de Tics | Proceso | Asegurar la disponibilidad de la infraestructura de tecnología para garantizar la continuidad de las operaciones en las unidades de negocio del grupo empresarial ALFA. |
| ALFAAI29 | seguridad y continuidad | Administración de seguridad y continuidad | Gerente de Tics | Proceso | Mantener un conjunto de planes de continuidad, mantenimiento y seguridad informática de los servicios de Tics. |
| ALFAAI30 | Proyectos | Administración de soporte de proyectos | Gerente de Tics | Proceso | Proponer y liderar técnicamente proyectos de mejora e innovación que permitan potenciar el conocimiento y el uso de los sistemas de información en las unidades de negocio del grupo empresarial ALFA. |
| ALFAAI31 | Operación | Red WIFI | Analista de telecomunicaciones | Red | Redes WIFI proporcionadas por la compañía para que sus colaboradores puedan tener acceso tanto a la red corporativa como a internet. |
| ALFAAI32 | Operación | Red MPLS | Analista de telecomunicaciones | Red | Infraestructura adquirida por la compañía para comunicar las diferentes sedes nacionalmente. |
| ALFAAI33 | Operación | Canales de Internet | Analista de telecomunicaciones | Red | Infraestructura adquirida por la compañía, para el acceso a la red pública. |
| ALFAAI34 | Operación | Cableado estructurado | Analista de telecomunicaciones | Red | Infraestructura adquirida por la compañía, para garantizar la conexión de usuarios a los diferentes servicios de red. |

**Cuadro 3. (Continuación)**

| ID | Proceso | Activo | Responsable | Tipo | Descripción y observaciones |
|---|---|---|---|---|---|
| ALFAAI35 | Operación | Centros de cómputo | Jefe de redes y comunicaciones | Hardware | Lugares definidos por la organización, para la instalación de la infraestructura de redes y procesamiento de datos. |
| ALFAAI36 | Operación | Zonas de almacenamiento | Jefe de redes y comunicaciones | Sitio | Lugares definidos por la organización, para el almacenamiento de equipos. |
| ALFAAI37 | Operación | Sistemas operativos | Analista de infraestructura | Software | Sistemas operativos usados por la compañía, en los equipos de cómputo y servidores. |
| ALFAAI38 | Operación | SAP | Analista de infraestructura | Software | Sistema de información adquirido por la compañía, para el apoyo de los procesos de la compañía |
| ALFAAI39 | Operación | Correo electrónico | Analista de infraestructura | Software | Servicio adquirido por la compañía para facilitar la comunicación entre colaboradores, clientes y proveedores. |
| ALFAAI40 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Información estratégica del negocio | Gerente de Tics | Información | Información del negocio entregada al área de Tics, para lograr cumplir con los objetivos del negocio |
| ALFAAI41 | Soporte/ Operación/ seguridad y continuidad/ proyectos | Información Personal de colaboradores y clientes de la compañía | Gerente de Tics | Información | Información de personas naturales, que tienen vínculos laborales o comerciales con la compañía. |

Fuente. Los Autores

## 6.4 VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Por medio de la valoración de los activos de información, se pretende tabular el nivel de impacto que se presentaría en la organización, en el caso de que uno de los activos identificados para el área de infraestructura tecnológica de ALFAGRES S.A, pierda su propiedad de confidencialidad, integridad o disponibilidad. Para cada propiedad se establecieron criterios específicos y lineamientos que permiten otorgar una clasificación.

En los Cuadros 4, 5, y 6, se puede observar los niveles de clasificación para cada uno de los atributos de la seguridad de la información, como se puede observar; existen 3 criterios identificados como baja, media y alta, que permiten determinar el valor de cada activo.

Según la ISO 27000, "el principio de confidencialidad se refiere a la propiedad de la información, que pretende garantizar el acceso a la misma, únicamente de las personas o sistemas autorizados"[16]. Para ALFAGRES S.A. existe información cuyo criterio de confidencialidad, es muy alto, debido a que la misma, hace parte de las estrategias comerciales trazadas por la compañía, para el cumplimiento de sus objetivos.

**Cuadro 4. Valoración de activos según la confidencialidad**

| Atributo | Criterio | Valor | Descripción |
|---|---|---|---|
| **Confidencialidad** | Alta | 3 | Todo activo que, al ser accedido o divulgado sin autorización, afecte los procesos de la organización o la imagen de la compañía, colaboradores y clientes. |
| | Media | 2 | Todo activo que, al ser accedido o divulgado sin autorización, dificulta la ejecución de los procesos de la organización sin afectar la imagen de la organización, colaboradores o clientes. |
| | Baja | 1 | Todo activo que, al ser accedido o divulgado sin autorización, no afecta los procesos de la organización, colaboradores y clientes |

Fuente. Los Autores

La integridad es un atributo de la información, muy importante, ya que sin este no sería posible la comunicación y la toma de decisiones para la compañía. Por esto es vital mantener la exactitud y completitud en todo el ciclo de vida de la información.

[16] PORTAL ISO 27000. Introducción a los sistemas de gestión de seguridad de la información. [en línea]. Madrid: ISO 27000, 2010 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

**Cuadro 5. Referencia para la valoración de activos según la integridad**

| Atributo | Criterio | Valor | Descripción |
|---|---|---|---|
| **Integridad** | Alta | 3 | El daño o modificación del activo afecta totalmente los procesos de la organización y el impacto en la empresa es importante, puede conllevar a falla total del negocio. |
| | Media | 2 | El daño o modificación del activo afecta parcialmente los procesos de la organización. |
| | Baja | 1 | El daño o modificación del activo, no afecta los procesos de la organización y el impacto en la empresa es insignificante o menor. |

Fuente. Los Autores

Según la ISO 27000, "la disponibilidad es la propiedad de la información, que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad, o proceso autorizado, cuando así lo requiera, al igual que los recursos necesarios para su uso"[17]. Para el área de infraestructura tecnológica de ALFAGRES S.A, este atributo de la información es uno de los más relevantes, ya que la compañía requiere para su operación diaria.

**Cuadro 6. Referencia para la valoración de activos según la disponibilidad**

| Atributo | Criterio | Valor | Descripción |
|---|---|---|---|
| **Disponibilidad** | Alta | 3 | No se puede tolerar que el activo de información no esté disponible por una hora o menos |
| | Media | 2 | Se puede tolerar que el activo información no esté disponible entre 1 y 12 horas. |
| | Baja | 1 | Se puede tolerar que el activo información no esté disponible por más de un día |

Fuente. Los Autores

Al valorar cada uno de los activos, con respecto a la criticidad de los atributos de la seguridad de la información, se obtendría un puntaje total que puede estar entre 3 y 9, de acuerdo con el valor total ponderado, se clasificara cada uno de los activos tal y como se ve en el Cuadro 7.

[17] PORTAL ISO 27000. Introducción a los sistemas de gestión de seguridad de la información. [en línea]. Madrid: ISO 27000, 2010 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

**Cuadro 7. Niveles de valoración del activo**

| | Criterio | Valor | Descripción |
|---|---|---|---|
| **Valor del activo** | Alta | 7-9 | La suma de la valoración parcial de los atributos de seguridad de la información debe estar entre 7 y 9. |
| | Media | 5-6 | La suma de la valoración parcial de los atributos de seguridad de la información debe estar entre 5 y 6. |
| | Baja | 3-4 | La suma de la valoración parcial de los atributos de seguridad de la información debe estar entre 3 y 4. |

Fuente. Los Autores.

En el Cuadro 8, se presenta el resultado de la valoración de los activos, otorgando una valoración cualitativa, según la criticidad de la confidencialidad, integridad y disponibilidad, con estos tres valores es posible obtener un nivel total de criticidad para el activo, y así direccionar los esfuerzos y recursos de la organización en mitigar los riesgos para los activos más críticos.

**Cuadro 8. Valoración para activos de información**

| ID | Activo | Responsable | Tipo | Confidencialidad | Integridad | Disponibilidad | Nivel de criticidad | Criticidad del activo |
|---|---|---|---|---|---|---|---|---|
| ALFAAI1 | Teléfonos celulares | Analista de telecomunicaciones | Hardware de usuario final | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI2 | Teléfonos IP | Analista de telecomunicaciones | Hardware de usuario final | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI3 | Firewalls | Analista de telecomunicaciones | Hardware de infraestructura | 2 | 3 | 3 | 8 | Alto |
| ALFAAI4 | Switches | Analista de telecomunicaciones | Hardware de infraestructura | 2 | 2 | 2 | 6 | Medio |
| ALFAAI5 | Access Point | Analista de telecomunicaciones | Hardware de infraestructura | 2 | 2 | 2 | 6 | Medio |
| ALFAAI6 | Equipos de cómputo | Analista de infraestructura | Hardware de usuario final | 2 | 2 | 1 | 5 | Medio |
| ALFAAI7 | Tabletas | Analista de infraestructura | Hardware de usuario final | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI8 | Impresoras | Analista de infraestructura | Hardware de infraestructura | 1 | 1 | 2 | 4 | Bajo |
| ALFAAI9 | Scanner | Analista de infraestructura | Hardware de infraestructura | 1 | 1 | 1 | 3 | Bajo |
| ALFAAI10 | Servidores corporativos | Analista de infraestructura | Hardware de infraestructura | 2 | 3 | 3 | 7 | Alto |
| ALFAAI11 | IBM | Analista de infraestructura | Organización | 2 | 3 | 3 | 8 | Alto |
| ALFAAI12 | Telefónica | Jefe de redes y comunicaciones | Organización | 2 | 2 | 3 | 7 | Alto |
| ALFAAI13 | Neiser | Analista de telecomunicaciones | Organización | 1 | 1 | 1 | 3 | Bajo |
| ALFAAI14 | ACG of Américas | Analista de telecomunicaciones | Organización | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI15 | 360 Security group | Analista de telecomunicaciones | Organización | 2 | 1 | 2 | 5 | Medio |
| ALFAAI16 | MCO Global | Analista de telecomunicaciones | Organización | 2 | 1 | 1 | 4 | Bajo |

**Cuadro 8. (Continuación)**

| ID | Activo | Responsable | Tipo | Confidencialidad | Integridad | Disponibilidad | Nivel de criticidad | Criticidad del activo |
|---|---|---|---|---|---|---|---|---|
| ALFAAI17 | Walter Bridge | Analista de telecomunicaciones | Organización | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI18 | Prointech | Analista de infraestructura | Organización | 1 | 1 | 1 | 3 | Bajo |
| ALFAAI19 | Milenio PC | Analista de infraestructura | Organización | 1 | 1 | 1 | 3 | Bajo |
| ALFAAI20 | Xertical Labs | Analista de infraestructura | Organización | 3 | 2 | 1 | 6 | Medio |
| ALFAAI21 | Soluciones .net | Analista de infraestructura | Organización | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI22 | Jefe de redes y comunicaciones | Gerente de Tics | Personal | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI23 | Jefe de infraestructura | Gerente de Tics | Personal | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI24 | Analista de infraestructura | Jefe de infraestructura | Personal | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI25 | Analista de telecomunicaciones | Jefe de redes y comunicaciones | Personal | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI26 | Gerente de Tics | VP financiera | Personal | 2 | 2 | 1 | 5 | Medio |
| ALFAAI27 | administración de servicios de soporte | Gerente de Tics | Proceso | 2 | 2 | 7 | 7 | Alto |
| ALFAAI28 | administración de servicios de operación | Gerente de Tics | Proceso | 2 | 2 | 3 | 7 | Alto |
| ALFAAI29 | administración de seguridad y continuidad | Gerente de Tics | Proceso | 3 | 3 | 2 | 8 | Alto |
| ALFAAI30 | administración de soporte de proyectos | Gerente de Tics | Proceso | 2 | 2 | 1 | 5 | Medio |

**Cuadro 8. (Continuación)**

| ID | Activo | Responsable | Tipo | Confidencialidad | Integridad | Disponibilidad | Nivel de criticidad | Criticidad del activo |
|---|---|---|---|---|---|---|---|---|
| ALFAAI31 | Red WIFI | Analista de telecomunicaciones | Red | 2 | 1 | 2 | 5 | Medio |
| ALFAAI32 | Red MPLS | Analista de telecomunicaciones | Red | 2 | 3 | 3 | 8 | Alto |
| ALFAAI33 | Canales de Internet | Analista de telecomunicaciones | Red | 2 | 1 | 3 | 6 | Medio |
| ALFAAI34 | Cableado estructurado | Analista de telecomunicaciones | Red | 2 | 1 | 1 | 4 | Bajo |
| ALFAAI35 | Centros de cómputo | Jefe de redes y comunicaciones | Sitio | 2 | 3 | 2 | 7 | Alto |
| ALFAAI36 | Zonas de almacenamiento | Jefe de redes y comunicaciones | Sitio | 1 | 1 | 1 | 3 | Bajo |
| ALFAAI37 | Sistemas operativos | Analista de infraestructura | Software | 2 | 2 | 2 | 6 | Medio |
| ALFAAI38 | SAP | Analista de infraestructura | Software | 3 | 3 | 3 | 9 | Alto |
| ALFAAI39 | Correo electrónico | Analista de infraestructura | Software | 3 | 3 | 3 | 9 | Alto |
| ALFAAI40 | Información estratégica del negocio | Gerente de Tics | Información | 3 | 3 | 2 | 8 | Alto |
| ALFAAI41 | Información Personal de colaboradores y clientes de la compañía | Gerente de Tics | Información | 3 | 3 | 2 | 8 | Alto |

Fuente. Los Autores

De acuerdo con la clasificación, se puede observar que 13 de los activos identificados para el área de infraestructura tecnológica de ALFAGRES S.A. son críticos para la operación de la compañía, por lo cual se deberían enfocar los recursos dispuestos por la organización, en la protección de los mismos, manteniendo un nivel de riesgo bajo y evitando afectar la operación del negocio.

# 7. ANÁLISIS DEL RIESGO

## 7.1 IDENTIFICACIÓN DE AMENAZAS

Las organizaciones se encuentran expuestas a diferentes tipos de amenazas que pueden afectar los activos o dañarlos totalmente, y así generar fallos en los procesos y la continuidad del negocio, hay que tener en cuenta que existen amenazas que pueden afectar más de un activo. Para esto se debe definir y aplicar un proceso para la identificación de amenazas y su respectivo análisis, que nos indique el impacto que puede causar a la organización la materialización de un escenario de incidente.

Para la identificación de amenazas, es importante la información que puedan aportar los propietarios y los usuarios de los activos de información y demás personas relacionadas, tratando de identificar antecedentes de eventos que hayan afectado la integridad, disponibilidad o confidencialidad de la información y el activo, acotando así las probables amenazas y sus orígenes.

Existen diferentes tipos de amenazas como deliberadas, accidentales y las ambientales o naturales, que se deben categorizar genéricamente o dependiendo su tipo, para ello es de vital importancia identificar su origen evitando que ninguna se pase por alto, ya que pueden tener diferentes orígenes. Hoy en día el factor humano es una de las fuentes de amenazas más altas, donde las organizaciones invierten más esfuerzo y recursos, para contrarrestar los impactos que pueden generar.

Posterior a las amenazas identificadas, se deben identificar el estado de madurez en que se encuentra la organización y así diseñar e implementar las contramedidas necesarias para disminuir la probabilidad de que las amenazas se materialicen y causen un impacto alto.

Como resultado de esta actividad se obtiene un listado de amenazas con la identificación del tipo y el origen de la misma. En el Cuadro 9 se puede observar el listado de amenazas para el área de infraestructura tecnológica de ALFAGRES S.A dicho cuadro fue elaborado con base en la norma ISO 27005 según la cual las amenazas pueden ser de tipo; accidental, ambiental o deliberada. Se pinta de color azul la columna correspondiente a los tipos, asociados para cada amenaza.

