FACULTAD DE POSTGRADOS

# PROYECTO DE IMPLEMENTACION DE UN PROGRAMA DE SEGURIDAD DE LA INFORMACION

AUTOR

Arellano Moncayo, Fabricio Gerardo

AÑO

2021

# UNIVERSIDAD DE LAS AMERICAS

FACULTAD DE POSTGRADOS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PROYECTO DE IMPLEMENTACION DE UN PROGRAMA DE SEGURIDAD DE LA INFORMACION

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magíster en Gestión de la Seguridad de la Información.

Autor:

Fabricio Gerardo Arellano Moncayo

Año:

2021

AGRADECIMIENTOS

Quiero agradecer a todos los docentes quienes han compartido sus enseñanzas y experiencia sobre la seguridad de la información.

DEDICATORIA

Dedico este trabajo a mis padres quienes han guiado y motivado mis proyectos con su apoyo incondicional.

## RESUMEN EJECUTIVO

El presente proyecto, tiene como objetivo señalar las diferentes consideraciones respecto a la implementación de un programa de seguridad de la información.

El objetivo del proyecto, es guiar a una empresa seleccionada a que se implemente un programa de seguridad; entendiéndose como programa al conjunto de actividades, procesos y mediciones para mantener y mejorar la seguridad de la información a lo largo del tiempo.

Estas actividades se encuentran plasmadas en el presente proyecto como las siguientes fases:

- Diagnóstico
- Clasificación de la información
- Inventario de activos de información
- Análisis de amenazas y vulnerabilidades de activos de información críticos.
- Generación de documentos claves del SGSI
- Operación

El alcance del presente proyecto contempla las 5 primeras fases, ya que en la sexta fase se pondrían a trabajar todos los planes, procesos y políticas definidas en las anteriores fases.

Cada una de las fases señaladas contempla la generación de documentos, que permiten documentar los hallazgos de cada fase y que permiten entender de mejor forma el estado actual de la empresa y las acciones que se deben ejecutar para generar mejoras o implementar lineamientos de seguridad entre otras actividades.

Los documentos desarrollados en el presente trabajo, se basan en marcos de referencia ampliamente utilizados como Cobit, ISO 27001, NIST que señalan lineamientos, métricas y recomendaciones que permiten alimentar al programa de seguridad reforzar el funcionamiento de la seguridad de la información, así

como para perseguir la mejora continua al medir las actividades y reforzar las políticas y controles señalados en este documento.

Finalmente, se incluye un listado de proyectos que contienen actividades para alimentar al programa de seguridad y que se ejecutarán dentro de la fase de operación del programa de seguridad de la información. Estos planes tienen un estimado de tiempo y de presupuesto como una referencia a las actividades que conllevan esas tareas.

## ABSTRACT

The present project aims to point out the different considerations regarding the implementation of an information security program.

The objective of the project is to guide a selected company to implement a security program; understanding as a program the set of activities, processes and measurements to maintain and improve information security over time.

The activities that are included in this project will be contained in the following phases:

- Diagnosis
- Information classification
- Inventory of information assets
- Analysis of threats and vulnerabilities of critical information assets.
- Generation of key documents of the ISMS
- Operation

The scope of this project includes the first 5 phases, since in the sixth phase would be the implementation of all the plans, processes and policies defined in the previous phases.

Each of the aforementioned phases contemplates the generation of documents, which allow documenting the findings of each phase and which allow a better understanding of the current state of the company and the actions that must be taken to generate improvements or implement security guidelines, among others activities.

The documents developed in this project are based on widely used reference frameworks such as Cobit, ISO 27001, NIST that indicate guidelines, metrics and recommendations that allow the security program to be fed to reinforce the operation of information security, as well as to pursue continuous improvement by measuring activities and reinforcing the policies and controls indicated in this document.

Finally, a list of projects is included that contain activities to feed into the security program and that will be executed within the operation phase of the information security program. These plans have a time and budget estimate as a reference to the activities that these tasks entail.

# ÍNDICE

# INTRODUCCIÓN

El proyecto de la implementación del programa de seguridad de la información pretende analizar un caso de estudio y establecer lineamientos sobre seguridad de la información.

Para el caso de este documento, se ha tomado en cuenta la definición de programa de seguridad de la información del fabricante ESET que señala que un programa de seguridad de la información es "un conjunto de proyectos, iniciativas y actividades realizadas de manera coordinada para lograr una estrategia de seguridad, es decir, llevar a la práctica un plan trazado que busca alcanzar los objetivos de protección de una organización."[1] (Mendoza, 2017).

Para que el programa de seguridad de la información pueda iniciar es necesario definir el estado actual de la empresa, de sus políticas y controles, así como tener una idea clara sobre los riesgos que la empresa ha venido abordando y las acciones que la empresa ha definido para tratar referente a la seguridad de la información.

La segunda consideración que se desarrollara a lo largo del presente proyecto y en consonancia con la definición antes vista es el análisis de las actividades que se propondrán como parte del análisis que se ejecutan en cada fase. Estos análisis utilizan marcos de referencia tales como Cobit, NIST, ISO 27001 entre otras que ayudarán a este programa de seguridad de la información a proponer planes para alcanzar los objetivos de seguridad que tiene la empresa.

Finalmente, la última consideración a tener en cuenta vendrá de las conclusiones y hallazgos de cada una de las fases que llevarán a brindar consideraciones aterrizadas al estado de la empresa y lo que se espera alcanzar luego de la evaluación de cada una de las fases.

[1] We Live Security, ESET. "Cómo desarrollar y aplicar un programa de seguridad de la información". Tomado de: https://www.welivesecurity.com/la-es/2017/01/11/desarrollo-programa-de-seguridad-informacion/

# DESARROLLO DEL PROYECTO

# FASE 1 – DIAGNÓSTICO

La fase de diagnóstico permitirá conocer el estado actual de la empresa en los temas relacionados con la seguridad de la información, así como definir los objetivos y metas que la empresa busca obtener al implementar un programa de seguridad de la información. En esta fase, se hará la revisión de 3 entregables que son el Caso de Negocio del Proyecto, la Metodología de evaluación del Estado Actual del Sistema de Gestión de Seguridad de la Información (SGSI) y el Informe de Estado Actual del Sistema de Gestión de Seguridad de la Información (SGSI).

## 1. Análisis del Caso de Negocio del Proyecto

El documento sobre el Caso de Negocio tiene por objetivo identificar las condiciones iniciales del proyecto, las necesidades y motivaciones iniciales que tendrá el proyecto, así como una estructura de tiempo y costos. En esta sección se señalarán las partes más importantes sobre el caso de negocio.

### 1.1. Objetivo del Proyecto

El objetivo principal del proyecto es implementar un programa de seguridad de la información, basado en marcos de referencia como ISO 27001 y 27002 para brindar lineamientos y políticas de seguridad actualizadas; así como identificar bases para un gobierno de IT dentro de la organización.

## 1.2. Alcance del Proyecto

Como parte del alcance de la implementación de este proyecto contempla lo siguiente:

- Evaluar e identificar el estado actual de las políticas y controles de seguridad existentes.
- Evaluar e identificar los riesgos asociados a 1 activo de información crítico.
- Proponer políticas y controles que mejoren la seguridad de la información en relación a los activos críticos de información.
- Proponer políticas de seguimiento y mejoras que permitan medir y evaluar la gestión de la seguridad y su alineación con los objetivos del negocio.

## 1.3. Expectativas del Proyecto

Se busca con la propuesta de implementación del programa de seguridad de la información y la actualización del SGSI alcanzar y cubrir las siguientes necesidades de la empresa:

- Establecer un sistema de gestión de seguridad de la información que funcione, se mantenga en el tiempo y se evalué con apoyo externo para su mejora.
- Definir políticas y métodos de protección de la información que administra la empresa basado en la Confidencialidad, Integridad y Disponibilidad y considerando en los casos que amerita la Privacidad.
- Establecer el cumplimiento efectivo de las regulaciones y obligaciones relacionadas a la seguridad de la información para las unidades de negocio.

## 1.4. Beneficios de implementar el proyecto

Como parte de los beneficios implementar un Programa de seguridad están:

- Minimizar los riesgos asociados a los activos críticos, así como el impacto de estos riesgos; lo que ayuda a una mejor entrega de servicios a otras empresas.
- Entregar servicios de tecnología al cliente interno y externo, en donde se tenga en cuenta temas de seguridad de la información.
- Respaldar el alcance de los objetivos del negocio basado en una inversión adecuada en soluciones IT y alineando estas con las necesidades actuales y futuras de la empresa.
- Mejorar la gestión de activos y procesos relacionados a IT, por medio de políticas y procesos más apegados a la realidad de las empresas en el tiempo.
- Reforzar la imagen empresarial al incluir características de seguridad en la entrega de servicios a los clientes potenciales.

## 1.5. Fases del proyecto

Estas son las fases contempladas en el proyecto:

1. Análisis y Diagnóstico del SGSI Actual
2. Clasificación de los tipos de la información y los activos de Información
3. Inventario de Activos de Información
4. Análisis de amenazas y vulnerabilidades de los activos críticos seleccionados
5. Elaboración de Documentos Claves del SGSI
6. Operación


Figura 1. Diagrama de fases del proyecto, tomada del material en clase sobre el proyecto de Titulación, UDLA 2021.

La fase de Operación se ejecutará una vez que las 5 primeras fases se encuentren aprobadas por la gerencia con la documentación y entregables a presentarse.