**Cuadro 9. Tipos de amenazas y orígenes**

| Tipo | Amenazas | Origen | | |
|---|---|---|---|---|
| | | Accidental | Ambiental | Deliberada |
| Acciones no autorizadas | Abuso de privilegios | | | |
| | Acceso no autorizado al sistema de información | | | |
| Amenazas humanas | Ataques de ingeniería social | | | |
| | Ataques de piratas informáticos | | | |
| | Espionaje industrial | | | |
| | Spam | | | |
| | Terrorismo | | | |
| Compromiso de información | Hurto de equipos | | | |
| | Interceptación de señales | | | |
| | Infección con software malicioso | | | |
| Compromiso de las funciones | Error en el uso de sistemas de información | | | |
| | Incumplimiento en el mantenimiento | | | |
| Daño físico | Fuego | | | |
| | Agua | | | |
| | Polvo, corrosión, golpes | | | |
| | Fluctuaciones de energía eléctrica | | | |
| Eventos naturales | Inundaciones | | | |
| | Terremotos | | | |
| Fallas técnicas | Mal funcionamiento del sistema de información | | | |
| | Falla de los equipos de telecomunicaciones | | | |
| | saturación del sistema de información | | | |
| Perdida de los Servicios esenciales | Pérdida del suministro de energía | | | |
| | Pérdida del suministro de ventilación | | | |

Fuente. Los Autores

## 7.2 IDENTIFICACIÓN DE LAS VULNERABILIDADES Y CONSECUENCIAS

Una vez se cuenta con el listado de amenazas conocidas, activos de información, y controles existentes, se procede con la identificación de las vulnerabilidades y consecuencias, con lo que se pretenden identificar las vulnerabilidades que pueden ser explotadas, y su posterior impacto en una o las tres variables de

seguridad de la información, para los activos primarios (procesos, información) definidos en el alcance del SGSI.

También se pueden identificar vulnerabilidades que no es necesario implementar contramedidas, debido a que no exista una amenaza que la pueda explotar, es decir, una vulnerabilidad que no tenga identificada una amenaza que se aproveche de ella no se puede identificar como un riesgo, pero se debe realizar un seguimiento adecuado, evitando que creen una amenaza que se pueda aprovechar y la pueda explotar causando un impacto alto.

Mediante la identificación de consecuencias de un evento, se busca establecer los daños ocasionados para la organización, en caso de que una de las vulnerabilidades existentes, sea explotada por una amenaza, generando un impacto alto, mediano o bajo dependiendo de los criterios establecidos en el contexto de la organización, generando perdida de reputación, condiciones adversas de operación, perdida de negocio, pérdida de eficacia, ó incumplimiento de obligaciones.

Las consecuencias se identifican de naturaleza temporal o permanente, donde se generan gastos en el tratamiento de incidentes, es decir si existe la solución de la falla de manera temporal, o si es de manera permanente la destrucción del activo. En la identificación de consecuencias encontramos tanto positivas como negativas.

El Cuadro 10 muestra las consecuencias que pueden llegar a tener lugar, si una vulnerabilidad existente en un activo llega a ser explotada por una amenaza, afectando así, el activo y procesos relacionados con el mismo. A continuación, se realiza una descripción de cada para los datos contenidos en cada una de las columnas del Cuadro 10.

- ID: código alfanumérico que representa el identificador asignado al activo, de acuerdo con el inventario de activos definido en el capítulo 6 del presente documento.

- Activo: es un recurso de la compañía, que interviene en el ciclo de vida de la información.

- Amenazas: es una situación que representa peligro para los recursos de la compañía.

- Vulnerabilidades: fallas o debilidades presentes en los activos de información, y que pueden ser explotadas por una amenaza.

- Consecuencias: es el resultado obtenido cuando una amenaza explota una vulnerabilidad afectando a uno o varios activos de información.

**Cuadro 10. Amenazas vulnerabilidades y consecuencias**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI1 | Teléfonos celulares | Hurto de equipos | Equipo con alta movilidad | Perdida de información por hurto de equipos, con posible pérdida de confidencialidad de información personal, y estratégica del negocio |
| | | Agua | Equipo con alta movilidad | Perdida de información por daño de equipos y sobrecostos económicos para la compañía |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Perdida de información por daño de equipos y sobrecostos económicos para la compañía |
| ALFAAI2 | Teléfonos IP | Hurto de equipos | Equipos con movilidad | Perdida de información por hurto de equipos, con posible pérdida de confidencialidad de información personal, y estratégica del negocio |
| | | Polvo, corrosión | Equipo sensible a humedad y polvo | Perdida de información por daño de equipos y sobrecostos económicos para la compañía |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Perdida de información por daño de equipos, generando indisponibilidad del servicio a uno o varios usuarios |
| ALFAAI3 | Firewalls | Fuego | Ubicación susceptible a incendios | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI4 | Switchs | Fuego | Ubicación susceptible a incendios | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| ALFAAI5 | Access Point | Fuego | Ubicación susceptible a incendios | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad en servicios de red, para una o varias sedes de la compañía, generando sobrecostos económicos por la sustitución del equipo. |
| ALFAAI6 | Equipos de cómputo | Fuego | Ubicación susceptible a incendios | Perdida de información personal y del negocio, de la compañía, generando sobrecostos por la reposición del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Perdida de información personal y del negocio, de la compañía, generando sobrecostos por la reposición del equipo. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI6 | Equipos de cómputo | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Perdida de información personal y del negocio, de la compañía, generando sobrecostos por la reposición del equipo. |
| ALFAAI7 | Tabletas | Hurto de equipos | Equipos con movilidad | Perdida de información por hurto de equipos, con posible pérdida de confidencialidad de información personal, y estratégica del negocio. |
| | | Agua | Equipo con alta movilidad | Perdida de información personal y del negocio, de la compañía, generando sobrecostos por la reposición del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Perdida de información personal y del negocio, de la compañía, generando sobrecostos por la reposición del equipo. |
| ALFAAI8 | Impresoras | Fuego | Ubicación susceptible a incendios | Indisponibilidad de servicios de impresión, generando sobrecostos por la reposición del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad de servicios de impresión, generando sobrecostos por la reposición del equipo. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad de servicios de impresión, generando sobrecostos por la reposición del equipo. |
| ALFAAI9 | Scanner | Fuego | Ubicación susceptible a incendios | Indisponibilidad de servicios de digitalización, generando sobrecostos por la reposición del equipo. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad de servicios de digitalización, generando sobrecostos por la reposición del equipo. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad de servicios de digitalización, generando sobrecostos por la reposición del equipo. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI10 | Servidores corporativos | Fuego | Ubicación susceptible a incendios | Indisponibilidad de servicio de autenticación, para red WIFI, correo electrónico, acceso al dominio, y sobrecostos económicos por reposición de los equipos. |
| | | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Indisponibilidad de servicio de autenticación, para red WIFI, correo electrónico, acceso al dominio, y sobrecostos económicos por reposición de los equipos. |
| | | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Indisponibilidad de servicio de autenticación, para red WIFI, correo electrónico, acceso al dominio, y sobrecostos económicos por reposición de los equipos. |
| ALFAAI11 | IBM | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI12 | Telefónica | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI13 | Neiser comunicaciones | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI14 | ACG of Américas | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI15 | 360 Security group | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI16 | MCO Global | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI17 | Walter Bridge | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI18 | Prointech | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI19 | Milenio PC | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI20 | Xertical labs | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor. |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor. |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI21 | Soluciones .net | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad de los servicios prestados por el proveedor |
| | | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de los servicios prestados por el proveedor |
| | | Espionaje industrial | Falta de política de seguridad de la información para suministradores. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI22 | Jefe de redes y comunicaciones | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas. | Indisponibilidad de servicios de red. |
| ALFAAI23 | Jefe de infraestructura | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas. | Indisponibilidad de servicios de infraestructura |
| ALFAAI24 | Analista de infraestructura | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| | | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas. | Indisponibilidad de servicios de infraestructura. |
| ALFAAI25 | Analista de telecomunicaciones | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Ataques de Ingeniería social | Falta de Concienciación y capacitación en seguridad de la información. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas. | Indisponibilidad de servicios de red |
| ALFAAI26 | Gerente de Tics | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| | | Ataques de Ingeniería social | Falta de Concienciación y capacitación en seguridad de la información. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. |
| ALFAAI31 | Red WIFI | Interceptación de señales | Falta de política para el uso de controles criptográficos. | Perdida de confidencialidad de información estratégica del negocio, e información personal |
| | | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos. | Indisponibilidad de servicios de Red WIFI |
| | | Saturación del sistema de información | Falta de controles de red. | Indisponibilidad de servicios de Red WIFI |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| | | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones. | Perdida de confidencialidad de información estratégica del negocio, e información personal |
| ALFAAI32 | Red MPLS | Interceptación de señales | Falta de política para el uso de controles criptográficos. | Perdida de confidencialidad de información estratégica del negocio, e información personal |
| | | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos. | Indisponibilidad de servicios de Red WIFI |
| | | Saturación del sistema de información | Falta de controles de red. | Indisponibilidad de servicios de Red WIFI |
| | | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones. | Perdida de confidencialidad de información estratégica del negocio, e información personal |
| ALFAAI33 | Canales de Internet | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos. | Indisponibilidad de servicios de Red WIFI. |
| | | Saturación del sistema de información | Falta de controles de red. | Indisponibilidad de servicios de Red WIFI. |
| | | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones. | Perdida de confidencialidad de información estratégica del negocio, e información personal. |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI34 | Cableado estructurado | Interceptación de señales | Falta de especificaciones para el suministro de cableado estructurado. | Perdida de confidencialidad de información estratégica del negocio, e información personal. |
| ALFAAI35 | Centros de cómputo | Fuego | Ubicación susceptible a incendios. | Indisponibilidad de servicios de Red e Infraestructura, y sobrecostos económicos por reposición de equipos. |
| | | Polvo, corrosión, golpes | Ubicación con altos niveles de polución. | Indisponibilidad de servicios de Red e Infraestructura, y sobrecostos económicos por reposición de equipos. |
| | | Pérdida del suministro de energía | Falta de sistema para el suministro de energía ininterrumpida. | Indisponibilidad de servicios de Red e Infraestructura. |
| | | Pérdida del suministro de ventilación | Falta de mantenimiento de sistema de ventilación. | Posibles daños de los equipos de red e infraestructura. |
| ALFAAI35 | Centros de cómputo | Inundaciones | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de servicios de Red e Infraestructura. |
| | | Incumplimiento en el mantenimiento | Indisponibilidad de personal. | Posibles daños de los equipos de red e infraestructura. |
| | | Terremotos | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Indisponibilidad de servicios de Red e Infraestructura |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI36 | Zonas de almacenamiento | Fuego | Ubicación susceptible a incendios. | Sobrecostos económicos por pérdida de equipos. |
| | | Polvo, corrosión, golpes | Ubicación con altos niveles de polución. | Sobrecostos económicos por pérdida de equipos. |
| | | Hurto de equipos | Falta de control en los puntos de acceso como áreas de despacho, carga y demás puntos donde puede ingresar personal no autorizado. | Sobrecostos económicos por pérdida de equipos. |
| ALFAAI37 | Sistemas operativos | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Problemas en la operación normal de la compañía. |
| | | Mal funcionamiento del sistema de información | Falta de procedimientos para el control de la instalación de software en sistemas operativos. | Problemas en la operación normal de la compañía. |
| | | Infección con software malicioso | Falta de controles de detección, prevención y recuperación contra códigos maliciosos. | Problemas en la operación normal de la compañía. |
| ALFAAI38 | SAP | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Problemas en la operación. |
| | | Mal funcionamiento del sistema de información | Falta de controles para el uso adecuado de recursos. | Indisponibilidad del servicio de SAP |

**Cuadro 10. (Continuación)**

| ID | Activo | Amenazas | Vulnerabilidades | Consecuencias |
|---|---|---|---|---|
| ALFAAI39 | Correo electrónico | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas. | Perdida de confidencialidad e integridad de información estratégica de la compañía, e información personal. Indisponibilidad del servicio de correo electrónico corporativo |
| | | Mal funcionamiento del sistema de información | Falta de controles para el uso adecuado de recursos. | Indisponibilidad del servicio de correo electrónico corporativo |
| | | Spam | Falta de controles sobre la mensajería electrónica. | Mal funcionamiento del servicio de correo electrónico |

Fuente. Los Autores

## 7.3 IMPACTO Y PROBABILIDAD DE INCIDENTE

Antes de realizar la evaluación del riesgo, se debe determinar el impacto que se presentaría para la organización, cuando una vulnerabilidad llega a ser explotada por una amenaza, teniendo en cuenta los valores de criticidad asignados a cada uno de los activos de información. Para el caso de ALFAGRES S.A se definió clasificar el impacto, en 5 niveles, tal como se puede observar en el Cuadro 11.

**Cuadro 11. Niveles de impacto**

| Nivel de impacto | Descripción del impacto |
|---|---|
| Muy alto | Afectación total e indefinida de los procesos de negocio, representando pérdidas económicas o afectando la imagen de la compañía. |
| Alto | Afectación de la operación en una o varias sedes de la compañía, por lo menos 1 día. |
| Medio | Afectación de la operación en una o varias sedes de la compañía, por lo menos 6 horas hábiles. |
| Bajo | Afectación la operación en una o varias sedes de la compañía, por lo menos 1 hora hábil. |
| Muy bajo | El incidente no causa afectación a la operación de la compañía. |

Fuente. Los Autores

La probabilidad de incidente refleja la posibilidad de que una amenaza se materialice, y explote una vulnerabilidad, puede ser medida validando el historial de eventos pasados, y verificando con los usuarios, administradores del sistema, proveedores, o especialistas, la frecuencia de dichos eventos

Para el caso de ALFAGRES S.A, se definieron 5 niveles cualitativos de probabilidad, teniendo en cuenta la ocurrencia en ocasiones anteriores, obtenida de historiales de eventos registrados en los sistemas de monitoreo, herramienta de gestión de tickets de mesa de ayuda, e informes de disponibilidad además de la retroalimentación de usuarios, administradores de sistemas, y proveedores véase el Cuadro 12.

**Cuadro 12. Niveles de probabilidad**

| Nivel de probabilidad | Descripción de la probabilidad |
|---|---|
| Muy alta | Es seguro que la amenaza explota la vulnerabilidad, esto ha ocurrido por lo menos una vez a la semana. |
| Alta | Es probable que la amenaza explote la vulnerabilidad, ha ocurrido por lo menos una vez al mes. |
| Media | Existe una probabilidad razonable de que la amenaza explote la vulnerabilidad, ha ocurrido por lo menos una vez al año. |
| Baja | Es poco probable que la amenaza explote la vulnerabilidad, no ha ocurrido anteriormente. |
| Muy baja | No es probable que la amenaza afecte a la vulnerabilidad. |

Fuente. Los Autores

## 7.4 NIVEL DE RIESGO

El nivel del riesgo es la relación entre la probabilidad de ocurrencia de un incidente, y las consecuencias o impacto resultante del mismo, en el Cuadro 13 se presentan los niveles de riesgo definidos para el área de infraestructura tecnológica de ALFAGRES S.A

**Cuadro 13. Niveles de riesgo**

| Nivel de riesgo | Descripción |
|---|---|
| Critico | Riesgo que implique la materialización eminente de una amenaza, y que como consecuencia afecte de manera indefinida la operación de la compañía. |
| Medio | Riesgo que implique la posible materialización de una amenaza, y que como consecuencia afecte de la operación de la compañía, por un periodo de tiempo no mayor a 6 horas. |
| Bajo | Significa que la materialización de una amenaza podría tener un efecto adverso insignificante de la operación de la compañía, o activos de información |

Fuente. Los Autores

Para tener una visión más clara de los niveles de riesgo de acuerdo con el impacto de un incidente, y la probabilidad de que ocurra el mismo, se diseña un mapa de calor véase el Cuadro 14, sobre el cual se ubicara posteriormente cada uno de los riesgos de información, de acuerdo con el nivel estimado.

**Cuadro 14. Mapa de calor**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Impacto** | **Muy alto** | Medio | Medio | Alto | Alto | Alto |
| | **Alto** | Medio | Medio | Alto | Alto | Alto |
| | **Medio** | Medio | Medio | Alto | Alto | Alto |
| | **Bajo** | Medio | Medio | Medio | Medio | Medio |
| | **Muy bajo** | Bajo | Bajo | Bajo | Bajo | Bajo |
| | | **Muy baja** | **Baja** | **Media** | **Alta** | **Muy alta** |
| | | **Probabilidad** | | | | |

Fuente. Los Autores

# 8. EVALUACIÓN DEL RIESGO

Para comprender la naturaleza de los riesgos que se presentan en las organizaciones y afectan los activos de información, o los diferentes tipos de procesos, se realiza primero un análisis de riesgo, precedido por la evaluación de los mismos, asignando un valor que permita identificar los más significativos para enfocar los recursos en la reducción de los mismos. Como resultado de la evaluación de riesgo para el área de infraestructura tecnológica de ALFAGRES S.A, se generó el Cuadro 15, en el cual se puede observar el nivel de riesgo, según el impacto que provocaría en la organización, y la probabilidad de que una amenaza, llegue a materializarse para explotar una vulnerabilidad, a continuación, se describe el contenido para cada columna del Cuadro 15.

- ID: es un código alfanumérico asignado al activo de información.

- Activo: es el recurso de información, sobre el cual se está evaluando el riesgo.

- IR: es un identificador alfanumérico, asignado a cada riesgo identificado.

- Amenaza: causa del riesgo para un activo de información.

- Vulnerabilidad: debilidad o falla que puede ser aprovechada para afectar un activo de información, proceso, u operación de la compañía.

- Nivel de impacto: afectación que tendrían los activos, o la operación de la organización, si llegase a materializarse el escenario de incidente.

- Nivel de probabilidad: es un valor cualitativo asignado a la posibilidad de que se materialice un escenario de incidente.

- Nivel de riesgo: relación entre la probabilidad de ocurrencia del escenario de incidente, y el impacto que ocasionaría a los procesos del área o la operación de la organización. De acuerdo con los niveles de riesgo definidos en el Cuadro 15, en el cuadro número 21, se pinta la columna de la derecha, con el color correspondiente para el nivel de riesgo asociado.

**Cuadro 15. Matriz de riesgos**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI1 | Teléfonos celulares | ALFARI1 | Hurto de equipos | Equipo con alta movilidad | Medio | Muy alta | Alto |
| | | ALFARI2 | Agua | Equipo con alta movilidad | Muy bajo | Alta | Bajo |
| | | ALFARI3 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Muy bajo | Alta | Bajo |
| ALFAAI2 | Teléfonos IP | ALFARI4 | Hurto de equipos | Equipos con movilidad | Muy bajo | Baja | Bajo |
| | | ALFARI5 | Polvo, corrosión | Equipo sensible a humedad y polvo | Muy bajo | Media | Bajo |
| | | ALFARI6 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Muy bajo | Media | Bajo |
| ALFAAI3 | Firewalls | ALFARI7 | Fuego | Ubicación susceptible a incendios | Muy alto | Baja | Medio |
| | | ALFARI8 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Muy alto | Baja | Medio |
| | | ALFARI9 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Muy alto | Alta | Alto |
| ALFAAI4 | Switchs | ALFARI10 | Fuego | Ubicación susceptible a incendios | Medio | Baja | Medio |
| | | ALFARI11 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Medio | Baja | Medio |
| | | ALFARI12 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Medio | Media | Alto |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI5 | Access Point | ALFARI13 | Fuego | Ubicación susceptible a incendios | Medio | Baja | Medio |
| | | ALFARI14 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Medio | Baja | Medio |
| | | ALFARI15 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Medio | Baja | Medio |
| ALFAAI6 | Equipos de cómputo | ALFARI16 | Fuego | Ubicación susceptible a incendios | Medio | Baja | Medio |
| | | ALFARI17 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Medio | Baja | Medio |
| | | ALFARI18 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Medio | Media | Alto |
| | | ALFARI19 | Hurto de equipos | Equipos con movilidad | Medio | Alta | Alto |
| ALFAAI7 | Tabletas | ALFARI20 | Hurto de equipos | Equipos con movilidad | Medio | Alta | Alto |
| | | ALFARI21 | Agua | Equipo con alta movilidad | Bajo | Baja | Medio |
| | | ALFARI22 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Bajo | Media | Medio |
| ALFAAI8 | Impresoras | ALFARI23 | Fuego | Ubicación susceptible a incendios | Bajo | Baja | Medio |
| | | ALFARI24 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Bajo | Baja | Medio |
| | | ALFARI25 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Bajo | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI9 | Scanner | ALFARI26 | Fuego | Ubicación susceptible a incendios | Bajo | Baja | Medio |
| | | ALFARI27 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Bajo | Baja | Medio |
| | | ALFARI28 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Bajo | Media | Medio |
| ALFAAI10 | Servidores corporativos | ALFARI29 | Fuego | Ubicación susceptible a incendios | Muy alto | Baja | Medio |
| | | ALFARI30 | Polvo, corrosión, golpes | Equipo sensible a humedad y polvo | Muy alto | Baja | Medio |
| | | ALFARI31 | Fluctuaciones de energía eléctrica | Equipos sensibles a variaciones de voltaje | Muy alto | Media | Alto |
| ALFAAI11 | IBM | ALFARI32 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Alto | Media | Alto |
| | | ALFARI33 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Alto | Baja | Medio |
| | | ALFARI34 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Alto | Baja | Medio |
| | | ALFARI35 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Alto | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI12 | Telefónica | ALFARI36 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Alto | Alta | Alto |
| | | ALFARI37 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Muy alto | Baja | Medio |
| | | ALFARI38 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Alto | Baja | Medio |
| | | ALFARI39 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Alto | Media | Alto |
| ALFAAI13 | Neiser comunicaciones | ALFARI40 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI41 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Medio | Baja | Medio |
| | | ALFARI42 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI43 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI14 | ACG of Américas | ALFARI44 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Media | Alto |
| | | ALFARI45 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Medio | Baja | Medio |
| | | ALFARI46 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI47 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |
| ALFAAI15 | 360 Security group | ALFARI48 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI49 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Medio | Baja | Medio |
| | | ALFARI50 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI51 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Alto | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI16 | MCO Global | ALFARI52 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI53 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Medio | Baja | Medio |
| | | ALFARI54 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI55 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |
| ALFAAI17 | Walter Bridge | ALFARI56 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI57 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Medio | Baja | Medio |
| | | ALFARI58 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI59 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI18 | Prointech | ALFARI60 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI61 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Medio | Baja | Medio |
| | | ALFARI62 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI63 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |
| ALFAAI19 | Milenio PC | ALFARI64 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI65 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Medio | Baja | Medio |
| | | ALFARI66 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI67 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI20 | Xertical labs | ALFARI68 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Alto | Media | Alto |
| | | ALFARI69 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Alto | Baja | Medio |
| | | ALFARI70 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Alto | Baja | Medio |
| | | ALFARI71 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Alto | Baja | Medio |
| ALFAAI21 | Soluciones .net | ALFARI72 | Ataques de piratas informáticos | Falta de política para la actualización de sistemas operativos | Medio | Baja | Medio |
| | | ALFARI73 | Terrorismo | Falta de procesos para asegurar la continuidad del negocio. | Medio | Baja | Medio |
| | | ALFARI74 | Espionaje industrial | Falta de política de seguridad de la información para suministradores | Medio | Baja | Medio |
| | | ALFARI75 | Abuso de privilegios | Falta de supervisión y revisión de los servicios prestados por terceros | Medio | Media | Alto |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI22 | Jefe de redes y comunicaciones | ALFARI76 | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados | Medio | Media | Alto |
| | | ALFARI77 | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Medio | Baja | Medio |
| | | ALFARI78 | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas | Medio | Media | Alto |
| ALFAAI23 | Jefe de infraestructura | ALFARI79 | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados | Medio | Media | Alto |
| | | ALFARI80 | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Medio | Baja | Medio |
| | | ALFARI81 | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas | Medio | Media | Alto |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI24 | Analista de infraestructura | ALFARI82 | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados | Medio | Media | Alto |
| | | ALFARI83 | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Medio | Baja | Medio |
| | | ALFARI84 | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas | Medio | Media | Alto |
| ALFAAI25 | Analista de telecomunicaciones | ALFARI85 | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados | Medio | Media | Alto |
| | | ALFARI86 | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Medio | Baja | Medio |
| | | ALFARI87 | Error en el uso de sistemas de información | Falta de proceso de control de cambios en los sistemas | Medio | Media | Alto |
| ALFAAI26 | Gerente de Tics | ALFARI88 | Abuso de privilegios | Falta de controles para el uso de derechos de accesos privilegiados | Alto | Media | Alto |
| | | ALFARI89 | Ataques de Ingeniería social | Falta de Concienciación, educación y capacitación en seguridad de la información. | Alto | Media | Alto |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI31 | Red WIFI | ALFARI90 | Interceptación de señales | Falta de política para el uso de controles criptográficos | Alto | Baja | Medio |
| | | ALFARI91 | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos | Medio | Alta | Alto |
| | | ALFARI92 | Saturación del sistema de información | Falta de controles de red | Medio | Alta | Alto |
| | | ALFARI93 | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones | Alto | Media | Alto |
| ALFAAI32 | Red MPLS | ALFARI94 | Interceptación de señales | Falta de política para el uso de controles criptográficos | Alto | Baja | Medio |
| | | ALFARI95 | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos | Medio | Alta | Alto |
| | | ALFARI96 | Saturación del sistema de información | Falta de controles de red | Medio | Alta | Alto |
| | | ALFARI97 | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones | Alto | Media | Alto |
| ALFAAI33 | Canales de Internet | ALFARI98 | Falla de los equipos de telecomunicaciones | Falta de mantenimiento de equipos | Medio | Alta | Alto |
| | | ALFARI99 | Saturación del sistema de información | Falta de controles de red | Medio | Alta | Alto |
| | | ALFARI100 | Acceso no autorizado al sistema de información | Falta de controles para la seguridad de las comunicaciones | Alto | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI34 | Cableado estructurado | ALFARI101 | Interceptación de señales | Falta de especificaciones para el suministro de cableado estructurado | Alto | Baja | Medio |
| ALFAAI35 | Centros de cómputo | ALFARI102 | Fuego | Ubicación susceptible a incendios | Alto | Baja | Medio |
| | | ALFARI103 | Polvo, corrosión, golpes | Ubicación con altos niveles de polución | Medio | Media | Alto |
| | | ALFARI104 | Pérdida del suministro de energía | Falta de sistema para el suministro de energía ininterrumpida | Bajo | Alta | Medio |
| | | ALFARI105 | Pérdida del suministro de ventilación | Falta de mantenimiento de sistema de ventilación | Bajo | Baja | Medio |
| | | ALFARI106 | Incumplimiento en el mantenimiento | Indisponibilidad de personal | Bajo | Alta | Medio |
| | | ALFARI107 | Inundaciones | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Muy alto | Baja | Medio |
| | | ALFARI108 | Terremotos | Falta de procesos para asegurar la continuidad del negocio, durante desastres o crisis. | Muy alto | Baja | Medio |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI36 | Zonas de almacenamiento | ALFARI109 | Fuego | Ubicación susceptible a incendios | Alto | Baja | Medio |
| | | ALFARI110 | Polvo, corrosión, golpes | Ubicación con altos niveles de polución | Medio | Baja | Medio |
| | | ALFARI111 | Hurto de equipos | Falta de control en los puntos de acceso como áreas de despacho, carga y demás puntos donde puede ingresar personal no autorizado. | Medio | Media | Alto |
| ALFAAI37 | Sistemas operativos | ALFARI112 | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas | Medio | Alta | Alto |
| | | ALFARI113 | Mal funcionamiento del sistema de información | Falta de procedimientos para el control de la instalación de software en sistemas operativos | Alto | Alta | Alto |
| | | ALFARI114 | Infección con software malicioso | Falta de controles de detección, prevención y recuperación contra códigos maliciosos | Alto | Alta | Alto |

**Cuadro 15. (Continuación)**

| ID | Activo | IR | Amenaza | Vulnerabilidad | Nivel de impacto | Nivel de probabilidad | Nivel de riesgo |
|---|---|---|---|---|---|---|---|
| ALFAAI38 | SAP | ALFARI115 | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas | Muy alto | Media | Alto |
| | | ALFARI116 | Mal funcionamiento del sistema de información | Falta de controles para el uso adecuado de recursos | Medio | Alta | Alto |
| ALFAAI39 | Correo electrónico | ALFARI117 | ataques de piratas informáticos | Falta de proceso para la gestión de vulnerabilidades técnicas | Muy alto | Media | Alto |
| | | ALFARI118 | Mal funcionamiento del sistema de información | Falta de controles para el uso adecuado de recursos | Medio | Alta | Alto |
| | | ALFARI119 | Spam y Pishing | Falta de controles sobre la mensajería electrónica | Medio | Media | Alto |

Fuente. Los Autores

Como resultado del proceso de evaluación de riesgos, para el área de infraestructura tecnológica de ALFAGRES S.A. se presenta el Cuadro 16 en el cual es posible verificar los riesgos clasificados en cada uno de los niveles definidos anteriormente. Se evidencia que 41 de los riesgos identificados fueron catalogados como altos; de acuerdo con la relación entre su probabilidad de ocurrencia y el impacto que causarían a los procesos del área, o la operación del negocio. Estos riesgos deben ser priorizados para su tratamiento, con la finalidad de reducirlos a un valor aceptable para la compañía.

Es importante resaltar que el proceso de evaluación de riesgos debe ser realizado constantemente, con la finalidad de validar la clasificación otorgada a los riesgos, y logrando verificar que los mismos sean reducidos a niveles aceptables para el negocio, con lo que también es posible validar la eficiencia de los controles aplicados, y obtener una retroalimentación, para la toma de decisiones, y planeación de nuevas acciones, que permitan reducir el riesgo.

**Cuadro 16. Mapa de riesgos de infraestructura tecnológica**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Nivel de impacto** | **Muy alto** | | ALFARI7, ALFARI8, ALFARI29, ALFARI30, ALFARI37, ALFARI107, ALFARI108, | ALFARI31, ALFARI115, ALFARI117, | ALFARI9, | |
| | **Alto** | | ALFARI33, ALFARI34, ALFARI35, ALFARI38, ALFARI51, ALFARI69, ALFARI70, ALFARI71, ALFARI90, ALFARI94, ALFARI100, ALFARI101, ALFARI102, ALFARI109, | ALFARI32, ALFARI39, ALFARI68, ALFARI88, ALFARI89, ALFARI93, ALFARI97, | ALFARI36, ALFARI113, ALFARI114, | |
| | **Medio** | | ALFARI10, ALFARI11, ALFARI13, ALFARI14, ALFARI15, ALFARI16, ALFARI17, ALFARI40, ALFARI41, ALFARI42, ALFARI43, ALFARI45, ALFARI46, ALFARI47, ALFARI48, ALFARI49, ALFARI50, ALFARI52, ALFARI53, ALFARI54, ALFARI55, ALFARI56, ALFARI57, ALFARI58, ALFARI59, ALFARI60, ALFARI61, ALFARI62, ALFARI63, ALFARI64, ALFARI65, ALFARI66, ALFARI67, ALFARI72, ALFARI73, ALFARI74, ALFARI77, ALFARI80, ALFARI83, ALFARI86, ALFARI110, | ALFARI12, ALFARI18, ALFARI44, ALFARI75, ALFARI76, ALFARI78, ALFARI79, ALFARI81, ALFARI82, ALFARI84, ALFARI85, ALFARI87, ALFARI103, ALFARI111, ALFARI119, | ALFARI19, ALFARI20, ALFARI91, ALFARI92, ALFARI95, ALFARI96, ALFARI98, ALFARI99, ALFARI112, ALFARI116, ALFARI118, | ALFARI1 |
| | **Bajo** | | ALFARI21, ALFARI23, ALFARI24, ALFARI25, ALFARI26, ALFARI27, ALFARI105, | ALFARI22, ALFARI28, | ALFARI104, ALFARI106, | |
| | **Muy bajo** | | ALFARI4 | ALFARI5, ALFARI6 | ALFARI2, ALFARI3 | |
| | | **Muy baja** | **Baja** | **Media** | **Alta** | **Muy alta** |
| | | **Nivel de probabilidad** | | | | |