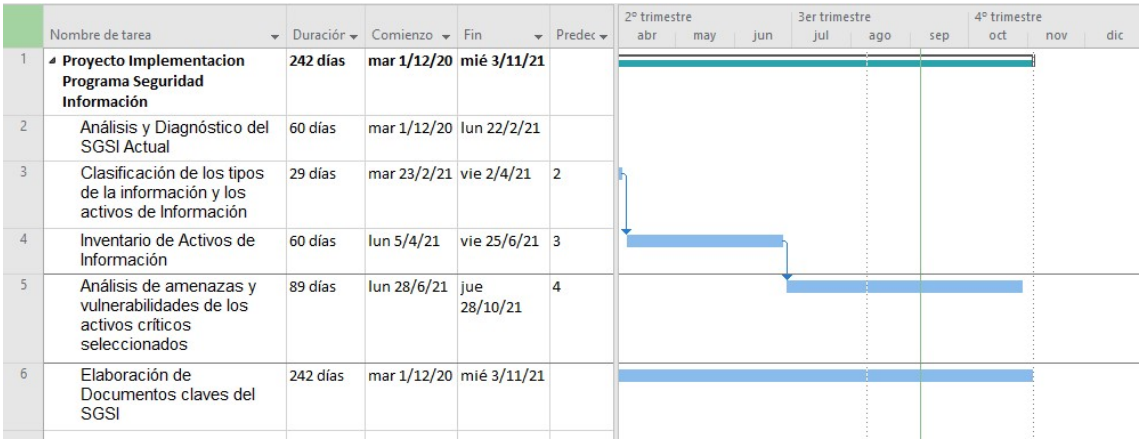
## 1.6. Entregables del Proyecto

Como parte de los entregables del proyecto considerarán los siguientes entregables:

- Informe de Evaluación del estado actual de la Gestión del SGSI
- Clasificación de los tipos de Información
- Activos de Información críticos identificados y clasificados
- Análisis de amenazas y vulnerabilidades de un activo de información crítico
- Documento que incluye objetivo, políticas de alto nivel, roles y Responsabilidades de alto nivel, Procesos clave.
- Programa de mejora continua del SGSI incluyendo los proyectos, planes de acción definidos.

## 1.7. Cronograma del Proyecto

En la figura 2 se adjunta el cronograma del proyecto, que incluyen las 5 primeras fases del proyecto.



| | Nombre de tarea | Duración | Comienzo | Fin | Predec |
|---|---|---|---|---|---|
| 1 | **Proyecto Implementacion Programa Seguridad Información** | **242 días** | **mar 1/12/20** | **mié 3/11/21** | |
| 2 | Análisis y Diagnóstico del SGSI Actual | 60 días | mar 1/12/20 | lun 22/2/21 | |
| 3 | Clasificación de los tipos de la información y los activos de Información | 29 días | mar 23/2/21 | vie 2/4/21 | 2 |
| 4 | Inventario de Activos de Información | 60 días | lun 5/4/21 | vie 25/6/21 | 3 |
| 5 | Análisis de amenazas y vulnerabilidades de los activos críticos seleccionados | 89 días | lun 28/6/21 | jue 28/10/21 | 4 |
| 6 | Elaboración de Documentos claves del SGSI | 242 días | mar 1/12/20 | mié 3/11/21 | |



Figura 2. Cronograma Inicial del proyecto

Este cronograma contempla 242 días en donde se ejecutarán cada una de las fases y se harán las revisiones respectivas con los Gerentes Técnico y Gerente General de la empresa.

## 1.8. Premisas del Proyecto

Para el presente proyecto se han considerado las siguientes premisas:

- La disposición de los socios para actualizar el SGSI e implementar un programa de seguridad acorde a las necesidades de la empresa.
- El acceso a la información existente referente a la documentación de seguridad definida anteriormente.
- La disponibilidad de reuniones con el Gerente técnico actual y el Gerente General de 2 horas por semana para consultas.

## 1.9. Limitaciones del Proyecto

Para el presente proyecto se han considerado las siguientes limitaciones:

- El personal que trabaja en el área de TI que estarían a cargo del programa tienen poca experiencia en temas de seguridad de la información.
- Existe un presupuesto limitado para las inversiones en tecnología y seguridad de la información.

## 1.10. Costos relacionados a la Implementación del Proyecto

Para que el proyecto pueda cumplir con los objetivos establecidos, se han identificado algunos recursos que ayudarán a conseguir los objetivos que persigue la implementación del programa de seguridad de la información. Estos costos se los puede apreciar en la tabla 1.

| **Recurso** | **Costo Anual** |
|---|---|
| Personal encargado de las políticas de seguridad de la información y soporte de políticas de seguridad para empresa. 1 Recurso | $ 12000 |
| Auditoría externa respecto al SGSI | $ 3000 |
| Inversión en tecnología de seguridad de la información | $ 8000 |
| Consultor Informático para revisión semestral | $4000 |
| Licencia para Software de Seguimiento de SGSI | $3500 |

Tabla 1. Estimación de Costos anual del proyecto

El cálculo de los recursos se lo ha hecho anualmente, tomando en consideración las actividades que ayuden al SGSI a mantenerse y mejorar en el tiempo, así como un responsable de mantener y seguir las actividades de seguridad dentro de la empresa.

## 1.11. Conclusiones sobre el Caso de Negocio

El caso de negocio ofrece una visión amplia de lo que busca el proyecto, así como algunos datos de vital importancia en un proyecto que son el tiempo del proyecto, las fases que abarca y los resultados que se esperan obtener del proyecto.

Al tener que implementarse un programa de seguridad de la información, el tener este documento servirá como una guía de hacia dónde debe llegar la empresa seleccionada y servirá como arranque de la Fase 1, que hace referencia al Diagnóstico de la organización.

Para entender un poco más sobre la organización, se ha incluido en el documento una sección sobre la empresa, sus actividades, procesos clave, así como su estructura organizacional y su esquema de funcionamiento desde el punto de vista de tecnología. Esta información se encuentra en el Anexo 1 – Caso de Negocio.

# 2. Metodología de evaluación del Estado Actual del SGSI

Para poder arrancar con la definición de seguridad que lleva la empresa al momento, es necesario definir en qué punto se encuentra la empresa respecto al manejo de la seguridad de la organización en sus diferentes actividades. Para ello, es necesario definir marcos de referencia y escalas de medición para definir acciones de mejora al estado de la empresa. Esta sección busca definir qué herramientas se consideraron para esta evaluación y el respectivo proceso de evaluación ejecutado.

## 2.1 Selección de la metodología de evaluación

Para el caso de la selección de la metodología de evaluación, se ha considerado utilizar a la ISO 27001 y su Anexo A(ISO27002). Este marco de referencia ha sido ampliamente utilizado como un conjunto de prácticas y procedimientos sobre seguridad de la información. Según CEDIA, el marco de referencia ISO 27001:2013 “proporciona un enfoque común y una estructura para las normas de los sistemas de gestión que se presta más fácilmente para la integración con otras normas de sistemas de gestión”[2], lo que ha ayudado a que sea incorporada con otras prácticas y ampliamente conocida en el mundo.

A su vez, se ha adaptado los lineamientos de la ISO 27002, como un conjunto de prácticas y definiciones de políticas que ayudan en la gestión de las actividades que se señalan en el marco ISO 27001.

[2] CEDIA (2014), “Gestión de la Seguridad”, tomado de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf, Pág. 21

## 2.2 Selección de la escala de medición

Una vez definido que se debe medir, es necesario definirle una escala, para esto se ha tomado en cuenta el modelo de medición que maneja Cobit 2019 que realizar la Integración del Modelo de Madurez de Capacidad o CMMI. La figura 3 muestra el esquema de este modelo que Cobit 2019 lo adapta.

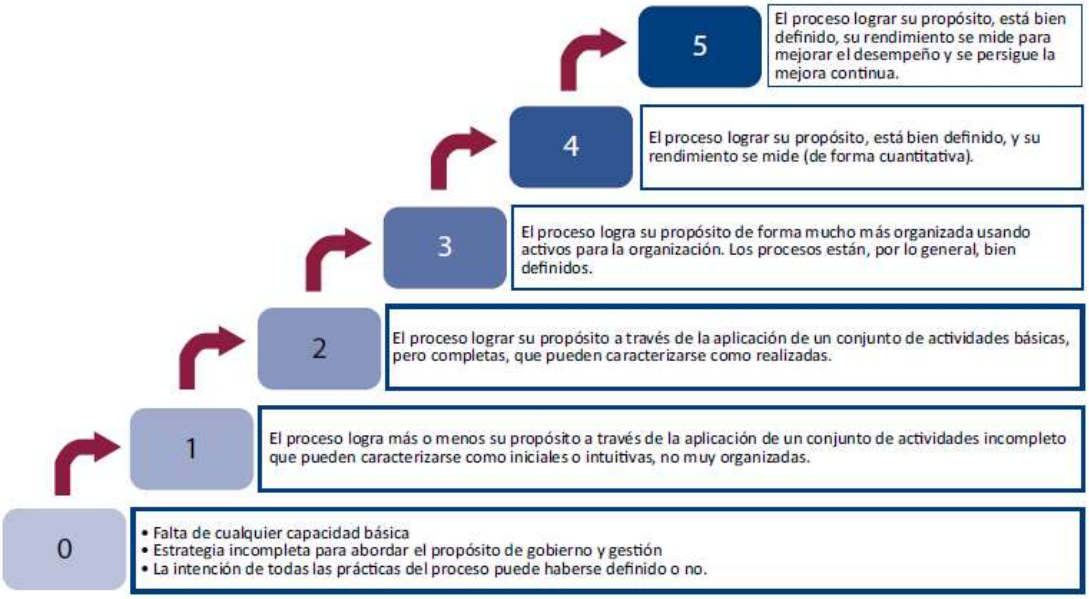



Figura 3. Modelo de Medición de Madurez, tomada de Cobit 2019[3]

En este modelo se puede apreciar que existen varios niveles, cada nivel señala la madurez de un proceso en base a que tan bien se ejecuta ese proceso. Tomando en consideración este modelo de madurez, se ha definido una escala personalizada que se utilizará para medir la madurez de los diferentes Ítems que componen los macros de referencia ISO 27001 y 27002. La tabla 2 muestra el resultado de la escala de medición que se utilizó para evaluar la madurez.

[3] ISACA. (2019). “Cobit 2019: Objetivos de gobierno y gestión”. Pág. 20.

| Valor | Efectividad | Significado | Descripción |
|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. |
| 3 | 65% | Proceso definido | La organización participa en el proceso. Los procesos están formalizados, implantados, documentados y comunicados. |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. |

Tabla 2. Escala de medición personalizada sobre los niveles de madurez.

En este caso, cada escala tiene asociada una noción sobre la madurez de cada proceso referente a lo que muestra los diferentes capítulos de la ISO 27001 y el listado que expone la ISO 27002. La figura 4 muestra la estructura de como se observa el formato de la evaluación ejecutada.

| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Código de Plan de Acción |
|---|---|---|---|---|---|
| 8 | Operación | | | | |
| 8.1 | Planificación y control operacional | | | | |

Figura 4. Estructura de la evaluación de las secciones de los marcos de referencia ISO 27001-27002.

En este caso, en la columna “Requerimientos obligatorios para el SGSI” se incluyó el ítem a ser evaluado referente a cada una de las secciones que señala ISO 27001/ISO27002. El campo “Valoración” contiene la escala de madurez asignada, la columna “Estado Actual” muestra la justificación de la valoración. Los campos “Planes de Acción” y Código de Plan de Acción” hacen referencia a

los planes de mejora que pueden aplicar y que se verán con mayor detalle en el entregable “Programa de mejora continua del SGSI”.

Para poder evidenciar los resultados a detalle en las mediciones, es necesario revisar el Anexo II – Medición de Madurez del SGSI.

## 2.3 Conclusiones sobre la selección de la metodología.

El haber utilizado el marco de referencia de las ISO 27001/27002 ayudó a estructurar la medición de forma clara y concisa, adicionalmente esta estructura ha hecho que la evaluación tenga una visión más amplia de lo que cubre un Sistema de Gestión de Seguridad de la Información o SGSI. Junto con las escalas del nivel de madurez expuestos por Cobit 2019 hacen un gran conjunto para determinar el estado de la seguridad de la información de la empresa.

A pesar de que ISO 27001/27002 es un esquema ampliamente utilizado, no es el único ya que existen otros buenos marcos de referencia como NIST que se verán más adelante, en otras secciones del presente documento.

# 3. Informe del estado actual del SGSI

Para el caso del informe del estado actual, que recopila los hallazgos obtenidos sobre las evaluaciones generadas por el previo entregable, brinda un resumen de cómo está la empresa en cada una de las secciones que señala la ISO 27001 y también se hace un análisis general de lo que señala la ISO 27002.

## 3.1 Resultado de las mediciones sobre ISO 27001

Al realizar la evaluación de cada Ítem/Sección que señala el marco de referencia de ISO 27001 se puede observar el número de literales/secciones que han sido evaluadas en los diferentes niveles de madurez. La tabla 3 muestra el resultado de la medición de los controles ofreciendo un valor sumariado.

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 0 |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. | 24 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. | 77 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. | 9 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. | 0 |

Tabla 3. Nivel de madurez medido en los ítems del marco de referencia ISO 27001

Ahora, en la figura 5 se puede apreciar la distribución de los niveles de madurez versus el número de ítems evaluados dentro de ISO27001.

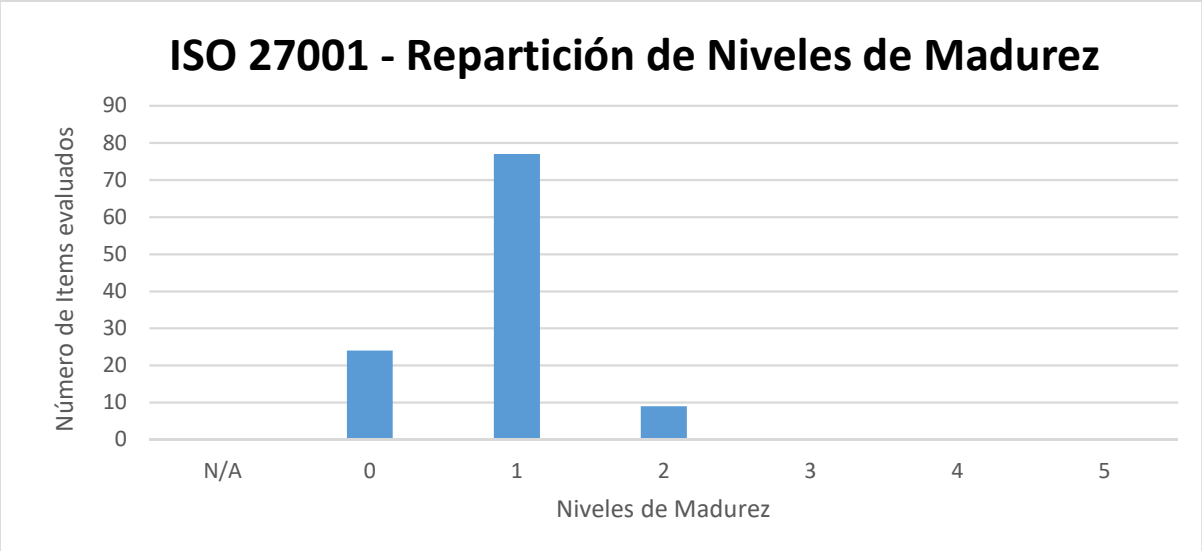



Figura 5. Repartición de los Niveles de Madurez calificados en conjunto con en el marco de referencia ISO 27001

La distribución muestra que existe una tendencia marcada a que los elementos analizados por ISO 27001 están en su mayoría en un nivel de madurez 1, seguidos por los ítems con niveles de madurez de 0 y finalmente unos pocos ítems con nivel de madurez 2. Cabe mencionarse que no existen políticas calificadas con un nivel de madurez 3 o superior.

Ahora, para poder determinar qué áreas o secciones son las que necesitan un mayor enfoque se ha definido la tabla 4, aquí se puede apreciar las áreas que necesitan un enfoque de completitud de los ítems del marco de referencia de la ISO 27001. Como existe una tendencia marcada de ítems evaluados con un nivel de madurez 1 o 2 se los agrupo en la columna llamada “Mayor o igual a 1”, por otro lado, la columna “Igual a 0” lleva el número de objetivos que han sido calificados con un 0. No existen ítems en esta parte que hayan sido calificados como “No Aplica” (N/A). la columna “Nro. Ítems” contiene el total de políticas que tiene asociada esa sección. Finalmente, la columna “Promedio” ha sido calculada como un promedio de los niveles de madurez de los controles asociados a esa sección.

| Dominio | Promedio | Nro. Ítems | Mayor o igual a 1 | Igual a 0 |
|---|---|---|---|---|
| 4.- Contexto de la organización | 1.13 | 8 | 8 | 0 |
| 5.- Liderazgo | 1.06 | 17 | 15 | 2 |
| 6.- Planificación | 0.90 | 29 | 26 | 3 |
| 7.- Soporte | 0.90 | 25 | 23 | 2 |
| 8.- Operación | 1.00 | 3 | 3 | 0 |
| 9.- Evaluación y Desempeño | 0.45 | 20 | 9 | 11 |
| 10.- Mejoramiento | 0.25 | 8 | 2 | 6 |

Tabla 4. Distribución resumida de los niveles de madurez junto con las secciones del marco de referencia ISO 27001

Para poder comprender mejor las áreas de enfoque, se puede visualizar los datos en una forma gráfica, tal como se expone en la figura 9.


Figura 6. Comparativa de los ítems con madurez versus las secciones del marco de referencia ISO 27001

En esta gráfica, se puede observar que las secciones 4, 5, 6, 7 y 8 muestran que cuentan ítems ya existentes; además se puede ver que en estas secciones el número de ítems que tienen niveles de madurez 0 son bajos. Por el contrario, en las secciones 9 y 10 existe un mayor número de ítems que fueron evaluados con un nivel de madurez de 0.

## 3.2 Resultado de las mediciones sobre ISO 27002

Para el caso de la evaluación de los objetivos descritos en el marco de referencia ISO 27002 se ha mantenido el mismo esquema de evaluación. En esta sección se hizo una evaluación de 119 puntos que hacen referencia a controles que pueden estar implementados dentro de la empresa en forma de políticas de seguridad que ayuden al complimiento de los ítems descrito en la ISO 27001. La tabla 5 muestra el número de ítems evaluados respecto a la escala de nivel de madurez.