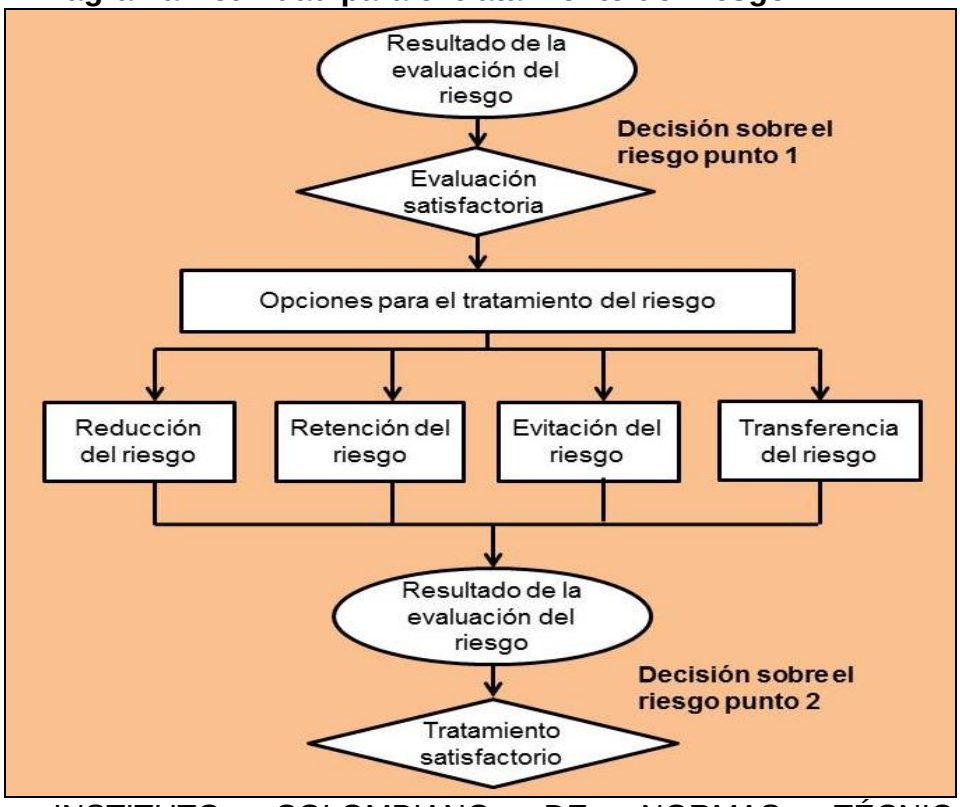
Fuente. Los Autores

## 9. PLAN DE TRATAMIENTO DE LOS RIESGOS

El tratamiento del riesgo es el proceso mediante el cual se deberían seleccionar controles que permitan reducir, evitar, o transferir el riesgo, de tal manera que este factor sea aceptable según los criterios definidos por la organización. Par realizar un correcto tratamiento del riesgo, es vital que la evaluación del mismo sea satisfactoria.

Para definir el tratamiento de cada uno de los riesgos, se debe tener en cuenta el resultado de la evaluación del riesgo, el costo de los controles a implementar, y el beneficio que implica la implementación, teniendo como horizonte, la reducción de la mayor cantidad de riesgo posible, al menor costo económico véase la Figura 4. En ocasiones es posible realizar un tratamiento del riesgo, "combinando las cuatro opciones de tratamiento; la reducción de probabilidad del riesgo, reducción de consecuencias, y transferencia o retención del riesgo residual"[18]

**Figura 4. Diagrama Actividad para el tratamiento del riesgo**




Fuente. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. p. 13.

[18] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Op. cit. p. 14

El tratamiento del riesgo no implica la ausencia del mismo, por lo cual es muy importante mantener monitoreo constante sobre los riesgos identificados, de tal manera que se logren identificar los factores que lo puedan incrementar, o disminuir, ya que es de vital importancia centrar los recursos en los riesgos que así lo requiera.

## 9.1 CRITERIOS PARA EL TRATAMIENTO DEL RIESGO

A continuación, se definen los criterios para el tratamiento de los riesgos identificados y evaluados, para el área de infraestructura tecnológica de ALFAGRES S. A. En el Cuadro 17 se pueden observar las acciones definidas a tomar, según el nivel de riesgo evaluado.

➢Reducir: disminuir el nivel de riesgo, mediante la implementación de controles, de tal manera que el riesgo residual aceptable para la organización.

➢Retener: aceptar el riesgo de acuerdo con la evaluación del mismo, y teniendo en cuenta que los criterios de aceptación sean cumplidos.

➢Transferir: de entrega el riesgo a una entidad o área, que pueda manejarlo de una manera más adecuada, teniendo en cuenta sus capacidades y experticia.

**Cuadro 17. Criterios para el tratamiento del riesgo según el nivel de riesgo**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Impacto** | **Muy alto** | Reducir | Reducir | Transferir Reducir | Transferir Reducir | Transferir Reducir |
| | **Alto** | Reducir | Reducir | Transferir Reducir | Transferir Reducir | Transferir Reducir |
| | **Medio** | Reducir | Reducir | Transferir Reducir | Transferir Reducir | Transferir Reducir |
| | **Bajo** | Reducir | Reducir | Reducir | Reducir | Reducir |
| | **Muy bajo** | Retener | Retener | Retener | Retener | Retener |
| | | **Muy baja** | **Baja** | **Media** | **Alta** | **Muy alta** |
| | | **Probabilidad** | | | | |

Fuente. Los Autores

## 9.2 PLAN DE ACCIÓN PARA EL TRATAMIENTO DEL RIESGO

El Cuadro 18, muestra la propuesta de tratamiento para los riesgos identificados y evaluados, teniendo en cuenta su nivel de riesgo, y los criterios de tratamiento definidos, más adelante se presentarán los controles de la norma ISO/IEC 27001:2013 que aplican a la compañía, de acuerdo con las funciones del área dentro de ALFAGRES S.A.

**Cuadro 18. Plan de acción**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Abuso de privilegios | 360 Security group | Medio | Reducir | - Realizar auditorías periódicas sobre los dispositivos administrados por el proveedor.<br>- Realizar auditorías periódicas sobre los permisos de usuarios que tiene el empleado.<br>- Revisión de los usuarios con permisos de administración sobre los sistemas de información. |
| | ACG of Américas | Medio | Reducir | |
| | Analista de infraestructura | Alto | Transferir o Reducir | |
| | Analista de telecomunicaciones | Alto | Transferir o Reducir | |
| | Xertical labs | Medio | Reducir | |
| | Gerente de Tics | Alto | Transferir o Reducir | |
| | IBM | Medio | Reducir | |
| | Jefe de infraestructura | Alto | Transferir o Reducir | |
| | Jefe de redes y comunicaciones | Alto | Transferir o Reducir | |
| | MCO Global | Medio | Reducir | |
| | Milenio PC | Medio | Reducir | |
| | Neiser comunicaciones | Medio | Reducir | |
| | Prointech | Medio | Reducir | |
| | Soluciones .net | Alto | Transferir o Reducir | |
| | Telefónica | Alto | Transferir o Reducir | |
| | Walter Bridge | Medio | Reducir | |
| Acceso no autorizado al sistema de información | Canales de Internet | Medio | Reducir | - Realizar pruebas de pentesting sobre los sistemas de información, para identificar posibles fallos de seguridad.<br>- Realizar revisión de los usuarios que tienen permisos para el acceso al sistema de información. |
| | Red MPLS | Alto | Transferir o Reducir | |
| | Red WIFI | Alto | Transferir o Reducir | |
| Agua | Tabletas | Medio | Reducir | - Implementar normativa de uso correcto de dispositivos móviles, incluyendo el cuidado y responsabilidades del usuario. |
| | Teléfonos celulares | Bajo | Retener | |
| Ataques de Ingeniería social | Analista de infraestructura | Medio | Reducir | - Implementar un plan de capacitación, para los usuarios con permisos de administración. |
| | Analista de telecomunicaciones | Medio | Reducir | |
| | Gerente de Tics | Alto | Transferir o Reducir | |
| | Jefe de infraestructura | Medio | Reducir | |
| | Jefe de redes y comunicaciones | Medio | Reducir | |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Error en el uso de sistemas de información | Analista de infraestructura | Alto | Transferir o Reducir | - Establecer procedimiento para el control y ejecución de cambios.<br><br>- Realizar capacitaciones a los usuarios, para el uso adecuado de los sistemas de información. |
| | Analista de telecomunicaciones | Alto | Transferir o Reducir | |
| | Jefe de infraestructura | Alto | Transferir o Reducir | |
| | Jefe de redes y comunicaciones | Alto | Transferir o Reducir | |
| Espionaje industrial | 360 Security group | Medio | Reducir | - Incluir en los contratos para proveedores acuerdos de confidencialidad y de seguridad con respecto a la información que es tratada en los sistemas de información que administran. |
| | ACG of Américas | Medio | Reducir | |
| | Xertical labs | Medio | Reducir | |
| | IBM | Medio | Reducir | |
| | MCO Global | Medio | Reducir | |
| | Milenio PC | Medio | Reducir | |
| | Neiser comunicaciones | Medio | Reducir | |
| | Prointech | Medio | Reducir | |
| | Soluciones .net | Medio | Reducir | |
| | Telefónica | Medio | Reducir | |
| | Walter Bridge | Medio | Reducir | |
| Falla de los equipos de telecomunicaciones | Canales de Internet | Alto | Transferir o Reducir | - Incluir en el contrato con el proveedor mantenimientos preventivos a los sistemas de información.<br><br>- Diseñar e implementar sistemas de contingencia.<br><br>- Realizar afinamiento del monitoreo para los sistemas de información, de tal manera que se puedan identificar y corregir los eventos que puedan afectar a los sistemas de información. |
| | Red MPLS | Alto | Transferir o Reducir | |
| | Red WIFI | Alto | Transferir o Reducir | |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Fluctuaciones de energía eléctrica | Access Point | Medio | Reducir | - Realizar revisión de los sistemas de administración de energía en los centros de cableado y datacenter.<br><br>- Definir la ejecución de mantenimientos periódicos, a los sistemas de administración de energía.<br><br>- Validar el estado de los sistemas de potencia ininterrumpida y corregir las fallas de los mismos.<br><br>- Establecer con los proveedores, tiempos de cambio de los equipos por daños. |
| | Equipos de cómputo | Medio | Reducir | |
| | Firewalls | Alto | Transferir o Reducir | |
| | Impresoras | Medio | Reducir | |
| | Scanner | Medio | Reducir | |
| | Servidores corporativos | Medio | Reducir | |
| | Switches | Alto | Transferir o Reducir | |
| | Teléfonos IP | Bajo | Retener | |
| Fuego | Access Point | Medio | Reducir | - Realizar mantenimiento a los sistemas de ventilación en los centros de cableado y datacenter.<br><br>- Realizar afinamiento del sistema de monitoreo, para establecer alertas por temperatura elevada en los equipos.<br><br>- Revisar los mecanismos de contención de fuego en los centros de cableado y datacenter.<br><br>- Establecer controles de acceso a las zonas seguras, para evitar el acceso de elementos que puedan causar incendios. |
| | Centros de cómputo | Medio | Reducir | |
| | Equipos de cómputo | Medio | Reducir | |
| | Firewalls | Medio | Reducir | |
| | Impresoras | Medio | Reducir | |
| | Scanner | Medio | Reducir | |
| | Servidores corporativos | Medio | Reducir | |
| | Switches | Medio | Reducir | |
| | Zonas de almacenamiento | Medio | Reducir | |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Hurto de equipos | Equipos de cómputo | Alto | Transferir o Reducir | - Implementar sistemas de borrado remoto y seguridad, para los dispositivos móviles que pueden ser hurtados.<br>- Capacitar a los usuarios sobre el uso adecuado de los dispositivos, para evitar ser víctimas de hurto. |
| | Tabletas | Alto | Transferir o Reducir | |
| | Teléfonos celulares | Alto | Transferir o Reducir | |
| | Teléfonos IP | Bajo | Retener | |
| | Zonas de almacenamiento | Alto | Transferir o Reducir | |
| Incumplimiento en el mantenimiento | Centros de cómputo | Medio | Reducir | - Definir un cronograma de mantenimiento para los centros de cableado de la organización. |
| Infección con software malicioso | Sistemas operativos | Alto | Transferir o Reducir | - Realizar planes de capacitación a los usuarios, para indicar los controles y cuidados que deben tener con respecto a programas maliciosos.<br>-Monitorear permanentemente las nuevas amenazas contra los sistemas operativos usados en la compañía, y validar con los proveedores de seguridad, las acciones a tomar para evitar infección. |
| Interceptación de señales | Cableado estructurado | Medio | Reducir | - Implementar política de cifrado para la información crítica.<br>- Fortalecer los controles de acceso para evitar ingresos de personas ajenas a la organización<br>- Solicitar a los proveedores el monitoreo en los sistemas de información, para identificar anomalías en la seguridad de los mismos. |
| | Red MPLS | Medio | Reducir | |
| | Red WIFI | Medio | Reducir | |
| Inundaciones | Centros de cómputo | Medio | Reducir | - Establecer Sistemas de contingencia que permitan la continuidad de la operación. |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Mal funcionamiento del sistema de información | Correo electrónico | Alto | Transferir o Reducir | - Establecer con los proveedores sistemas de contingencia que permitan la continuidad de la operación.<br><br>- Realizar pruebas periódicas del funcionamiento de los sistemas. |
| | SAP | Alto | Transferir o Reducir | |
| | Sistemas operativos | Alto | Transferir o Reducir | |
| Pérdida del suministro de energía | Centros de cómputo | Medio | Reducir | - Establecer plan de mantenimiento preventivo con el área encargada de la administración de los sistemas de administración de energía.<br><br>- Establecer sistemas de redundancia que permitan la continuidad de la operación en casos de pérdida de suministro de energía. |
| Pérdida del suministro de ventilación | Centros de cómputo | Medio | Reducir | - Establecer plan de mantenimiento preventivo con el área encargada de la administración de los sistemas de ventilación. |
| Polvo, corrosión, golpes | Access Point | Medio | Reducir | - Establecer planes de mantenimiento preventivo con los proveedores. |
| | Centros de cómputo | Alto | Transferir o Reducir | |
| | Equipos de cómputo | Medio | Reducir | |
| | Firewalls | Medio | Reducir | |
| | Impresoras | Medio | Reducir | |
| | Scanner | Medio | Reducir | |
| | Servidores corporativos | Medio | Reducir | |
| | Switches | Medio | Reducir | |
| | Teléfonos celulares | Bajo | Retener | |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Saturación del sistema de información | Canales de Internet | Alto | Transferir o Reducir | - Mantener constante monitoreo para los sistemas de información.<br>- Definir niveles críticos para la saturación de los sistemas de información y configurar estos en los sistemas de monitoreo.<br><br>- Realizar revisión de los permisos de usuarios y las políticas de calidad de servicios.<br><br>- Realizar capacitación a los usuarios, sobre el buen uso de los recursos de la compañía, con respecto a los sistemas de información. |
| | Red MPLS | Alto | Transferir o Reducir | |
| | Red WIFI | Alto | Transferir o Reducir | |
| Spam y Pishing | Correo electrónico | Alto | Transferir o Reducir | - Realizar capacitación a los usuarios, sobre las precauciones en el uso de correo electrónico.<br><br>- Validar con el proveedor la implementación de controles existentes para la seguridad de correo electrónico. |
| Terremotos | Centros de cómputo | Medio | Reducir | - Diseñar e implementar sistemas de contingencia, que permitan la continuidad de la operación. |
| Terrorismo | 360 Security group | Medio | Reducir | - Diseñar e implementar sistemas de contingencia, que permitan la continuidad de la operación |
| | ACG of Américas | Medio | Reducir | |
| | Xertical labs | Medio | Reducir | |
| | IBM | Medio | Reducir | |
| | MCO Global | Medio | Reducir | |
| | Milenio PC | Medio | Reducir | |
| | Prointech | Medio | Reducir | |
| | Soluciones .net | Medio | Reducir | |
| | Telefónica | Alto | Transferir o Reducir | |

**Cuadro 18. (Continuación)**

| Riesgo | Activo | Nivel de riesgo | Tratamiento | Plan de acción |
|---|---|---|---|---|
| Ataques de piratas informáticos | Correo electrónico | Alto | Transferir o Reducir | - Realizar pruebas periódicas de pentesting, sobre los sistemas de información.<br>- Implementar un plan de capacitación para los usuarios de los sistemas de información.<br>- Monitorear permanentemente, la aparición de vulnerabilidades técnicas sobre los sistemas de información<br>- Establecer con los proveedores, acuerdos de seguridad para los sistemas de información y la compañía. |
| | SAP | Alto | Transferir o Reducir | |
| | Sistemas operativos | Alto | Transferir o Reducir | |
| | 360 Security group | Medio | Reducir | |
| | ACG of Américas | Alto | Transferir o Reducir | |
| | Xertical labs | Alto | Transferir o Reducir | |
| | IBM | Alto | Transferir o Reducir | |
| | MCO Global | Medio | Reducir | |
| | Milenio PC | Medio | Reducir | |
| | Neiser comunicaciones | Medio | Reducir | |
| | Prointech | Medio | Reducir | |
| | Soluciones .net | Medio | Reducir | |
| | Telefónica | Alto | Transferir o Reducir | |
| | Walter Bridge | Medio | Reducir | |

Fuente. Los Autores

## 9.3 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad es uno de los elementos más relevantes en el diseño de un sistema de gestión de seguridad, ya que indica los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001:2013 que deben ser adoptados por la organización, de acuerdo con el proceso de análisis de riesgos ejecutado, permitiendo a la organización, tener una visión completa de las acciones que se están tomando para disminuir los riesgos de seguridad en la información.