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 4 |
| 0 | 0% | Inexistente | Carencia completa de cualquier proceso conocido. | 19 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales. | 71 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual | 25 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos | 0 |

Tabla 5. Nivel de madurez medido en los ítems del marco de referencia ISO 27002

La distribución de la tabla 5 muestra una tendencia marcada en que existe un número alto de políticas en el nivel de madurez 1, seguido del número de políticas calificadas con un nivel de madurez 2, seguidas por las políticas calificadas con un nivel de madurez 0 y al final contando con únicamente 4 políticas que no aplican al contexto de la empresa. Esta distribución se la puede apreciar de forma gráfica y más clara en la figura 7.

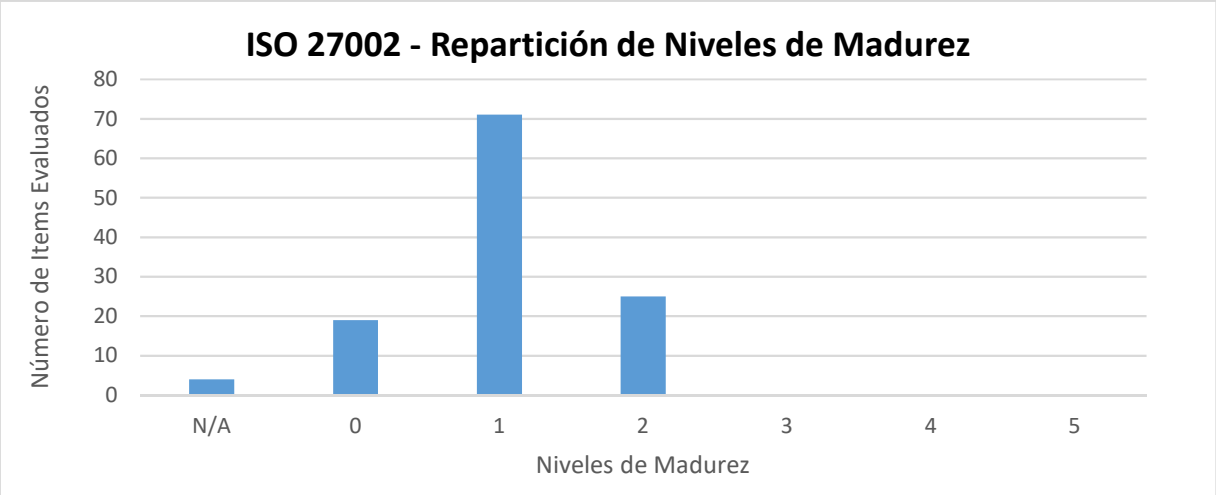



Figura 7. Repartición de los niveles de Madurez basados en el marco de referencia ISO 27002.

Esta figura muestra la tendencia anteriormente mencionada, que hace referencia al predominio del número de políticas calificadas con un nivel de madurez 1. Cabe mencionarse que no existen políticas calificadas con un nivel de madurez 3 o superior.

Como siguiente punto en el análisis, se ha incluido la distribución de las calificaciones sobre cada una de las secciones de la ISO 27002. Al verificarse anteriormente que las calificaciones no pasan el nivel de madurez 3, se ha decidido unir el conteo de las políticas evaluadas con nivel 1 y 2 en la columna “Mayor o igual a 1”, mientras que en la columna “Igual a 0” se han contabilizado aquellas políticas cuyo nivel de madurez fue calificado como 0; la columna “Nro. Ítems” contiene el total de políticas que tiene asociada esa sección. Finalmente, la columna “Promedio” ha sido calculada como un promedio de los niveles de madurez de los controles asociados a esa sección. Esta distribución se lo puede ver en la tabla 6.

| Dominio | Promedio | Nro. Ítems | Mayor o igual a 1 | Igual a 0 | No Aplica |
|---|---|---|---|---|---|
| Políticas de seguridad | 1.00 | 2 | 2 | 0 | 0 |
| Organización de la seguridad de la Información | 1.27 | 11 | 10 | 1 | 0 |
| Seguridad de los recursos humanos | 0.86 | 7 | 6 | 1 | 0 |
| Gestión de activos | 1.33 | 10 | 9 | 0 | 1 |
| Control de acceso | 1.29 | 14 | 14 | 0 | 0 |
| Criptografía | 2.00 | 2 | 1 | 0 | 1 |
| Seguridad física y del entorno | 1.07 | 15 | 13 | 2 | 0 |
| Seguridad en la Operación | 1.00 | 14 | 10 | 4 | 0 |
| Seguridad de las comunicaciones | 0.86 | 7 | 4 | 3 | 0 |
| Adquisición, desarrollo y mantenimiento de los sistemas de información | 1.00 | 13 | 10 | 2 | 1 |
| Relación con proveedores | 0.80 | 5 | 3 | 2 | 0 |
| Gestión de incidentes de seguridad de la información | 1.00 | 7 | 7 | 0 | 0 |
| Aspectos de seguridad de la información para la gestión de la continuidad de negocio | 0.50 | 4 | 2 | 2 | 0 |
| Cumplimiento | 0.86 | 8 | 5 | 2 | 1 |

Tabla 6. Distribución resumida de los niveles de madurez junto con las secciones del marco de referencia ISO 27002

De forma general, se puede ver que el número de políticas calificadas como iguales a cero son menores que las vistas en las calificaciones de las secciones vistas en la evaluación de ISO 27001. Por otro lado, también se puede ver que los promedios de las secciones son bastante cercanos a 1, a excepción de un par de valores.

Para ver una distribución gráfica de esta tabla, se ha añadido la figura 8 que muestra la distribución de las secciones con las calificaciones obtenidas por sección.

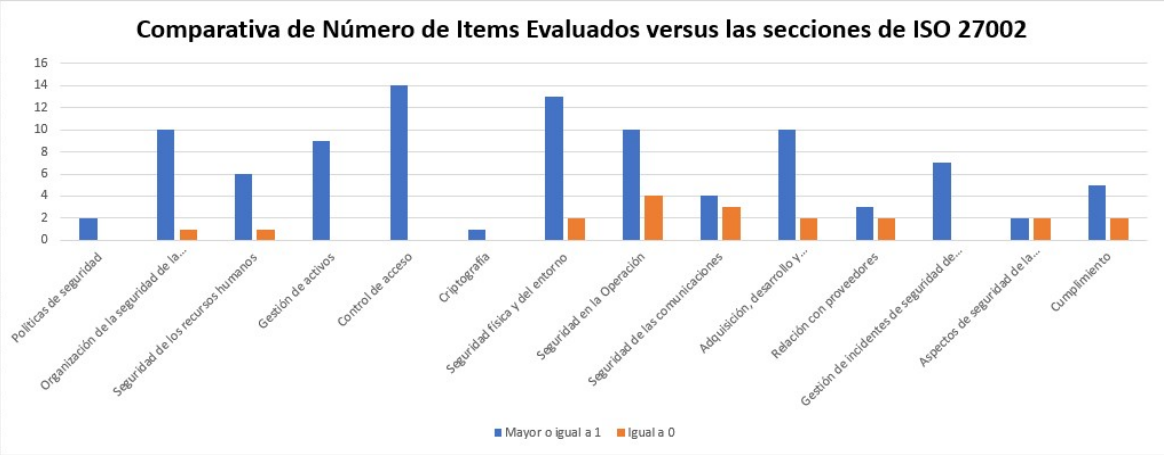



Figura 8. Comparativa de los ítems con madurez versus las secciones del marco de referencia ISO 27002

En esta gráfica se puede ver que la distribución de políticas evaluadas con un nivel de madurez de 1 o más se encuentra muy bien distribuida en todos los temas que maneja la ISO27002, en este caso no existe una sección con un número superior de políticas evaluadas con un nivel de madurez 0.

## 3.3 Conclusiones sobre la evaluación del SGSI

Respecto al análisis de los gráficos y las medidas tomadas se ha llegado a las siguientes conclusiones:

- Al realizarse las mediciones de madurez utilizando los ítems de los marcos de referencia ISO 27001/27002 se pudo evidenciar que su nivel de madurez mayoritariamente se encuentra en el nivel 1, por lo que los conceptos sobre seguridad de la información se encuentran en estados iniciales, por ende, es necesario cultivar mejores prácticas y definiciones sobre temas de seguridad de la información dentro de la empresa.
- Es importante señalar, que adicionalmente es necesario que la empresa tenga una revisión externa de los temas de seguridad a modo de consultorías para reforzar las prácticas y políticas e implementar prácticas que les hacen falta como el manejo de auditorías y el manejo de sus observaciones y no conformidades.

- Es necesario generar una capacitación y concienciación sobre la seguridad de la información dentro de la empresa y explicar los beneficios de la seguridad de la información en las operaciones del día a día de la empresa.

# FASE 2 – CLASIFICACIÓN DE LA INFORMACIÓN

La fase de clasificación de la información comprende entender que información maneja la empresa y que tan sensible es esa información respecto al apetito al riesgo que ha definido la empresa. Es importante mencionar que para que las políticas de seguridad de la información y el tratamiento de los riesgos sea eficiente, es necesario conocer que se va a proteger y cuál sería el impacto de no proteger adecuadamente.

## 4. Clasificación de Tipos de Información

Para este trabajo se ha realizado la clasificación de la información basado en el concepto de Entidad de Información. La Entidad de información no es nada más que aquel sujeto del cual se almacena información en una empresa. Según el giro de negocio la empresa pudiera tener varias entidades de las cuales maneja información y es necesario identificarlas.

### 4.1. Identificación de las Entidades de información.

Para el caso de la organización seleccionada, se han identificado las siguientes entidades:

- Clientes
- Proveedores
- Organización
- Cartera de los clientes
- Empleados

Cada una de las entidades tiene asociado uno o más tipos de información, estos tipos de información son clasificaciones de la información que maneja esta entidad.

En la tabla 7 se puede apreciar el ejemplo de que tipos de información tiene asociado la entidad clientes.

| Nro. | Nombre ENTIDAD | Nombre Tipo de Información | Descripción Tipo de Información |
|---|---|---|---|
| 1 | Clientes | Información de contacto del cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. |
| 2 | | Información Financiera del Cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. |
| 3 | | Información de Prospecto del Cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. |

Tabla 7. Tabla que contiene la información que se asocia a la entidad “Clientes”

En este caso, se ha clasificado que la entidad Clientes posee 3 tipos de información, la información de contacto del cliente, la Información Financiera del Cliente y la Información de Prospecto del Cliente. Cada uno de estos tipos de información esta descrito en que información se encuentra descrita dentro de cada Tipo de Información. Así se puede clasificar de mejor manera la información que maneja la empresa.

Se pudo identificar 19 Tipos de Información diferente que se encuentra asociada a las entidades señaladas anteriormente. Para ver a mayor detalle la definición de entidades se debe revisar el Anexo 4 que hace referencia a la definición y evaluación de entidades de información.

## 4.2. Identificación del apetito al riego de la empresa.

El riesgo es un concepto ampliamente definido en mucha literatura y marcos de referencia, para el caso de presente documento se tomará en cuenta el termino de riesgo definido en la ISO 31001, en donde "el riesgo se define como la incertidumbre que surge durante la consecución de un objetivo"[4].

El riesgo como tal se encuentra presente en cada actividad de la empresa, por lo que es necesario definir los principales riesgos que afronta la empresa y determinar en una escala el impacto de las mismas. En la tabla 8 se puede apreciar como columnas los riesgos más importantes para la empresa, y a modo de filas se ha determinado escalas de impacto a tomarse en cuenta para cada riesgo.

| | Impacto | | | | |
|---|---|---|---|---|---|
| | **Escala numérica** | **Pérdidas Financieras** | **Interrupción de operaciones parciales y/o totales** | **Multas y Sanciones de los Organismos de Control** | **Perdida de Cartera** |
| Catastrófico | 5 | Perdidas mayores al 30% del ingreso neto | | Mayor a 3 sanciones al año | Perdida de 4 o más clientes |
| Mayor | 4 | Perdidas mayores al 15% y menores al 30% del ingreso neto | Perdida del servicio mayor a 8 horas y menor a 12 horas. | Mayor a 2 sanciones al año | Perdida de 2 o 3 clientes |
| Moderado | 3 | Perdidas mayores al 8% y menores al 15% del ingreso neto | Perdida del servicio mayor a 4 horas y menor a 8 horas | Mayor a 1 sanciones al año | Perdida de 1 cliente |
| Menor | 2 | Perdidas mayores al 3% y menores al 8% del ingreso neto | Perdida del servicio mayor a 2 horas y menor a 4 horas | | |
| Insignificante | 1 | Perdidas menores al 3% del ingreso neto | Perdida de servicio menor a 2 horas | | |

Tabla 8. Tabla con la definición de riesgos de la empresa y sus diferentes impactos.

También es necesario definir una escala de probabilidades, la cual ayudará de forma cuantitativa y cualitativa definir la probabilidad que un riesgo se manifieste, la tabla 9 muestra dicha información.

[4] ISOTools. "Norma ISO 31000. El valor de la gestión de riesgos en las organizaciones". Tomado de https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

| Probabilidad | | |
|---|---|---|
| | % | Descripción |
| 5 | 100% | Casi Certeza |
| 4 | 85% | Probable |
| 3 | 50% | Posible |
| 2 | 25% | Poco probable |
| 1 | 5% | Raro |

Tabla 9. Tabla con la definición de los diferentes niveles de probabilidades considerados.

La tabla 9 hace referencia a la probabilidad que se utilizó para los cálculos de riesgos y sus posibles impactos.

Como siguiente punto, la figura 9 muestra un cruce entre la probabilidad y el impacto considerado, esto para catalogar la criticidad de la información.

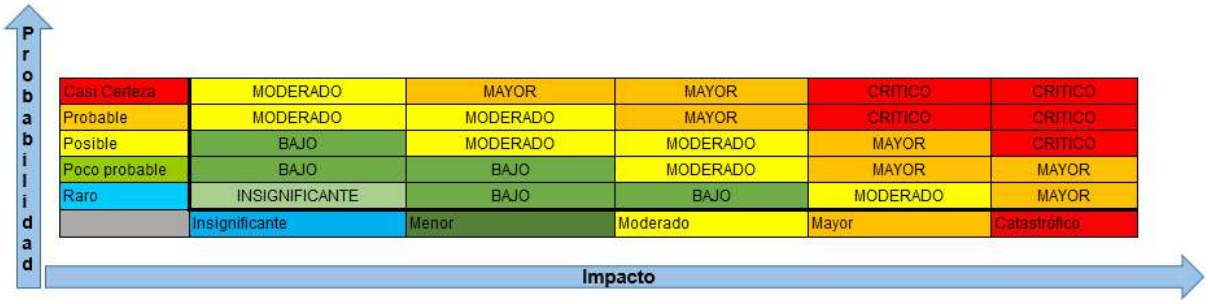



Figura 9. Tabla de referencia del Impacto versus la probabilidad para definir la criticidad.

## 4.3. Método de medición de la criticidad de los tipos de información

En el análisis ejecutado, la criticidad indica en una escala que va desde “Insignificante” hasta “Crítico” que tan sensible es el ítem evaluado en base a la relación Impacto/Probabilidad. Esta escala fue utilizada para evaluar de forma cualitativa las severidades sobre los tipos de información.

Como parte del desarrollo de este análisis, en el Anexo 4, se hizo una evaluación de los tipos de información que se manejan y se evaluó el impacto sobre la Confidencialidad, Integridad, Disponibilidad y en los casos que aplicaba se consideró la Privacidad, la cual hace referencia al manejo de datos personales.

La primera evaluación se la hizo de forma cuantitativa, calificando la afectación a la información en las áreas de Confidencialidad, Integridad, Disponibilidad y Privacidad en relación a los riesgos identificados inicialmente, tomando en consideración en esta calificación el impacto y la probabilidad como una sola calificación. Una vez hecha esta consideración, se hizo un promedio de los impactos en cada característica, y luego se asoció la criticidad en una escala a cada tipo de información.

La tabla 10 muestra la sección de la tabla del Anexo 4 que tiene este cálculo.

| Impacto Confidencialidad | Impacto Integridad | Impacto Disponibilidad | Impacto Privacidad | Calculo Impacto | Criticidad |
|---|---|---|---|---|---|
| 3 | 3 | 2 | 0 | 2.67 | Moderado |
| 4 | 5 | 3 | 0 | 4.00 | Crítico |
| 4 | 3 | 3 | 0 | 3.33 | Mayor |

Tabla 10. Extracto del cálculo de Impactos sobre los diferentes tipos de Información.

De esta evaluación cuantitativa, se obtiene en una siguiente tabla la evaluación de forma cualitativa para identificar los tipos de información que son sensibles para la empresa. De este análisis se pudieron detectar 2 entidades que contienen información crítica. Las tablas 11 y 12 muestran estas entidades y los tipos de información críticos identificados.

| Nro. | Nombre ENTIDAD | Nombre Tipo de Información | Impacto Confidencialidad | Impacto Integridad | Impacto Disponibilidad | Impacto Privacidad | Criticidad |
|---|---|---|---|---|---|---|---|
| 1 | Clientes | Información de Contacto del Cliente | Moderado | Moderado | Bajo | N/A | Moderado |
| 2 | | Información Financiera del Cliente | Mayor | Crítico | Moderado | N/A | Crítico |
| 3 | | Información de Prospecto del Cliente | Mayor | Moderado | Moderado | N/A | Mayor |

Tabla 11. Resultado de Evaluación de Criticidad de los tipos de información de la Entidad “Clientes”.

| Nro. | Nombre ENTIDAD | Nombre Tipo de Información | Impacto Confidencialidad | Impacto Integridad | Impacto Disponibilidad | Impacto Privacidad | Criticidad |
|---|---|---|---|---|---|---|---|
| 13 | Cartera de los Clientes | Información de contacto de la cartera del cliente. | Crítico | Mayor | Crítico | Mayor | Crítico |
| 14 | | Información de adquisiciones de la cartera del cliente. | Mayor | Mayor | Moderado | Crítico | Crítico |
| 15 | | Información de Gestión del Servicio de Atención a Clientes | Moderado | Moderado | Moderado | N/A | Moderado |
| 16 | | Información de Operación del Servicio Contratado | Moderado | Moderado | Moderado | N/A | Moderado |

Tabla 12. Resultado de Evaluación de Criticidad de los tipos de información de la Entidad “Cartera de los Clientes”.

De la Tabla 11 se puede concluir que el tipo de información que es más sensible o más crítica es la denominada “Información Financiera del Cliente”, mientras que los tipos de información más críticos para la entidad “Cartera de Clientes” son los denominados “Información de Contacto con el Cliente” y “Información de adquisiciones de la cartera del cliente”.

En esta segunda entidad se puede resaltar que, la Privacidad juega un papel fundamental ya que como esta información contiene Datos Personales es necesario ponerle un cuidado especial y adicional.

## 4.4. Conclusiones sobre la Clasificación de la Información.

La Clasificación de la información juega un papel muy importante y orientador en la seguridad de la información, ya que es necesario definir que se va a proteger y asegurar.