En el Cuadro 19 se puede observar la declaración de aplicabilidad para el sistema de gestión de seguridad diseñado para el área de infraestructura tecnológica de ALFAGRES S.A, justificando la elección o descarte de cada uno de los 114 controles propuestos por el Anexo A del estándar ISO/IEC 27001:2013.

**Cuadro 19. Declaración de aplicabilidad**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| **Dominio** | **A.5 Políticas de seguridad de la información** | | |
| Objetivo de control | A.5.1 Orientación de la dirección para la gestión de la seguridad de la información | | |
| Control | A.5.1.1 Políticas para la seguridad de la información. | SI | Se deben definir las políticas de seguridad de la información, acordes a los objetivos de la organización, y debe ponerse a disposición de los empleados, usuarios, proveedores, y todo aquel que intervenga en la administración o manejo de información de la empresa, aclarando la perspectiva de la organización, con respecto a la seguridad de la información. |
| Control | A.5.1.2 Revisión de la política de seguridad de la información. | SI | Las políticas de seguridad de la información deben ser revisadas y evaluadas periódicamente, o cuando se presenten cambios en procesos que alteren la seguridad de la información, para revalidar la perspectiva de la organización con respecto a la seguridad de la información. |
| **Dominio** | **A.6 Organización de la seguridad de la información** | | |
| Objetivo de control | 6.1 Organización interna | | |
| Control | A.6.1.1 Roles y responsabilidades para la seguridad de información. | SI | Se debe definir el área o responsables, y se deben atribuir los roles y responsabilidades pertinentes para la correcta ejecución de los procesos de seguridad de la información |
| Control | A.6.1.2 Separación de deberes. | SI | Se debe ejecutar una separación de las funciones, para disminuir el riesgo de accesos autorizados y abuso de privilegios por parte de los administradores de sistemas de información. |
| Control | A.6.1.3 Contacto con las autoridades. | SI | Se deben aclarar y documentar los procedimientos para el reporte de incidentes y problemas que así lo ameriten, a las autoridades correspondientes, de acuerdo con lo estipulado por la reglamentación nacional de delitos informáticos. |
| Control | A.6.1.4 Contacto con grupos de interés especial. | SI | Se debe fortalecer el contacto con las autoridades territoriales, grupos académicos, y prestadores de servicios, que trabajan en el ámbito de la seguridad de la información, de tal manera que se tenga una visión general por parte del área encargada de la seguridad de la información, de las nuevas amenazas y posibles riesgos generados. |
| Control | A.6.1.5 Seguridad de la información en la gestión de proyectos. | SI | Se debe implementar un procedimiento, para la evaluación de la seguridad de la información, con respecto a los proyectos que ejecuta el área. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 6.2 Dispositivos móviles y teletrabajo | | |
| Control | A.6.2.1 Política para dispositivos móviles. | SI | Se debe generar una política de seguridad que permita asegurar los dispositivos móviles de la organización, o de los usuarios, que tengan almacenada información corporativa, |
| Control | A.6.2.2 Teletrabajo. | SI | Se deben implementar medidas de protección para garantizar el trabajo remoto, manteniendo la seguridad de la información, y disminuyendo el riesgo de divulgación o interceptación de información sensible. |
| **Dominio** | **A.7 Seguridad de los recursos humanos** | | |
| Objetivo de control | 7.1 Antes de asumir el empleo | | |
| Control | A.7.1.1 Selección | SI | El personal es seleccionado de acuerdo con el perfil requerido, y el proceso incluye verificaciones de seguridad de la información. |
| Control | A.7.1.2 Términos y condiciones del empleo. | SI | Se deben incluir cláusulas de confidencialidad y penalidades cuando sea requerido, en los contratos laborales, de tal manera que se pueda garantizar la seguridad de la información confidencial. |
| Objetivo de control | 7.2 Durante la ejecución del empleo | | |
| Control | A.7.2.1 Responsabilidades de la dirección. | SI | Se debe establecer la responsabilidad de la dirección, con respecto a la seguridad de la información y la importancia del SGSI |
| Control | A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. | SI | Se deben diseñar e implementar procesos de conciencia, educación y formación, por parte del área encargada de la seguridad de la información, para disminuir el riesgo de ataques informáticos que usan ingeniería social, y técnicas que aprovechan el desconocimiento de los funcionarios. |
| Control | A.7.2.3 Proceso disciplinario | SI | Se deben establecer procesos disciplinarios para los funcionarios que se vean implicados en incumplimientos de las políticas de seguridad de la información, para generar un ambiente de cumplimiento y responsabilidad, con respecto a la seguridad de la información. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 7.3 Terminación o cambio de empleo | | |
| Control | A.7.3.1 Terminación o cambio de responsabilidades de empleo. | SI | Se debe establecer un procedimiento, mediante el cual reporte el personal que se desvincula de la compañía, y aquellos funcionarios, que son promovidos o cambian de funciones. El área encargada de la seguridad debe realizar una validación de los accesos y permisos del usuario, para disminuir el riesgo de accesos no autorizados y abuso de privilegios. |
| **Dominio** | **A.8 Gestión de activos** | | |
| Objetivo de control | 8.1 Responsabilidad por los activos | | |
| Control | A.8.1.1 Inventario de activos. | SI | El área de seguridad de la información debe elaborar y mantener actualizado el inventario de activos de información, incluyendo el código del activo, el responsable y los procesos con los que se relaciona. |
| Control | A.8.1.2 Propiedad de los activos. | SI | Se debe asignar un responsable a cada uno de los activos de información, asegurando un control constante de los mismos. |
| Control | A.8.1.3 Uso aceptable de los activos. | SI | Se debe generar un plan de concienciación, con respecto al uso adecuado de los activos de información con el fin de evitar usos inadecuados y saturación en los sistemas de información. |
| Control | A.8.1.4 Devolución de activos. | SI | Se debe fortalecer el proceso para la devolución de los activos de información, que tienen a su cargo los funcionarios para la ejecución de sus labores, para disminuir el riesgo de divulgación de información corporativa y accesos no autorizados. |
| Objetivo de control | 8.2 Clasificación de la información | | |
| Control | A.8.2.1 Clasificación de la información. | SI | Se debe realizar la clasificación de la información para cada uno de los activos, de acuerdo con los niveles de seguridad establecidos para priorizar de manera correcta los riesgos de seguridad en la información. |
| Control | A.8.2.2 Etiquetado de la información. | SI | Se debe asegurar que cada uno de los activos de información sea clasificado de acuerdo con los niveles de criticidad establecidos para priorizar de manera correcta los riesgos de seguridad en la información. |
| Control | A.8.2.3 Manejo de activos. | SI | Se deben establecer procedimientos que permitan el manejo de los activos de información, de acuerdo con la clasificación de criticidad establecida. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| **Dominio** | **A.8 Gestión de activos** | | |
| Objetivo de control | 8.3 Manejo de medios | | |
| Control | A.8.3.1 Gestión de medios removibles. | SI | Se deben implementar procedimientos que aseguren la gestión de medios removibles, para disminuir el riesgo de pérdida de confidencialidad en la información, e infección con software malicioso. |
| Control | A.8.3.2 Disposición de los medios. | SI | Se debe elaborar un procedimiento para la disposición de medios al terminar su vida útil, de tal manera que no representen riesgos para la seguridad de la información. |
| Control | A.8.3.3 Transferencia de medios físicos. | SI | Se deben implementar controles que permitan proteger los medios físicos, de accesos no autorizados. |
| **Dominio** | **A.9 Control de acceso** | | |
| Objetivo de control | 9.1 Requisitos del negocio para control de acceso | | |
| Control | A.9.1.1 Política de control de acceso. | SI | Se debe generar una política para el control de acceso que permita disminuir los riesgos por daños físicos y hurto para los activos de información. |
| Control | A.9.1.2 Política sobre el uso de los servicios de red. | SI | Se debe generar una política para asegurar el uso de los servicios de red, y disminuir el riesgo de mal uso de recursos, saturación de sistemas de información, accesos no autorizados, divulgación o la perdida de integridad de la información |
| Objetivo de control | 9.2 Gestión de acceso de usuarios | | |
| Control | A.9.2.1 Registro y cancelación del registro de usuarios. | SI | Existe un procedimiento claro de registro y cancelación de registro de usuarios para posibilitar la asignación de los derechos de acceso. |
| Control | A.9.2.2 Suministro de acceso de usuarios. | SI | Existe un proceso mediante el cual se asignan o revocan derechos de accesos a los usuarios para todos los sistemas y servicios que presta el área |
| Control | A.9.2.3 Gestión de derechos de acceso privilegiado. | Si | Se restringe y controla la asignación y uso de derechos de acceso privilegiado, teniendo en cuenta el perfilamiento del cargo para cada uno de los usuarios. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 9.2 Gestión de acceso de usuarios | | |
| Control | A.9.2.4 Gestión de información de autenticación secreta de usuarios. | SI | Se debe generar un proceso de asignación de información secreta, garantizando la confidencialidad de la misma. |
| Control | A.9.2.5 Revisión de los derechos de acceso de usuarios. | SI | Se debe implementar un proceso, mediante el cual los responsables de cada activo realicen la revisión de los derechos de acceso para los usuarios, disminuyendo el riesgo de accesos no autorizados y abuso de privilegios. |
| Control | A.9.2.6 Retiro o ajuste de los derechos de acceso. | SI | Se debe establecer un procedimiento, mediante el cual no solo se reporte el personal que se desvincula de la compañía, si no también aquellos funcionarios, que son promovidos o cambian de funciones dentro de la compañía. El área encargada de la seguridad debe realizar una validación de los accesos y permisos del usuario, para disminuir el riesgo de accesos no autorizados y abuso de privilegios. |
| Objetivo de control | 9.3 Responsabilidades de los usuarios | | |
| Control | A.9.3.1 Uso de la información de autenticación secreta. | SI | El área encargada de la seguridad de la información debe generar una política de autenticación secreta, que permita disminuir el riesgo de accesos no autorizados a los sistemas de información. |
| Objetivo de control | 9.4 Control de acceso a sistemas y aplicaciones | | |
| Control | A.9.4.1 Restricción de acceso Información. | SI | Se debe generar una política de restricción de acceso, que permita disminuir el riesgo de accesos no autorizados a los sistemas de información. |
| Control | A.9.4.2 Procedimiento de ingreso seguro. | SI | Se debe establecer controles para el acceso seguro a los sistemas de información, disminuyendo así el riesgo de accesos no autorizados. |
| Control | A.9.4.3 Sistema de gestión de contraseñas. | SI | Se encuentran implementados requisitos de seguridad mínimos para las contraseñas, asegurando la calidad de estas, de igual manera se encuentra configurado en los sistemas de información del área un tiempo de vencimiento de las contraseñas, forzando a los usuarios a cambiarlas cada cierto tiempo. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 9.4 Control de acceso a sistemas y aplicaciones | | |
| Control | A.9.4.4 Uso de programas utilitarios privilegiados | SI | Se encuentran definidos y aplicados controles para evitar que los usuarios puedan instalar herramientas que puedan afectar el funcionamiento de los sistemas de información. |
| Control | A.9.4.5 Control de acceso a códigos fuente. | SI | El código fuente de las aplicaciones corporativas es restringido y solo tienen acceso quienes por sus labores lo requieren. |
| **Dominio** | **A.10 Criptografía** | | |
| Objetivo de control | 10.1 Controles criptográficos | | |
| Control | A.10.1.1 Política sobre el uso de controles criptográfico | SI | Se debe establecer una política para el uso de controles criptográficos, que permitan disminuir el riesgo de la pérdida de confidencialidad de la información, en caso de ser interceptada. |
| Control | A.10.1.2 Gestión de llaves. | SI | Se debe implementar una política de protección y tiempo de vida de las llaves criptográficas, de tal manera que se pueda mantener la seguridad. |
| **Dominio** | **A.11 Seguridad física y del entorno** | | |
| Objetivo de control | 11.1 Áreas seguras | | |
| Control | A.11.1.1 Perímetro de seguridad física. | SI | Las redes que contienen información sensible se encuentran segmentadas, y filtradas por FW, que supervisan el tráfico que se genera hacia ellas, de igual manera se cuenta con protección en todas las zonas de frontera a internet. |
| Control | A.11.1.2 Controles físicos de entrada. | SI | Se encuentran implementados controles de acceso biométricos y controles físicos de seguridad para la protección de los centros de datos que manejan información sensible. |
| Control | A.11.1.3 Seguridad de oficinas, recintos. | SI | Se encuentran implementados controles físicos de acceso a las oficinas del área, para garantizar la seguridad tanto física como lógica del área. |
| Control | A.11.1.4 Protección contra amenazas externas | SI | Se deben diseñar e implementar medidas físicas de protección ante desastres naturales, para garantizar la continuidad del negocio. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 11.1 Áreas seguras | | |
| Control | A.11.1.5 Trabajo en áreas seguras. | SI | Se debe elaborar un procedimiento que indique los requisitos para el acceso y trabajo en áreas seguras, de tal manera que se disminuya el riesgo de daños físicos o hurto de los activos de información que se encuentran en estas áreas. |
| Control | A.11.1.6 Áreas de despacho y carga. | SI | Se encuentran implementados controles físicos, que impiden el acceso al área, de personal no autorizado |
| Objetivo de control | 11.2 Equipos | | |
| Control | A.11.2.1 Ubicación y protección de los equipos | SI | Los equipos se encuentran ubicados dentro de zonas protegidas por controles de acceso, temperatura e incendios, lo que reducen el riesgo de amenazas y peligros del entorno |
| Control | A.11.2.2 Servicios de suministro. | SI | Se debe definir un estándar y los requerimientos mínimos de controles, que protejan los equipos de fallas o interrupciones en los servicios de suministro. Para asegurar la continuidad necesaria para la operación del negocio. |
| Control | A.11.2.3 Seguridad del cableado. | SI | Se debe definir medidas de protección y estándar para el cableado usado por la compañía, de tal manera que se pueda asegurar la continuidad de la operación, y la protección de los datos que porta esta infraestructura. |
| Control | A.11.2.4 Mantenimiento de equipos. | SI | Se debe establecer un plan de mantenimiento con sus respectivos responsables, y se debe asegurar el cumplimiento, de tal manera que se logren disminuir los eventos de indisponibilidad por daño de equipos. |
| Control | A.11.2.5 Retiro de activos. | SI | Se debe implementar un procedimiento para el retiro de equipos, disminuyendo el riesgo de hurto. |
| Control | A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones. | SI | Se encuentran aplicados controles de seguridad, contra programas maliciosos, y control de acceso a internet. Adicionalmente se debe implementar sistemas de cifrado que permitan proteger la información almacenada en los equipos que así lo requieran de acuerdo con el perfil del usuario. |
| Control | A.11.2.7 Disposición segura o reutilización de equipos. | SI | Se debe generar el procedimiento para la reutilización de equipos, incluyendo el proceso de borrado seguro, garantizando que cualquier dato sensible haya sido retirado o sobrescrito en forma segura antes de su reutilización. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 11.2 Equipos | | |
| Control | A.11.2.8 Equipos de usuario desatendido. | SI | Se debe incluir dentro del programa de capacitación de usuarios las buenas prácticas, con respecto al bloqueo de equipos cuando estos no se encuentran en uso, disminuyendo el riesgo de accesos no autorizados a los sistemas de información. |
| Control | A.11.2.9 Política de escritorio limpio y pantalla limpia. | SI | Se debe generar una política de escritorio limpio, otorgando un mayor nivel de seguridad a la información que maneja cada uno de los usuarios. De igual manera se debe incluir las mejores prácticas, en el programa de capacitación. |
| **Dominio** | **A.12 Seguridad de las operaciones** | | |
| Objetivo de control | 12.1 Procedimientos operacionales y responsabilidades | | |
| Control | A.12.1.1 Procedimientos de operación documentados | SI | Se deben documentar y poner a disposición de los usuarios todos los procedimientos generados, una vez sea aprobado por la alta dirección, esto con el fin de que los usuarios puedan observar y adoptar dichos procedimientos, para mejorar la seguridad. |
| Control | A.12.1.2 Gestión de cambios | SI | Se debe generar un procedimiento para la gestión de cambios en el área, disminuyendo los riesgos de mal uso de sistemas de información. |
| Control | A.12.1.3 Gestión de capacidad | SI | En el área se realizan el seguimiento al uso de recursos, y control de los mismos, con el fin de identificar cuando es necesario realizar ajustes para cumplir con los requisitos de capacidad futura, y optimizar los recursos del área. |
| Control | A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación | SI | Se cuenta con separación de ambientes en los sistemas de información core para el negocio, administrados por el área. |
| Objetivo de control | 12.2 Protección contra códigos maliciosos | | |
| Control | A.12.2.1 Controles contra códigos maliciosos. | SI | Se cuenta con un servicio de antivirus contratado para los computadores corporativos, mediante el cual se logra identificar y bloquear códigos maliciosos, se deben incluir las mejores prácticas para evitar infecciones con virus, en los planes de capacitación para los usuarios. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 12.3 Copias de respaldo | | |
| Control | A.12.3.1 Respaldo de información. | SI | Se deben realizar copias periódicamente de los sistemas de información, y ejecutar pruebas periódicas para garantizar su funcionamiento. |
| Objetivo de control | 12.4 Registro y seguimiento | | |
| Control | A.12.4.1 Registro de eventos. | SI | Se debe generar un proceso para la conservación de logs de eventos críticos, y realizar revisiones de los mismos, para identificar eventos que puedan afectar la seguridad de la información. |
| Control | A.12.4.2 Protección de la información de registro. | SI | Se cuenta con controles de autenticación en los sistemas de información críticos para el negocio, con la finalidad de evitar alteraciones y accesos no autorizados |
| Control | A.12.4.3 Registros del administrador y del operador. | SI | Se deben registrar las actividades realizadas por los administradores de los sistemas de información, y revisar regularmente, para identificar abusos de privilegios y demás riesgos en la seguridad de la información. |
| Control | A.12.4.4 Sincronización de relojes. | SI | Los relojes de los sistemas de información críticos se encuentran sincronizados de acuerdo con el servidor de hora legal Colombia, sin embargo, no hay una política que exija esto. |
| Objetivo de control | 12.5 Control de software operacional | | |
| Control | A.12.5.1 Instalación de software en sistemas operativos. | SI | La instalación de software en los sistemas operativos está limitada al personal de soporte de la organización, los usuarios no cuentan con los permisos necesarios para la instalación de ningún software, y para cualquier instalación se debe solicitar autorización de los administradores. |
| Objetivo de control | 12.6 Gestión de la vulnerabilidad técnica | | |
| Control | A.12.6.1 Gestión de las vulnerabilidades técnicas. | SI | Se debe generar un proceso, para la evaluación de vulnerabilidades técnicas, el cual debe ser ejecutado de manera periódica, con la finalidad de disminuir los riesgos de seguridad para los sistemas de información. |
| Control | A.12.6.2 Restricciones sobre la instalación de software. | SI | La instalación de software en los sistemas operativos está limitada al personal de soporte de la organización, los usuarios no cuentan con los permisos necesarios para la instalación de ningún software, y para cualquier instalación se debe solicitar autorización de los administradores |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 12.7 Consideraciones sobre auditorías de sistemas de información | | |
| Control | A.12.7.1 Información controles de auditoría de sistemas | SI | Se debe mejorar el proceso de auditoría actual, incluyendo pruebas de vulnerabilidades técnicas, que permitan identificar y subsanar posibles riesgos de seguridad en la información. |
| **Dominio** | **13. Seguridad de las comunicaciones** | | |
| Objetivo de control | 13.1 Gestión de la seguridad de las redes | | |
| Control | A.13.1.1 Controles de redes. | SI | Se realiza un control y gestión de la infraestructura de redes dentro de la compañía, con apoyo de varios proveedores, especializados. |
| Control | A.13.1.2 Seguridad de los servicios de red. | SI | Se encuentran identificados mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red, y se encuentran estipulados dentro de los contratos con los diversos proveedores. |
| Control | A.13.1.3 Separación en las redes. | SI | Se encuentran segmentadas las redes de usuarios, servicios de información, y sistemas, de igual manera se encuentran filtrados por cortafuegos, para restringir el tráfico no permitido en cada una de las zonas. |
| Objetivo de control | 13.2 Transferencia de información | | |
| Control | A.13.2.1 Políticas y procedimientos de transferencia de información. | SI | Se debe implementar una política para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones |
| Control | A.13.2.2 Acuerdos transferencia de información | SI | Se incluyen cláusulas en los contratos con proveedores del área, para exigir controles que permitan garantizar la transferencia segura de información del negocio. |
| Control | A.13.2.3 Mensajería electrónica | SI | Se deben implementar controles para la protección de la información que es transferida por medio de correo electrónico. |
| Control | A.13.2.4 Acuerdos confidencialidad o de no divulgación. | SI | Se debe implementar un proceso que permita la identificar revisar y documentar, regularmente los requisitos para los acuerdos de confidencialidad |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| **Dominio** | **14 Adquisición, desarrollo y mantenimientos de sistemas** | | |
| Objetivo de control | 14.1 Requisitos de seguridad de los sistemas de información | | |
| Control | A.14.1.1 Análisis y especificación de requisitos de seguridad de la información | SI | Se debe generar un procedimiento para incluir los requisitos de seguridad de la información en los procesos de adquisición de nuevos equipos. |
| Control | A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas | SI | Se debe trasladar esta responsabilidad a los proveedores de las aplicaciones que generan tráfico sobre las redes públicas. |
| Control | A.14.1.3 Protección de transacciones de los servicios | SI | Se deben aplicar controles para la protección de la información en las transacciones, evitando malos enrutamientos, alteraciones y reproducción de mensajes no autorizados. |
| Objetivo de control | 14.2 Seguridad en los procesos de desarrollo y soporte | | |
| Control | A.14.2.1 Política de desarrollo seguro. | NO | El área no realiza actividades de desarrollo de software |
| Control | A.14.2.2 Procedimientos de control de cambios en sistemas. | SI | Existe un proceso de control de cambios para los sistemas core de la compañía. |
| Control | A.14.2.3 Revisión de las aplicaciones después de cambios. | SI | Se realizan pruebas al ejecutar cambios sobre los sistemas de información de los cuales es responsable el área |
| Objetivo de control | 14.2 Seguridad en los procesos de desarrollo y soporte | | |
| Control | A.14.2.4 Restricciones en los cambios a los paquetes de software. | NO | El área no realiza tareas de desarrollo de software |
| Control | A.14.2.5 Principios de construcción de sistemas seguros. | NO | El área no realiza tareas de desarrollo de software |
| Control | A.14.2.6 Ambiente de desarrollo seguro. | NO | El área no realiza tareas de desarrollo de software |
| Control | A.14.2.7 Desarrollo contratado externamente | NO | El área no realiza tareas de desarrollo de software |
| Control | A.14.2.8 Pruebas de seguridad de sistemas | NO | El área no realiza tareas de desarrollo de software |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Control | A.14.2.9 Prueba de aceptación de sistemas. | SI | Se establecen pruebas y criterios de aceptación, para la adquisición de sistemas nuevos, o actualizaciones, antes de iniciar el proceso de compra o mejora. |
| Objetivo de control | 14.3 Datos de Prueba | | |
| Control | A.14.3.1 Protección de datos de prueba. | NO | No se realizan desarrollos de software en el área |
| **Dominio** | **15. Relación con los proveedores** | | |
| Objetivo de control | 15.1 Seguridad de la información en las relaciones con los proveedores | | |
| Control | A.15.1.1 Política de seguridad de la información para las relaciones con proveedores. | SI | Se debe definir una política de seguridad, que asegure la información corporativa que es entregada a los proveedores, de igual manera esta política debe dictar los requisitos de seguridad que deben cumplir los proveedores para asegurar la información. |
| Control | A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores. | SI | |
| Control | A.15.1.3 Cadena de suministro de tecnología de información. | SI | |
| Objetivo de control | 15.2 Gestión de la prestación de servicios con los proveedores | | |
| Control | A.15.2.1 Seguimiento y revisión de los servicios de los proveedores. | SI | Se debe definir un procedimiento, para revisar con regularidad la prestación de servicios de los proveedores. |
| Control | A.15.2.2 Gestión de cambios en los servicios de proveedores. | SI | Se encuentran estipulados en los diferentes contratos con los proveedores, los procedimientos para la solicitud, ejecución y control de cambios realizados por los proveedores. |
| **Dominio** | **16. Gestión de incidentes de seguridad de la información** | | |
| Objetivo de control | 16.1 Gestión de incidentes y mejoras en la seguridad de la información | | |
| Control | A.16.1.1 Responsabilidad y procedimientos. | SI | Se debe establecer un procedimiento para la respuesta a incidentes de seguridad de la información que se lleguen a presentar, de tal forma que se pueda disminuir el impacto. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Control | A.16.1.2 Reporte de eventos de seguridad de la información. | SI | Se debe definir un procedimiento para el reporte de eventos de seguridad, de tal manera que se puedan identificar y gestionar aquellos que representen un riesgo elevado para la organización. |
| Control | A.16.1.3 Reporte de debilidades de seguridad de la información. | SI | Se debe definir un procedimiento para el reporten debilidades de los sistemas de información, con el fin de poder evaluar y mitigar el riesgo de que se presente un incidente de seguridad. |
| Control | A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | SI | Se debe generar un proceso para la evaluación de eventos, que pueda dar pautas claras para identificar los eventos relacionados con la seguridad. |
| Control | A.16.1.5 Respuesta a incidentes de seguridad de la información. | SI | Se debe establecer un procedimiento para la respuesta a incidentes de seguridad de la información que se lleguen a presentar, de tal forma que se pueda disminuir el impacto |
| Control | A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información. | SI | Se debe incluir en el procedimiento de respuesta a incidentes, el estudio de los mismos, y de las posibles mejoras, para disminuir su ocurrencia. |
| Control | A.16.1.7 Recolección de evidencia. | NO | Se debe trasladar esta responsabilidad a los proveedores según sea el caso. |
| **Dominio** | **17 Aspectos de seguridad de la información de la gestión de continuidad de negocio** | | |
| Objetivo de control | 17.1 Continuidad de seguridad de la información | | |
| Control | A.17.1.1 Planificación de la continuidad de la seguridad de la información. | SI | Se deben determinar los requisitos para la seguridad de la información, y la gestión de la continuidad de la gestión de seguridad, en situaciones adversas. |
| Control | A.17.1.2 Implementación de la continuidad de la seguridad de la información. | SI | Se deben establecer, documentar implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información de tal manera que la organización pueda continuar con su operación de una manera segura. |
| Control | A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | SI | Se deben establecer y ejecutar pruebas periódicas de los planes de continuidad de la seguridad de la información, para garantizar su funcionamiento. |