Además, de esta clasificación se pueden desprender varias formas de proteger y manejar los tipos de información, los cuales serán pilares fundamentales a considerarse en las futuras secciones del documento.

La clasificación de la información ayuda a visualizar los objetivos de seguridad de la información, sin embargo, este es el primer paso ya que es necesario identificar donde se encuentra esa información, que componentes manejan esa información. Este tema será revisado en la Fase 3 con mayor profundidad.

# FASE 3 – INVENTARIO DE ACTIVOS DE INFORMACIÓN

La fase de Inventario de activos de Información, hace alusión a que activos de información se manejan dentro de la empresa y guardan una estrecha relación con los Tipos de Información que se identificaron en la Fase 2. De esta fase se obtendrán los activos de información críticos, los cuales requieren un análisis de riesgos detallado.

## 5. Inventario de activos de Información

El siguiente hito que debe seguir en la planificación del programa es validar el inventario tecnológico de la empresa. Para iniciar, se ha solicitado a la organización un listado con todos los activos tecnológicos que se encuentren dentro de la empresa, el cual se puede ver en la tabla 13.

| Nro. Activo | Nombre Activo | Formato de Activo | Dueño del Activo |
|---|---|---|---|
| 1 | Servidor ERP/CRM | Físico | CFO - Gerente Financiero |
| 2 | Carpeta Compartida OC | Digital | CFO - Gerente Financiero |
| 3 | Servidor Información Contact Center | Digital | Supervisor Call Center |
| 4 | Firewall | Físico | CSO - Gerente Técnico |
| 5 | Switch Core Empresarial | Físico | CSO - Gerente Técnico |
| 6 | Switch Core Call Center | Físico | Supervisor Call Center |
| 7 | Session Border Controler | Físico | CSO - Gerente Técnico |
| 8 | Central Telefónica Cloud | Físico | CSO - Gerente Técnico<br>Supervisor de Call Center |
| 9 | Router Internet 1 | Físico | CSO - Gerente Técnico |
| 10 | Router Internet 2 | Físico | CSO - Gerente Técnico |
| 11 | Router Canal SIP 1 | Físico | CSO - Gerente Técnico |
| 12 | Router Canal SIP 2 | Físico | CSO - Gerente Técnico |
| 13 | Laptop Gerente General | Físico | CEO - Gerente General |
| 14 | Laptop Gerente Financiero | Físico | CFO - Gerente Financiero |
| 15 | Laptop Gerente Técnico | Físico | CSO - Gerente Técnico |
| 16 | Laptop Supervisor Call Center | Físico | Supervisor Call Center |
| 17 | Laptop Líder Desarrollo | Físico | Líder Desarrollo |
| 18 | Laptop Desarrollador 1 | Físico | Desarrollador 1 |
| 19 | Laptop Desarrollador 2 | Físico | Desarrollador 2 |
| 20 | Laptop Asesor 1 | Físico | Asesor 1 |

| | | | |
|---|---|---|---|
| 21 | Laptop Asesor 2 | Físico | Asesor 2 |
| 22 | Laptop Asesor 3 | Físico | Asesor 3 |
| 23 | Laptop Asesor 4 | Físico | Asesor 4 |
| 24 | Laptop Asesor 5 | Físico | Asesor 5 |
| 25 | Laptop Asesor 6 | Físico | Asesor 6 |
| 26 | Laptop Asesor 7 | Físico | Asesor 7 |
| 27 | Laptop Asesor 8 | Físico | Asesor 8 |
| 28 | Laptop Asesor 9 | Físico | Asesor 9 |
| 29 | Laptop Asesor Calidad | Físico | Asesor Calidad |
| 30 | Impresora Oficina | Físico | CSO - Gerente Técnico |
| 31 | Impresora Call Center | Físico | Supervisor Call Center |

Tabla 13. Inventario Tecnológico General de la Empresa

En este listado inicial, se han considerado todos los elementos de IT que existen dentro de la organización.

## 5.1. Definición de Activos Críticos de la Organización

Para el siguiente punto, que es la priorización de los activos de información se considerarán únicamente los equipos tecnológicos referente a la infraestructura sin considerar equipos personales o periféricos como impresoras, esto debido a que el impacto de la afectación en alguno de los componentes de IT es mayor que la afectación a estos componentes de uso empresarial, por lo que se trabajarán con los 12 primeros ítems de la tabla 13.

Con estos ítems, el siguiente paso ejecutado es el correlacionar que tipo de información se encuentra en que Activo de Información. Para el presente trabajo, se está considerando a un Activo de Información como un elemento organizacional que crea, genera, transmite y almacena información.

En el Anexo 4, en la sección “Activos de Información” se puede apreciar los 12 primeros ítems de la tabla 13 relacionados a los diferentes tipos de Información identificados en la fase 2.

De igual manera, en el Anexo 4, Sección “Definición Activos Críticos” se ha incluido también la definición de criticidad de cada Activo de Información considerando que cada Tipo de Información tiene asociado una criticidad definida, así llegando a determinar los Activos de Información Críticos. Al hacer esta analogía se puede concluir que un Activo de Información Crítico es un elemento organizacional que crea, genera, transmite y almacena información crítica.

Para poder resumir el trabajo que se encuentra en el Anexo 4, la tabla 14 muestra un resumen de cada Activo de Información y si es que este activo cuenta con al menos 1 Tipo de información que se haya catalogado como Crítica.

| Nro. Activo | Nombre Activo | Nro. Tipos de Información | Nro. Tipos Información Crítica | Prioridad |
|---|---|---|---|---|
| 1 | Servidor ERP | 6 | 1 | 4 |
| 2 | Carpeta Compartida OC | 11 | 0 | 5 |
| 3 | Servidor Información Contact Center | 4 | 2 | **3** |
| 4 | Firewall | 14 | 5 | **1** |
| 5 | Switch Core Empresarial | 11 | 1 | 4 |
| 6 | Switch Core Call Center | 4 | 2 | **3** |
| 7 | Session Border Controler | 2 | 0 | 5 |
| 8 | Central Telefónica Cloud | 3 | 1 | 4 |
| 9 | Router Internet 1 | 10 | 3 | **2** |
| 10 | Router Internet 2 | 4 | 2 | **3** |
| 11 | Router Canal SIP 1 | 1 | 0 | 5 |
| 12 | Router Canal SIP 2 | 1 | 0 | 5 |

Tabla 13. Inventario de Activos de Información Critica junto con su prioridad.

Inicialmente, se puede ver que los 12 Activos de Información Originales, 8 contienen al menos 1 Tipo de Información catalogado como crítica, por ende, se vuelven activos de información crítica. Para poder priorizar que activo crítico es prioritario se ha considerado evaluar el número de Tipos de información crítica que se procesas por ese activo, así obteniendo como prioridades en primer lugar al Firewall, en segundo lugar, al Router de Internet 1 y como tercer lugar lo comparten los activos de información “Servidor Información Contact Center”,

“Switch Core Contact Center” y “Router Internet 2”. Para todos estos activos es necesario definir un análisis de riesgos detallados y establecer mejoras para que estos componentes no sean afectados.

## 5.2. Conclusiones sobre Inventario de activos de Información

Si bien es cierto el conocer que activos y con cuantos activos de tecnología cuenta una organización; esto solo es el paso inicial a una identificación de activos de información crítica.

La identificación de los activos de información, es un proceso que debe llevarse en relación con la identificación de los tipos de información, ya que así se identifica que proteger y en donde se encuentra lo que se debe proteger.

Una vez que ya se ha definido la priorización de los activos críticos de información de la organización, es necesario evaluar que tan bien se encuentran protegidos, tema con el cual está relacionada la fase 4.

# FASE 4 – ANÁLISIS DE AMENAZAS Y VULNERABILIDADES DE ACTIVOS DE INFORMACIÓN CRÍTICOS

La fase de Análisis de amenazas y vulnerabilidades de activos de información críticos tiene como objetivo hacer una evaluación tanto sobre los riesgos, así como sobre los controles que se tienen para gestionar los riegos. En esta fase se verán el uso de marcos de referencia para evaluar los riesgos, las vulnerabilidades y así ir identificando los planes de mejora para gestionar los riesgos. En esta fase se hará la evaluación de riesgos del activo crítico denominado “Firewall” que resultó ser el equipo que maneja más tipos de información crítica.

## 6. Amenazas y Vulnerabilidades

Para poder avanzar en esta fase, es necesario revisar algunas definiciones sobre amenazas y vulnerabilidades. Se menciona también como estas amenazas puede impactar a la organización.

### 6.1. Definiciones sobre Amenazas y Vulnerabilidades

Para arrancar con las definiciones vistas durante el desarrollo de esta maestría, se puede definir el término vulnerabilidad como una debilidad o fallo en un componente de tecnología, haciendo posible que una amenaza pueda comprometer la integridad, disponibilidad o confidencialidad. Por otro lado, una amenaza puede ser definida como un evento o acción capaz de afectar negativamente a la seguridad de la información.

Al relacionar estos 2 conceptos, se puede concluir que una amenaza pudiera utilizar una vulnerabilidad para afectar a la seguridad de la información. Para

poder mitigar el impacto que tienen las diferentes vulnerabilidades es necesario definir medidas de control que pueden ser procedimientos, políticas, controles.

Una vez definidos estos términos, es necesario referenciar un tercer término de vital importancia en esta fase y es el denominado riesgo. El riesgo no es más que la probabilidad que una amenaza se aproveche o explote una vulnerabilidad, generando un impacto a la seguridad de la información, este impacto puede ser a la Confidencialidad, Integridad, Disponibilidad y si se puede aplicar a la Privacidad.