**Cuadro 19. (Continuación)**

| | | Aplicable (SI/NO) | Justificación |
|---|---|---|---|
| Objetivo de control | 17.2 Redundancias | | |
| Control | A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. | SI | Se debe establecer un procedimiento para la respuesta a incidentes de seguridad de la información que se lleguen a presentar, de tal forma que se pueda disminuir el impacto. |
| **Dominio** | **18. Cumplimiento** | | |
| Objetivo de control | 18.1 Cumplimiento de requisitos legales y contractuales | | |
| Control | A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales. | SI | Se debe realizar la identificación de la legislación aplicable a la empresa, para incluir controles de protección de acuerdo a lo indicado por las regulaciones correspondientes. |
| Control | A.18.1.2 Derechos de propiedad intelectual. | SI | Este proceso es realizado por el área jurídica de la compañía. |
| Control | A.18.1.3 Protección de registros. | SI | Se deben implementar controles para la protección de registros, disminuyendo el riesgo de su perdida, destrucción, falsificación, acceso no autorizado, y liberación no autorizada. |
| **Dominio** | **18. Cumplimiento** | | |
| Control | A.18.1.4 Privacidad y protección de información de datos personales | SI | Se debe establecer una política de protección para los datos personales de acuerdo con lo reglamentado por las regulaciones vigentes. |
| Control | A.18.1.5 Reglamentación de controles criptográficos. | SI | Se deben usar los controles criptográficos en cumplimiento de la legislación y reglamentación correspondiente. |
| Objetivo de control | 18.2 Revisiones de seguridad de la información | | |
| Control | A.18.2.1 Revisión independiente de la seguridad de la información. | SI | Se deben generar revisiones periódicas para la gestión de la seguridad de la información. |
| Control | A.18.2.2 Cumplimiento con las políticas y normas de seguridad. | SI | Se debe establecer un procedimiento para la revisión con regularidad del cumplimiento con respecto a las políticas y normas de seguridad establecidas, para identificar posibles mejoras. |
| Control | A.18.2.3 Revisión del cumplimiento técnico. | SI | Se debe establecer un procedimiento para la revisión de los sistemas de información, con respecto a las políticas de seguridad de la información, y lograr identificar posibles mejoras. |

Fuente. Los Autores

# 10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En la actualidad la información para ALFAGRES S.A se ha convertido en un activo de bastante importancia, por ello es necesario efectuar de manera adecuada su protección y la de los sistemas que intervienen en su transmisión, almacenamiento o tratamiento.

Para la organización ALFAGRES S.A la creación de la política implica la implementación de las medidas necesarias que nos indica el estándar del sistema de gestión de seguridad de la información, preservando las propiedades fundamentales de confidencialidad, integridad y disponibilidad. Así poder realizar la aplicación de los controles, estándares y procedimientos necesarios.

La alta dirección debe establecer de manera pública para los colaboradores, proveedores, clientes, socios de negocios o terceros, la política de seguridad de la información.

## 10.1 OBJETIVO

Estimar la conservación de la confidencialidad, integridad y disponibilidad de la información y la infraestructura que la soporta, en el área de infraestructura tecnológica de ALFAGRES S.A, disminuyendo la probabilidad ocurrencia para los eventos que puedan afectar significativamente la operación de ALFAGRES S.A

Garantizar que los colaboradores en sus labores realizadas estén debidamente capacitados en los temas de seguridad de la información y puedan respaldar la política evitando el incumplimiento de ella.

Respaldo de la alta dirección de ALFAGRES S.A en la ejecución y seguimiento de la política de seguridad para su respectivo cumplimiento y promover la cultura de seguridad de la información, en el área de infraestructura tecnológica. Tomando las respectivas medidas disciplinarias cuando se realicen actividades contradictorias a lo establecido en la política.

## 10.2 ALCANCE

La política de seguridad de la información diseñada para el área de infraestructura tecnológica de ALFAGRES S.A y sus respectivos procesos, se aplica a todos los colaboradores, proveedores, clientes, socios de negocios o terceros, con el fin de minimizar los riesgos que pueden afectar la organización.

## 10.3 CUMPLIMENTO

El incumplimiento de lo establecido en la política conllevara a sanciones disciplinarias, legales y demás establecidas por las áreas de seguridad informática, gestión de recursos humanos y división legal.

## 10.4 TÉRMINOS Y DEFINICIONES

- Activo de información: todo elemento relacionado con la seguridad de la información y que tenga relevancia para los procesos de una organización.

- Auditoría: proceso de evaluación y revisión de los controles, obteniendo resultados de evidencias positivos o negativos, al cumplimiento de políticas y estándares establecidos.

- Riesgo: probabilidad de que una vulnerabilidad sea explotada por una amenaza, afectando los objetivos del área de infraestructura de comunicaciones de ALFAGRES SA.

- Confidencialidad: propiedad de garantizar que la información no sea divulgada o accedida por personas no autorizadas.

- Vulnerabilidad: debilidad en los activos de información, que los hace susceptibles a ser afectados.

- Integridad: propiedad de garantizar que la información se encuentre libre de modificaciones o alteraciones por procesos o personas no autorizadas.

- Disponibilidad: propiedad de la información, de ser accesible para ser utilizada cuando el usuario o sistema autorizado lo requiera.

- Alta dirección: personas altamente capacitadas, encargadas en función del cumplimiento de los objetivos de la organización.

- Amenaza: todo elemento, evento o acción que pueda causar daño a la información o sistema informático.

- Impacto: resultado obtenido al presentarse un incidente de seguridad de la información.

- Monitoreo: proceso para determinar el funcionamiento y cumplimiento de la política de seguridad de la información.

## 10.5 POLÍTICA GENERAL

Para el área de infraestructura tecnológica de ALFAGRES S. A. la información es un activo de vital importancia para la correcta ejecución de sus procesos y servicios, por consiguiente, debe ser debidamente protegida contra los riesgos identificados, garantizando la confidencialidad, integridad y disponibilidad de la información, la infraestructura que la soporta, la continuidad del negocio, y el cumplimiento de la misión y la visión de la organización.

La organización ALFAGRES S. A. consciente de la importancia de los sistemas de gestión de seguridad de la información y el cumplimiento de los requerimientos legales, contractuales y regulatorios que rigen para el respectivo manejo de la información, apoya el resultado del análisis y gestión de riesgos que se derivan en materia de seguridad de la información y con la realización del seguimiento continuo.

El incumplimiento de la política de seguridad de la información por los colaboradores, proveedores, clientes, socios de negocio o terceros, ocasionara medidas correctivas, mitigando el impacto contra la seguridad de la información, y aplicando las respectivas sanciones administrativas, disciplinarias o penales que amerite, teniendo en cuenta el impacto generado a la organización.

## 10.6 POLÍTICA DE CONTRASEÑAS

Objetivo: definir los lineamientos indicados por la norma ISO/IEC 27001:2013 para el uso correcto de las contraseñas a los colaboradores, proveedores, clientes y socios de negocio o terceros, en el área de infraestructura tecnológica de ALFAGRES S. A.

Directrices: todas las contraseñas utilizadas para diferentes tipos de accesos deben cumplir las siguientes directrices:

- Es obligatorio que todo usuario realice el cambio de su contraseña, cuando ingresen por primera vez a un sistema de información. Se asignará una contraseña por defecto, con vigencia de 24 horas.

- Las contraseñas deben tener mínimo de 10 caracteres y debe ser conformada por letras, números, caracteres alfanuméricos y signos de puntuación, pero no debe usar caracteres idénticos consecutivos.

- Las contraseñas deben ser cambiadas cada 30 días calendario, para todo tipo de usuario o aplicación del área de infraestructura tecnológica de ALFAGRES S.A. en caso de estar bajo riesgo o anomalía se debe realizar el respectivo cambio.

➢Las contraseñas no deben utilizar información personal de ningún tipo, como números de cédula, fechas de nacimiento, nombre o apellidos suyos o de familiares, números telefónicos, apodos, palabras que se contengan en diccionarios de cualquier idioma o el nombre de la mascota, etc. Se pueden utilizar frases poco comunes de interpretar.

➢Es prohibido realizar el préstamo de contraseñas sin previa autorización y/o realizar el envío de ellas por todo medio de transporte de datos o comunicación de información en texto plano.

➢No se deben almacenar las contraseñas en papel, documentos del sistema, aplicativos móviles, agendas personales o cualquier otro medio que le facilite a una persona mal intencionada conocerlas.

## 10.7 POLÍTICA DE SEGURIDAD PARA RECURSOS HUMANOS

Objetivo: definir las directrices para asegurar que los colaboradores, proveedores, clientes y socios de negocio o terceros, entienden las funciones de sus roles y responsabilidades, para reducir el riesgo de fraude, hurto, filtraciones, uso inadecuado de los recursos, o uso inadecuado de la información.

### 10.7.1 Directrices antes de asumir el empleo.

➢Para toda persona antes de ser contratada formalmente, se debe realizar la validación de los antecedentes penales, antecedentes fiscales, antecedentes disciplinarios, exámenes médicos y de conocimiento, así como la visita domiciliaria, con el fin de disminuir el riesgo y seleccionar la persona más adecuada, de acuerdo a los criterios de la oferta y las necesidades del negocio.

➢Toda persona después de ser seleccionada para realizar funciones o actividades debe leer y firmar el respectivo contrato acorde con la aceptación de los términos y condiciones del empleo en mención. Dentro del contrato se anexan cláusulas correspondientes a la seguridad de la información, que el usuario debe cumplir mientras realiza sus funciones.

➢Se debe realizar una respectiva capacitación de ingreso a todos los funcionarios nuevos en la compañía, conduciéndolos a conocer las políticas de seguridad de la información, procedimientos, y mejores prácticas establecidas en la organización, como también las respectivas sanciones que se efectúan en caso de incumplimiento.

➢Todos los colaboradores, proveedores, clientes y socios de negocio o terceros, después de ser seleccionados para realizar funciones o actividades con ALFAGRES SA, deben firmar el acuerdo de declaración de confidencialidad, que permite disminuir los riesgos de seguridad de la información, y comprometerse con

el cumplimiento de las políticas de seguridad establecidas por el área de seguridad informática de ALFAGRES S.A.

### 10.7.2 Directrices durante del empleo.

➢Se debe realizar un seguimiento a los colaboradores, proveedores, clientes, socios de negocio o terceros, del respectivo cumplimiento en las políticas de seguridad de la información de acuerdo a las funciones asignadas por ALFAGRES SA.

➢Todos los colaboradores, proveedores, clientes, socios o terceros, deben ser capacitados en toma de conciencia, educación y formación de la seguridad de la información, según las actividades asignadas por la organización, y permitiendo reducir los diferentes tipos de riesgos que pueden afectar los objetivos de la organización.

➢Se tomarán las respectivas sanciones contra los colaboradores, proveedores, clientes y socios de negocio o tercero que cometan violaciones e incumplimiento de las políticas de seguridad de la información.

### 10.7.3 Directrices para la terminación y cambio de empleo.

➢Todos los colaboradores, proveedores, clientes y socios de negocio o terceros al realizar la terminación y cambio de empleo, deben informar con anticipación de manera previa y escrita al área de recursos humanos.

➢Al momento que los colaboradores, proveedores, clientes y socios de negocio o terceros realiza la terminación y cambio de empleo, se debe informar a las áreas encargadas para la cancelación de los usuarios y demás accesos laborales.

➢Todo colaborador, proveedor, o tercero que de por terminado su vínculo con el área de infraestructura tecnológica de ALFAGRES S.A, debe regresar los activos asignados por la organización, para la ejecución de las funciones o actividades asignadas.

## 10.8 POLÍTICA PARA DISPOSITIVOS MÓVILES

Objetivo: definir las directrices que aseguren el buen uso de los dispositivos móviles que se encuentren bajo la responsabilidad del área de infraestructura tecnológica de ALFAGRES SA.

### 10.8.1 Directrices.

➢Todos los dispositivos móviles asignados a los colaboradores, proveedores, clientes, socios de negocios o terceros que tengan relación con el área de infraestructura tecnológica de ALFAGRES SA, deben estar protegidos mediante el uso de contraseñas y sistemas que aseguren el borrado seguro de los dispositivos.

➢Se prohíbe la instalación de aplicaciones en los dispositivos móviles asignados para labores del área, sin ser autorizado. El proceso de instalación y configuración de los dispositivos móviles la realizará la mesa de servicios de ALFAGRES S.A. con previa autorización del área de redes y seguridad.

➢Se prohíbe realizar copias de programas o su respectiva documentación, ya que estos programas son propiedad del área de infraestructura de comunicaciones de ALFAGRES SA.

➢En caso de pérdida del dispositivo móvil se debe realizar la denuncia correspondiente, y reportar en el menor tiempo posible a la mesa de servicios de ALFAGRES S.A. teniendo en cuenta los procedimientos estipulados por el área de infraestructura tecnológica.

➢Se prohíbe el uso de dispositivos móviles para la ejecución de actividades o funciones totalmente diferentes a las asignadas por ALFAGRES S.A y la divulgación de información, sin previa autorización de la compañía.

➢Todo evento o incidente que se presente en los dispositivos móviles afectando la seguridad de la información, se debe reportar al área de servicios compartidos, teniendo en cuenta los canales de comunicación dispuestos por ALFAGRES S.A.

➢Se prohíben a los usuarios de dispositivos móviles el almacenamiento de información personal íntima, pornografía infantil o de cualquier otra índole no relacionada con las funciones asignadas por ALFAGRES S.A.

➢Todos los colaboradores, proveedores, clientes, socios de negocio o tercero, al terminar relaciones con ALFAGRES S.A, deben realizar la devolución de los dispositivos móviles asignados teniendo en cuenta el desgaste normal de uso para los equipos.

## 10.9 POLÍTICA DE LOS ACTIVOS DE INFORMACIÓN

Objetivo: asegurar la protección de los activos de información durante el ciclo de vida en la organización.

### 10.9.1 Directrices.

➢Para la adquisición, solicitud o cambios de activos de información, se debe realizar la respectiva solicitud al área de tecnología de acuerdo con los procedimientos establecidos por ALFAGRES S.A

➢Todos los activos de información del área de infraestructura de comunicaciones de ALFAGRES S.A, cuentan con un responsable, encargado de realizar identificación, mantener un inventario, y realizar la clasificación según la funcionalidad y criticidad, teniendo como base los criterios de seguridad de la información.

➢Se debe realizar el acta de entrega para los colaboradores, proveedores, socios de negocio o tercero, a quienes se asignen activos de información, mediante dicha acta, se asume la responsabilidad de los activos, verificando el correcto funcionamiento y estado de los mismos antes de firmar.

➢Los activos de información asignados deben ser utilizados para las respectivas funciones y actividades asignadas por ALFAGRES S.A. En caso de que el área de infraestructura tecnológica identifique algún incumplimiento se realizara las respectivas sanciones administrativas o legales, de acuerdo al caso.

➢En caso de daño o falla del activo se debe reportar a la mesa de servicios de ALFAGRES S.A para que se inicie el proceso de reparación o reposición de acuerdo al procedimiento establecido por el área de infraestructura tecnológica.

➢Todo colaborador, proveedor y socio de negocio que identifique una falla de seguridad de información sobre cualquier activo de información, que se encuentre bajo la responsabilidad del área de infraestructura tecnológica de ALFAGRES S.A. está en la obligación de reportar dicha falla ante la mesa de servicios.

➢Para los colaboradores, proveedores, clientes y socios de negocio o tercero, que les haya sido asignado activos de información para realizar sus respectivas funciones o actividades deben realizar la respectiva entrega de todos los activos de información que pertenezcan al área de infraestructura tecnológica de ALFAGRES SA, cuando finalice su vínculo laboral.

➢Para la finalización de un activo en el área de infraestructura de comunicaciones de ALFAGRES SA, se debe realizar la debida acta y formato de destrucción de activos e informar a todas las áreas y demás que tengan relación con este activo.

## 10.10 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: asegurar que la información tenga respectiva protección, de acuerdo con la clasificación e importancia que le haya establecido el área de infraestructura tecnológica de ALFAGRES SA.

### 10.10.1 Directrices.

- Toda la información debe ser identificada, clasificada, materializada en documentos electrónicos y físicos. También etiquetada con los respectivos procedimientos establecidos por el área de seguridad de la información.

- El área de seguridad y el propietario de la información, teniéndola clasificada y establecida según su criticidad, deben establecer sistemas de cifrado, con el fin de preservar la integridad.

- Todos los colaboradores, proveedores, clientes y socios de negocio o tercero deben preservar la confidencialidad de la información sensible del área de infraestructura tecnológica de ALFAGRES SA.

- Para la información con medio y alto nivel de criticidad, se deben establecer los procedimientos necesarios de seguridad, al igual que para los sistemas de información que la procesas y/o almacenan.

## 10.11 POLÍTICA DE CONTROL DE ACCESO

Objetivo: asegurar el acceso a los sistemas de la organización, la información, los equipos e instalaciones, únicamente a los usuarios autorizados por la organización ALFAGRES SA.

### 10.11.1 Directrices.

- Todos los colaboradores, proveedores, clientes y socios de negocio o terceros se les asignarán acceso a los respectivos sistemas de información, de acuerdo a las funciones y actividades que hayan sido asignadas.

- El acceso con el usuario de administrador o root para los sistemas de información, es prohibido, para cualquier persona. Se puede ingresar con usuarios creados con privilegios de administrador.

- Todos los sistemas y aplicativos son restringidos con sistemas de contraseñas, para evitar el ingreso de personas no autorizadas que puedan afectar la integridad, confidencialidad, o disponibilidad de la información y los sistemas de información.

➢Si los colaboradores, proveedores, clientes socios de negocio o terceros, necesitan de acceso a alguno de los sistemas, aplicaciones, o áreas de infraestructura, se debe realizar la solicitud al área de seguridad de la información de ALFAGRES SA.

➢Todos los colaboradores, proveedores, clientes y socios de negocio o terceros, que realicen actividades o diversas funciones en las instalaciones de la organización, deben portar de manera visible el carné asignado.

➢Todo visitante a las instalaciones de la organización se le asignará un carné provisional para estar en las diversas áreas permitidas, este carné debe portarse de manera visible durante el tiempo que esté en las instalaciones.

➢Está totalmente prohibido la instalación de software en los equipos asignados para las respectivas funciones de la organización, sin previa autorización. Para la instalación de software se debe realizar la solicitud al área de mesa de ayuda.

➢Es prohibido el ingreso de dispositivos electrónicos y de almacenamiento de información a la organización, sin contar con la previa autorización.

➢Toda persona en el momento de retirarse del puesto de trabajo, debe bloquear los aplicativos o sistemas, evitando el acceso a personas no autorizadas.

➢El incumplimiento de la política de todos los colaboradores, proveedores, clientes y socios de negocio o terceros, ocasionará la toma de las respectivas sanciones disciplinarias y/o legales si es el caso y según sea determinado por las áreas de recursos humanos, seguridad de la información y división legal, de ALFAGRES S.A.

## 10.12 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: prevenir el acceso a las instalaciones y las áreas de procesamiento de información, de personas y objetos no autorizados.

### 10.12.1 Directrices.

➢Para el ingreso a la infraestructura todo el personal será identificado por sistemas de acceso seguro, adicional se cuenta con personas de seguridad validando el ingreso de objetos no autorizados.

➢Las personas que ingresen como visitantes, el área encargada debe enviar correo al área de seguridad y logística indicando la solicitud del acceso, el visitante debe reportarse en recepción para registrarse y asignarle un carné como visitante.

➢Es prohibido el ingreso de armas de fuego, objetos cortos punzantes, cámaras de video y/o fotográficas, alucinógenos, objetos de pornografía y explosivos a la organización.

➢Se prohíbe el ingreso a las instalaciones a todos los colaboradores, proveedores, clientes y socios de negocio o terceros que se encuentren en estado de embriaguez o bajo el estado de alucinógenos.

➢Todo sistema informático después de terminar su ciclo de vida en la organización, debe ser reciclado, bajo las normas que los rigen, evitando la contaminación del medioambiente.

➢Es prohibido tener documentos o cualquier objeto en el escritorio y la pantalla de los sistemas de información, es decir, no deben contener documentos, imágenes, accesos directo o cualquier tipo de información crítica.

➢Todos los dispositivos que se utilicen para diferentes funciones o actividades fuera de la organización deben tener controles de seguridad de acceso.