Para poder gestionar adecuadamente los riesgos, se han definido varios marcos de trabajo y para el presente documento se ha considerado utilizar a Magerit. Magerit responde a "Metodología de Análisis y Gestión de Riesgos para Sistemas de Información". Lo que Magerit hace es "implementar el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información."[5]

Este marco de referencia brinda guías para la implementación de la gestión de riesgos a activos previamente seleccionados, consideraciones que se han adaptado al Anexo 5.

[5] Ministerio de Hacienda y Relaciones Publica, España. "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método". Tomado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

## 6.2. Adaptación de Metodología Magerit

Para iniciar el proceso de adaptación de Magerit, al activo crítico seleccionado se le subdividió por capas. Por un lado, se tomó en cuenta en hardware como una capa y que hará referencia a los componentes físicos del activo de información. Por otro lado, se tomó en cuenta el software (Sistema Operativo) como una segunda capa y hará referencia a componentes lógicos y configuraciones del equipo.

Al dividir el activo de información en las diferentes capas, se pueden asociar estas capas a una clasificación de los diferentes activos/componentes que Magerit, los cuales se denominan Taxonomías. Las Taxonomías ayudan a identificar los roles que juegan esos componentes y señalan también los riesgos más comunes a los que están expuestos estos componentes.

Como siguiente punto Magerit ofrece un catálogo de medidas de control de riesgos, las cuales se denominan “Salvaguardas Esperadas”. La guía incluye la asociación de las salvaguardas con las taxonomías identificadas.

Otra de las bondades que Magerit ofrece, es que tiene ya catalogados riesgos dependiendo a los tipos de activos o taxonomías asociados a estos activos. En el caso de la evaluación de este documento, a las capas.

La figura 13 muestra la estructura que Magerit ofrece sobre los riesgos identificados.

### 5.2.6. [I.5] Avería de origen físico o lógico

| [I.5] Avería de origen físico o lógico | |
|---|---|
| **Tipos de activos:**<br>• [SW] aplicaciones (software)<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar | **Dimensiones:**<br>1. [D] disponibilidad |
| **Descripción:**<br>fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.<br>En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS:<br>28 - AVERÍA DEL HARDWARE<br>29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE | |

Figura 13. Ejemplo de enunciado de Riesgo en Magerit, tomado de Magerit[6].

Tomando en cuenta esta sección y la información sobre el activo crítico, en el Anexo 5 en la sección Análisis de Vulnerabilidades se ha realizado lo siguiente:

- Dividir el activo de información crítico seleccionado en capas o componentes.
- Asociar cada componente a las taxonomías que tiene cada capa o componente.
- Asociar las salvaguardas esperadas en base a las taxonomías asignadas.
- Identificar los riesgos más significativos por cada capa o componente.
- Identificar vulnerabilidades asociadas al riesgo expuesto, tomando en consideración la situación de funcionamiento de cada componente. El que uno de esos componentes no contase con una salvaguarda se consideraría como una vulnerabilidad.

[6] Ministerio de Hacienda y Relaciones Publica, España. “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de Elementos”. Tomado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

- Se calificó el riesgo en base a los moduladores de Impacto y Probabilidad expuestos en las tablas 8 y 9, y en base a esta parte, la severidad se fijó conforme la figura 9.
- Se generó un cálculo individual denominado “Severidad Individual” y para completar la severidad del riesgo, se añadió un campo denominado “Severidad General”

El ejemplo de un resultado de la asignación de severidades se lo puede ver en la tabla 14.

| Amenazas | Posibles Vulnerabilidades | Impacto | Probabilidad | Severidad Individual | Severidad General |
|---|---|---|---|---|---|
| I.5 Daño por averia fisica | No hay componentes de hardware de backup dentro de la empresa | Insignificante | Probable | MODERADO | MAYOR |
| | Los equipos tienen 4 años de ser adquiridos | Moderado | Probable | MAYOR | |
| | No hay mantenimiento físico en el hardware | Menor | Posible | MODERADO | |
| | No hay un análisis de impacto del negocio sobre el equipo | Moderado | Posible | MODERADO | |
| | No hay un plan de recuperación de desastres | Moderado | Probable | MAYOR | |

Tabla 14. Ejemplo de asignación de Severidades a los riesgos identificados.

Al concluir esta asignación, se tienen catalogados todos los riesgos asociados a ese activo de información crítica.

## 6.3. Evaluación de Controles

Una vez identificado los riesgos del activo de información crítico seleccionado, se debe evaluar los controles que estén asociado a ese riesgo en específico. Para este caso, se ha tomado 3 dimensiones de controles:

- Gobierno de IT: Hace referencia a los controles basados en planes de gobierno de IT, políticas y definiciones.
- Hardware: Hace referencia al análisis sobre los componentes de hardware y las políticas o controles asociados a problemas con hardware.
- Software: Hace referencia al análisis sobre los componentes de software, sistema operativo y configuraciones y las políticas o controles asociados a estos temas.

Al evaluarse los controles, si estos controles no existían o no cubrían los riesgos del todo, se generan oportunidades de mejora.

El proceso de evaluación de los controles, se lo puede encontrar en el Anexo 5, en las secciones:

- Análisis de Controles - Gob. IT
- Análisis de Controles - Hardware
- Análisis de Controles - Software

Las oportunidades de mejora identificadas, se encuentran documentadas en la sección “Resumen Planes de Acción”, y estas son parte de un entregable que se verá en la siguiente fase.

Estas oportunidades de mejora ayudarán a reforzar el programa de seguridad, y las mismas requieren de un esfuerzo y una planificación asociada.

## 6.4. Conclusiones sobre el análisis de amenazas y vulnerabilidades de activos de información críticos

La fase de análisis y amenazas es una de las fases más extensas de elaborar, ya que se requiere de una comprensión del entorno en el cual los activos de información están expuestos y contemplan múltiples escenarios.

El adaptar un marco de referencia en la gestión de riesgos es de vital importancia ya que guía al área de seguridad de la información con lineamientos importantes sobre los riesgos.

El manejo de los riesgos de seguridad de la información y su tratamiento debería ser elaborado en conjunto con la gerencia general, ya que es importante que estén conscientes de los riesgos y el tratamiento que le da la empresa, así como el impacto que tendría al no mitigar adecuadamente esos riesgos.

# FASE 5 – DOCUMENTOS CLAVE DEL SGSI

En esta fase se definen algunos documentos adicionales que ayudarán a definir actividades a ejecutarse en el programa y a delinear políticas para ser desarrollados en el programa de seguridad de la información. Existe también una definición de proyectos que el programa pueda alcanzar la evolución y mejora continua, que permitirá dar el impulso al programa en la fase de Operación.

# 7. Políticas de Alto Nivel

Las políticas de seguridad de la información tienen como objetivo definir lineamientos sobre la protección de activos de la información de la empresa, de la mano de procesos, prácticas, normas y documentación que permitan alcanzar los objetivos de seguridad de la información.

Las políticas expuestas en el presente documento tienen como referencia lo establecido en el marco de referencia ISO 27001 haciendo referencia a las diferentes secciones del marco de referencia.

## 7.1. Elaboración de las Políticas de Alto Nivel

Las políticas expuestas en Anexo 6 tienen como referencia lo establecido en el marco de referencia ISO 27001 haciendo referencia a las diferentes secciones de la ISO 27001 y adaptándose al estado actual de la empresa.

Por otra parte, para identificar la estructura de las políticas, se ha tomado la estructura del “Formato de Referencia de Política de Seguridad de la Información

–EGSI”[7], el mismo que señala una estructura que se compone de las siguientes consideraciones por política:

- **Descripción de la política:** Se señala una breve descripción de las políticas, y como estas políticas aportan a la empresa.
- **Objetivo:** Se señala cual es la meta de la política en la organización.
- **Roles y Responsabilidades:** En esta sección se mencionará quien o quienes serán los responsables de implementar, monitorear, evaluar e incluir mejoras a estas políticas.
- **Alcance:** Esta sección hará referencia a que componentes, procesos, personal de la empresa se hará aplicable la política.

En esta sección también se hace referencia a la **Comunicación de la política**, en este caso esta actividad se la hará por medio talleres de concienciación sobre las normas y la difusión del documento una vez que el programa de seguridad de la información inicie sus operaciones.

Las políticas que se pudieron definir son las siguientes:

1. Política de definición de objetivos de seguridad.
2. Política de seguimiento, medición y cumplimiento de objetivos de seguridad.
3. Política para la gestión de los riesgos de seguridad de la información.
4. Política de asignación de roles y responsabilidades dentro del programa de seguridad de la información.
5. Política de gestión de recursos de seguridad de la información.
6. Política de gestión de la documentación del sistema de seguridad de la información.
7. Política de operaciones seguras y gestión de incidentes
8. Política de Evaluación del desempeño del SGSI
9. Política de Auditorias de seguridad de la información

[7] Ministerio de Telecomunicaciones – Gobierno electrónico. “Formato referencial para la elaboración de la política de seguridad de la información (EGSI)”. Tomado de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/03/Formato-Referencial_Pol%C3%ADtica-de-Seguridad-de-la-Informaci%C3%B3n-EGSI.pdf

10. Política de mejora continua del SGSI
11. Política de seguimiento por parte de la alta dirección

El desarrollo a mayor detalle, así como la estructura se encuentra en el Anexo 6.