➢Todo el sistema de cableado de datos y voz debe ser instalado teniendo en cuenta los estándares internacionales, y las mejores prácticas adoptadas por el área de redes y comunicaciones de la organización.

➢Todo sistema de información electrónico con nivel de riesgo medio, alto o crítico, debe estar conectado a las tomas de electricidad regulada y UPS (sistema de alimentación ininterrumpida).

## 10.13 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

Objetivo: definir los lineamientos para mantener de forma segura las operaciones y las instalaciones del procesamiento de información.

### 10.13.1 Directrices.

➢Es obligatorio documentar todos los procedimientos de las operaciones que se realicen en ALFAGRES SA y mantenerlos disponibles para usarlos cuando sea necesario.

➢Para la gestión de cambios es obligatorio conformar un comité de cambios, con el fin de analizar las solicitudes de los cambios sobre los activos de información clasificados con niveles de criticidad altos.

➢Se debe realizar el análisis del uso y la capacidad de los sistemas de información con los que cuenta la organización, asegurando el mejor desempeño de los sistemas para alcanzar los objetivos establecidos por la organización.

➢Se debe realizar estudios de nueva tecnología, procesos e infraestructura, con el fin de diseñar e implementar nuevos proyectos, para el crecimiento de la organización, asegurando la confidencialidad, integridad y la disponibilidad de la información de ALFAGRES SA.

➢Se debe realizar los respectivos backups a la información sensible y confidencial de la organización, según lo especificado en la política de clasificación de la información y adicional a esto se debe realizar las respectivas validaciones del buen funcionamiento de los backups.

➢Se deben realizar imágenes de los sistemas de información, con su respectiva validación, teniendo en cuenta que al ser utilizadas funcionen correctamente.

➢Los accesos con privilegios de administración a los sistemas de información, deben ser registrados, almacenados y protegidos en lugares seguros, para su posterior revisión en caso de ser necesario.

➢Se deben realizar pruebas de seguridad a los activos críticos de la información anualmente, por el área encargada de la seguridad de la información, validando las vulnerabilidades y los riesgos que la pueden afectar.

➢El software o sistema de información que ingrese a la compañía ALFAGRES SA, deber ser evaluado por el encargado de la seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

➢Las vulnerabilidades que se evidencien en los sistemas de información deben ser reportadas al área encargada de la de seguridad de la información, con el fin de que se tomen las medidas adecuadas tratando el riesgo que se asocie a la vulnerabilidad.

➢El área de seguridad, deben realizar auditorías anualmente o antes, en caso de ser necesario, con el fin de evaluar el buen funcionamiento del sistema de gestión de seguridad de la información.

➢ Las no conformidades evidenciadas en la auditoría realizada se atenderán según el valor del activo, asignado en la política de clasificación de activos de información.

## 10.14 POLÍTICA DE SEGURIDAD DE RELACIÓN CON LOS PROVEEDORES

Objetivo: definir los lineamientos para mantener de forma segura la protección de los activos que van a ser accedidos o administrados por los proveedores.

**10.14.1 Directrices**.

➢Todos los proveedores deben conocer las políticas de seguridad de la información establecidas en ALFAGRES SA.

➢Se debe realizar un análisis previo con el proveedor identificando el estado de seguridad de la información con el que cuenta actualmente, antes de tener relación laboral.

➢El área de seguridad de la información debe identificar el nivel de seguridad y los riesgos que se pueden llegar presentar, al iniciar labores con un nuevo proveedor.

➢Los cambios que se vallan a realizar en tecnología, servicios, y demás procesos con los proveedores, se deben presentar al comité de control de cambios para el respectivo análisis, teniendo en cuenta la criticidad de los activos de información del negocio.

➢Todos los proveedores y empleados deben reportar todas las vulnerabilidades identificadas o sospechadas de los servicios y/o los sistemas de información, al área de seguridad de la información.

➢Todos los proveedores y empleados deben reportar de manera inmediata, por medio de correo electrónico y/o vía telefónica al área encargada de la seguridad de la información, cuando se presente un incidente de seguridad.

**10.15 POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES**

Objetivo: preservar la seguridad de la información que transita por las redes de comunicaciones y sistemas relacionados de ALFAGRES SA de modo interno y externo.

**10.15.1 Directrices**.

➢Se debe definir el uso de protocolos seguros para el tránsito de información sensible, de tal manera que no sea comprensible en caso de ser interceptada.

➢Los sistemas de información que se deban utilizar para la seguridad de la información como firewall, Reuters, IPS, IDS, debe ser avalados por el área encargada de la seguridad informática, adicionalmente debe ser documentado.

➢Si la comunicación presenta lentitud, estados diferentes al comportamiento normal, se debe reportar de manera inmediata al área encargada de la seguridad de la información en ALFAGRES SA.

➢Las comunicaciones externas deben realizarse por medio de IP públicas, con el fin de no exponer las direcciones IP internas.

➢Las aplicaciones web y demás servidores o aplicaciones expuestas a las redes públicas, deben estar ubicados en una zona desmilitarizada (DMZ).

➢Todas las conexiones que se realicen de modo externo a la red interna de ALFAGRES SA, debe ser realizada por medio de VPN.

## 10.16 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Objetivo: asegurar que en los sistemas de gestión de continuidad del negocio sea incluida la seguridad de la información.

### 10.16.1 Directrices.

➢Es obligatorio el cumplimiento de las leyes, normas y estándares que reglamentan la seguridad de la información.

➢En periodos anuales o cuando ocurran cambios significativos el área de seguridad informática, debe realizar la revisión de los controles, políticas, normas y demás procesos de ALFAGRES SA, que estén relacionados con la seguridad de la información, para determinar el respectivo cumplimiento.

➢Los archivos clasificados como críticos, por la política de clasificación de activos de información, deben estar cifrados por sistemas criptográficos como AES y adicional con su respectivo hash con MD5 o SAH1, asegurando la confidencialidad e integridad de estos archivos.

➢La información debe almacenarse en el lugar seguro establecido por la organización, con el fin de protegerla y que no pueda ser accedida, robada, falsificada o destruida por personas no autorizadas.

➢Los directores del área y dueños de procesos, deben realizar las revisiones con regularidad a los procesos, el manejo de información y demás sistemas relacionados, con el respectivo cumplimiento de las políticas y normas de seguridad establecidos.

## 11. PROPUESTA DE IMPLEMENTACIÓN

El diseño del sistema de gestión de la seguridad de la información propuesto en este documento, está diseñado de acuerdo a la norma ISO/IEC 27001:2013, por lo tanto, el ciclo de vida de este sistema se puede dividir en cuatro etapas; planear, hacer, verificar y actuar véase la Figura 5. Teniendo en cuenta que el diseño cubre la primera etapa, para la implementación del diseño propuesto, se deberían realizar las siguientes actividades, por medio de las cuales se puede poner en marcha el SGSI propuesto, y mejorarlo de acuerdo a las necesidades de la organización.

**Figura 5. Ciclo de vida del SGSI**


Fuente. Los Autores

### 11.1 ACEPTACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad propuesta, debe ser revisada y aprobada por la alta dirección, ya que, en dicho documento, enmarcan los principios adoptados por el área de infraestructura tecnológica, para asegurar la confidencialidad, integridad y disponibilidad de la información, durante la ejecución de los procesos, y con el fin de cumplir los objetivos de ALFAGRES S.A.

## 11.2 IMPLEMENTACIÓN DE CONTROLES

Un control es una medida aplicada para la modificación del riesgo, y se define de acuerdo al nivel estimado para el riesgo, y los recursos de la organización. En el caso del área de infraestructura tecnológica de ALFAGRE S.A. se identificaron un total de 119, riesgos, para los cuales se propone un plan de tratamiento Se recomienda iniciar con la aplicación de controles para los riesgos clasificados con niveles alto, o crítico, ya que, según el análisis de riesgos realizado en el presente documento, son los que mayor impacto ocasionarían sobre los procesos del área de infraestructura tecnológica, y la operación de ALFAGRES S.A.

## 11.3 PUBLICAR Y SOCIALIZAR LA POLÍTICA DE SEGURIDAD

Una vez la política de seguridad de información sea aprobada por la alta dirección, se debe iniciar un proceso de comunicación, a todos los usuarios, proveedores, contratistas, y demás individuos u organizaciones, que estén relacionados con los procesos del área de infraestructura tecnológica de ALFAGRES S.A. Se recomienda a la organización, realizar un proceso de socialización con todos los implicados, mediante el cual sean aclaradas las dudas con respecto a la política, y sea entendida, convirtiendo a los colaboradores y todos los implicados, en gestores de apoyo para garantizar el cumplimiento de la política.

## 11.4 DISEÑAR E IMPLEMENTAR CAMPAÑAS DE CAPACITACIÓN, EDUCACIÓN Y FORMACIÓN

Una de las mayores vulnerabilidades de las compañías, es la falta de conocimientos y comprensión por parte del recurso humano, con respecto a la seguridad de la información, es por esto que, en el diseño de un sistema de gestión de seguridad de la información, se resalta la necesidad de diseñar e implementar campañas de capacitación, educación, y formación, de acuerdo a las funciones de cada usuario de tal manera que puedan disminuir el riesgo de seguridad.

## 11.5 DEFINIR E IMPLEMENTAR AUDITORÍAS

La auditoría es la herramienta usada para validar el alineamiento de la organización, con la estrategia propuesta, en este caso, la política de seguridad. Por medio del proceso de auditoría de seguridad de la información, el área de infraestructura tecnológica de ALFAGRES S.A. lograr identificar posibles errores y tomar las medidas adecuadas, para mejorar el SGSI propuesto, y disminuir el riesgo para la compañía de una manera cada vez más acorde a los objetivos de ALFAGRES S.A.

Para una correcta implementación del SGSI propuesto, se recomienda definir la ejecución de auditorías de seguridad, de manera periódica, incluyendo las

siguientes actividades: evaluación de vulnerabilidades, pruebas de penetración, evaluación del nivel de madurez del SGSI, revisión del SGSI según métricas establecidas por la organización.

### 11.6 MANTENER Y MEJORAR

Teniendo en cuenta las actividades de auditoría, y a las lecciones aprendidas de acuerdo a las experiencias de la organización, es necesario identificar las oportunidades de mejora, e iniciar un proceso de implementación de las mismas, mejorando así el SGSI y disminuyendo el nivel de riesgos para la organización, y completando el ciclo de vida del SGSI.

# 12. CONCLUSIONES

- La seguridad de la información para el área de infraestructura tecnológica de ALFAGRES S.A, se encuentra en un nivel de madurez inicial, ya que la organización no cuenta con una identificación de activos y metodología para la gestión de riesgos, que permitan la implementación de controles optimizando los recursos existentes en la conservación de la integridad, confidencialidad y disponibilidad de la información.

- Durante la identificación del estado de seguridad de la información en el área de infraestructura tecnológica de ALFAGRES S.A. se evidencio la necesidad de identificar los activos de información para el área, y generar un inventario de activos, que contenga la información necesaria, para iniciar el análisis de riesgos.

- Por medio del análisis de riesgos para el área de infraestructura tecnológica de ALFAGRES S.A. se identificaron 119 riesgos, de los cuales 39 son clasificados como altos, 75 como medio y 5 como bajos, teniendo en cuenta la relación entre la probabilidad de ocurrencia y el impacto generado a los procesos del área, o la operación de la organización.

- El anexo A de la norma ISO/IEC 27001:2013 contiene un total de 114 controles, de los cuales 105 son aplicables al área de infraestructura tecnológica de ALFAGRES S.A., teniendo en cuenta los procesos y servicios brindados por el área dentro de la compañía.

- Es necesario definir las políticas de seguridad de la información, alineadas a los objetivos de ALFAGRES S.A. y teniendo en cuenta los recursos dispuestos, por la organización, con el objetivo de implementar controles, que puedan reducir el nivel de riesgo, para los activos de información identificados en el área de infraestructura tecnológica de ALFAGRES S.A.

## BIBLIOGRAFÍA


CARRILLO, Aldair. Contramedidas contra ataques informáticos. [en línea]. Bogotá: Blogspot, 2013 [fecha de consulta 3 de junio de 2017]. Disponible en: http://aldair-11b.blogspot.com.co/2013/04/ contramedidas-para-ataques-informaticos.html

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Seguridad y privacidad de la información. [en línea]. Bogotá: MinTic, 2016 [fecha de consulta 3 de junio de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_ General.pdf

--------. Política general. [en línea]. Bogotá: MinTic, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

--------. Guía para la Implementación de Seguridad de la Información en una MIPYME [en línea]. Bogotá: MinTic, 2014 [citado 7 de marzo de 2017]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

-------. Gestión de riesgo. [en línea]. Bogotá: MinTic, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

CORDOVA, JORGE. Ciber extorsiones: ransomware, denegaciones de servicio, fuga de información y más. [en línea]. Bogotá: Seguridad informática y de la información, 2016. [fecha de consulta 7 de marzo de 2017]. Disponible en: www.inseguridadinformatica.com

EL PORTAL DE LA ISO 27001. Glosario. [en línea]. Bogotá: ISO, 2012 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/glosario.html

GLOBAL ASSOCIATION ISACA. Implementación efectiva de un SGSI ISO 27001. [en línea]. Bogotá: ISACA, 2014 [fecha de consulta 3 de junio de 2017]. Disponible en: www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS 2014%20%20Exposici%C3%B3n%202%20CI GRAS%20ISO%2027001 %20-%20 rbq.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. 63 p.

-------. Gestión del riesgo. Principios y directrices. NTC-ISO31000. Bogotá: ICONTEC, 2014. 34 p.

ISOTOOLS EXCELLENCE. ISO 27001: Los activos de información. [en línea]. Bogotá: PMG, 2015 [fecha de consulta 3 junio de 2017]. Disponible en: www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-información/

-------. ISO 27005: Análisis de Riesgos. [en línea]. Bogotá: ISotools, 2015 [fecha de consulta 3 de junio de 2017]. Disponible en: www.isotools.pe/iso-27005-analisis-de-riesgos/

LARA MUÑOZ, Érica María. Fundamentos de investigación un enfoque por competencias. México: Alfaomega, 2011. 292 p.

LOPEZ NEIRA, Agustín. Sistemas de gestión de seguridad de la información [en línea]. Bogotá: ISO 27000, 2015 [fecha de consulta 3 de junio de 201]. Disponible en: http://www.iso27000.es/sgsi.html

MARKUS ERB. Gestión de riesgos en la seguridad informática [en línea]. Bogotá: Wordpress, 201 [fecha de consulta 3 de junio de 2017]. Disponible en: https://protejete.wordpress.com

MORENO, Andrea y ALARCÓN, Mariana. Gestión de riesgos y conformidad normativa. [en línea]. Bogotá: Blogspot, 2011 [fecha de consulta 7 de junio de 2017]. Disponible en: http://gestionriesgos2011.blogspot.com.co/2011/02/gestion-de-riesgos-informaticos.html

PORTAL DE ISO 27001 EN ESPAÑOL. ¿Qué es un SGSI? [en línea]. Bogotá: ISO, 2016 [fecha de consulta 7 de marzo de 2017]. Disponible en: http://www.iso27000.es/sgsi.html

PORTAL ISO 27000. Introducción a los sistemas de gestión de seguridad de la información. [en línea]. Madrid: ISO 27000, 2010 [fecha de consulta 3 de junio del 2017]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo en “texto claro”. [en línea]. Bogotá: MAGAZCITUM, 2013 [fecha de consulta 3 de junio de 2017]. Disponible en: www.magazcitum.com.mx/?p=2193#.WWKCUoQ1_IU

RECI. María de Jesús. De la seguridad informática a la seguridad de la información. En: Revista Calidad. Julio-septiembre, 2012. no. 5

REPUBLICA DE COLOMBIA, área de investigación y planeación. Modelo de seguridad de la información- sistema SANSI – SGSI – Modelo de seguridad de la información para la estrategia del gobierno en línea. Diciembre del 2008.

RUIZ SPOHR Javier. Sistemas de gestión de seguridad de la información [en línea]. Bogotá: ISO 27000, 2014 [fecha de consulta 3 de junio de 2017]. Disponible en: http://www.iso27000.es/sgsi.html