## 7.2. Conclusiones sobre las Políticas de Alto Nivel

Las políticas de alto nivel permiten definir los primeros escalones en la definición de las políticas de toda la empresa a nivel de la seguridad de la información. De estas políticas de alto nivel que hacen referencia a áreas en específico, al ir bajando deben ser más específicas a que área o elemento que van a cubrir.

Las políticas de alto nivel deben ser visionadas en cuanto a las áreas de necesidad de la empresa y como estas políticas pueden ayudar a las diferentes áreas o procesos de la empresa.

# 8. Definición del Modelo Operacional del SGSI y métricas de los procesos.

El modelo operacional del SGSI busca delimitar los pasos necesarios que se debe seguir el SGSI para que su operación se ejecute de mejor manera. Los modelos operacionales pueden construirse desde cero o ser adaptados desde marcos de referencia que señalen las etapas que deben seguir un SGSI.

## 8.1. Definición del modelo operacional.

Para este modelo operacional y siguiendo la estructura del NIST Cybersecurity Framework maneja un modelo de funcionamiento y operación en 5 etapas. El Marco de Referencia de NIST cita que "El Marco está diseñado para complementar las operaciones empresariales y de seguridad cibernética existentes. Puede servir como base para un nuevo programa de seguridad cibernética o un mecanismo para mejorar un programa existente." [8].

La figura 14 muestra el modelo de operación que propone NIST con respecto al SGSI.

[8] National Institute of Standards and Technology, NIST. "NIST Cibersecurity Framework". Tomado de: https://www.nist.gov/document/frameworkesmellrev20181102mncleanpdf Pág. 20


Figura 14. Gráfico sobre los pasos que comprende el modelo operacional basado en NIST, tomado de Forescout[9].

El Marco de referencia señala 5 áreas que se denominarán “Pasos”, ya que estos permiten delimitar las actividades que se hacen en cada etapa de operación del SGSI. Estos pasos cuentan con subdivisiones del proceso o identificadas como prácticas asociadas, que permiten completar el objetivo que persigue la práctica. En este marco de referencia en específico se incluyen referencias informativas hacia otros marcos de referencia, tales como ISO 27001, COBIT, NIST801, ISA, etc., para el caso de este análisis se ha tomado las referencias hacia COBIT 5 y COBIT 5 con enfoque a la seguridad.

Los pasos que se documentaron son los siguientes:

- **Paso 1 – Identificar:** Comprende desarrollar el entendimiento de la organización, así como su estado actual.
- **Paso 2 – Proteger:** Comprende la implementación de medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

[9] Forescout. “How to comply in 2020 with the 5 functions of the NIST Cybersecurity Framework”. Tomado de: https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/

- **Paso 3 – Detectar:** Comprende desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad.
- **Paso 4 – Responder:** Comprende el desarrollo e implementar actividades apropiadas para tomar medidas con respecto a un incidente.
- **Paso 5 – Recuperar:** Comprende determinar las acciones apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya afectado por incidentes de seguridad de la información.

De este cruce entre el marco de referencia NIST y COBIT, del segundo marco de referencia se han tomado las métricas asociadas a las Referencias Informativas que el marco de referencia NIST incluye, es por eso que en las métricas asociadas se incluyen las referencias a los objetivos de gobierno y gestión de donde se obtuvieron.

El desarrollo de estos pasos y las métricas principales asociados a cada paso se pueden observar en el Anexo 7.

## 8.2. Conclusiones sobre el modelo operacional.

Al definir un modelo operacional del SGSI, es posible definir las actividades asociadas a cada paso en base a las practicas señaladas por el marco de referencia y adaptar estos pasos a las políticas que la empresa necesite priorizar, haciendo un modelo apegado a las necesidades de la organización.

Las métricas asociadas a cada fase ayudarán a determinar que tan bien se está manejando el SGSI a lo largo del tiempo, así como evaluar su desempeño y las medidas para buscar la mejora continua de estas actividades.

# 9. Programa de mejora continua del SGSI

El programa de mejora continua del SGSI hace referencia a aquellos proyectos u oportunidades de mejora que se han ido identificado durante las fases 1 y 4; respectivamente se encuentran como parte de los Anexos 2 y 5.

Los planes se encuentran descritos en el Anexo 8, el cual cuenta con una tabla con las siguientes columnas y su propósito:

- **Código Plan:** Es el identificador del plan de acción, incluye un código único que ayuda a identificar de que Anexo se tomó.
- **Plan de Acción:** Es el nombre del plan de Acción, generalmente toma la idea principal respecto al plan a ejecutarse.
- **Categoría del Proyecto:** En este caso se ha identificado 6 categorías de los proyectos seleccionados y estas son: Implementación, Refuerzo, Capacitación, Prevención, Cumplimiento Norma, Mejora Continua.
- **Fuente:** Se señala de que documento se ha obtenido este plan.
- **Objetivos del Plan de Acción:** Se señala el objetivo principal del plan de acción
- **Desarrollo del Plan:** Se incluyen algunas tareas que se deben incluir como parte del proyecto.
- **Fecha de Inicio y Fecha Fin:** Hacen referencia a un periodo de tiempo en donde se debe ejecutar el proyecto.
- **Responsable(s):** En esta sección se señala a los integrantes de la empresa que deben colaborar en el proyecto.
- **Presupuesto:** En los casos que se requiera realizar una inversión, se ha asignado un monto estimado para el proyecto.
- **Estado:** Representa el estado del proyecto, sirve para dar seguimiento al proyecto. Al iniciar el programa, los estados de los proyectos serán “Aprobado” y “En revisión”**,** si los proyectos ya iniciaron sus actividades debería fijarse el estado “En Ejecución” hasta completarse y entregarse a la empresa.

- **Fase:** En esta columna, se ha determinado en qué etapa o fase se ejecutará el proyecto.

Estos planes de mejora han sido consolidados en una sola calendarización definiéndose fases según el siguiente esquema:

- Fase 1: 01/12/2021 - 30/03/2022
- Fase 2: 01/04/2022 - 31/07/2022
- Fase 3: 01/06/2022 - 30/12/2022

Los proyectos que se ejecutan dentro de la Fase 1 son de mayor prioridad, ya que estos proyectos ayudarán al programa de seguridad a cumplir partes fundamentales detectados en las fases del análisis del estado del SGSI o a cubrir riesgos identificados en el activo crítico seleccionado.

En total se han identificado 91 proyectos, los cuales 26 se ejecutarán en la Fase 1, 18 en la Fase 2 y 43 en la Fase 3. El número de proyectos podría cambiar y ajustarse conforme el avance de los primeros proyectos.

Para ver a mayor detalle los planes definidos, es necesario acceder al Anexo 8 del presente documento.

# 10. CONCLUSIONES GENERALES

Como parte del presente documento, se ha podido evidenciar que la empresa seleccionada tiene políticas, prácticas y nociones de seguridad de la información en un estado inicial, ya que las mediciones del estado del SGSI pudieron evidenciar que el nivel de madurez en general del SGSI se encontraba en nivel 1.

Se ha podido evidenciar que la empresa ha mantenido políticas y procesos de seguridad de la información, los cuales no han sido adaptados, ni medidos durante algún tiempo.

Se constató que la empresa no ha realizado auditorias externa respecto a los procesos de seguridad de la información dentro de la empresa ni ha buscado la actualización y la mejora continua de sus procesos, políticas y definiciones sobre seguridad de la información.

Se pudo evidenciar que el nivel del manejo del riesgo en los equipos se ha manejado de forma parcial, sin considerarse las nuevas definiciones sobre el funcionamiento de la empresa y los lineamientos de seguridad de la información que esto conllevaría.

# 11. RECOMENDACIONES GENERALES

Se pudieron identificar varios activos de información en el presente documento, por lo que será necesario completar la actividad de análisis de riesgos y vulnerabilidades y definir nuevos planes para incorporarlos a las mejoras que lleva el plan de mejora continua del programa de seguridad.

Se recomienda que para el proceso de seguimiento, ajuste y medición se contrate al menos 1 profesional dedicado y que tenga experiencia en seguridad de la información, mismo que se encargaría de dar seguimiento a las mediciones y actividades que contempla el programa de seguridad de la información con acompañamiento de Gerente Técnico y el área de IT.

Es recomendable que anualmente se contraten servicios profesionales para la evaluación del seguimiento del programa de seguridad de la información con el fin de mejorar, ajustar y evidenciar la mejora continua y la evaluación de las políticas de seguridad de la información.

Se recomienda involucrar a las revisiones sobre los temas de seguridad a los Gerentes General y Financiero para demostrar el avance del programa de seguridad de la información

# 12. REFERENCIAS


CEDIA (2014), “Gestión de la Seguridad”, tomado de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf, Pág. 21.

Forescout. “How to comply in 2020 with the 5 functions of the NIST Cybersecurity Framework”. Tomado de: https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/

ISACA. (2019). “Cobit 2019: Objetivos de gobierno y gestión”. Pág. 20.

ISOTools. “Norma ISO 31000. El valor de la gestión de riesgos en las organizaciones”. Tomado de https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

Ministerio de Hacienda y Relaciones Publica, España. “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método”. Tomado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Ministerio de Hacienda y Relaciones Publica, España. “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de Elementos”. Tomado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Ministerio de Telecomunicaciones – Gobierno electrónico. “Formato referencial para la elaboración de la política de seguridad de la información (EGSI)”. Tomado de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/03/Formato-Referencial_Pol%C3%ADtica-de-Seguridad-de-la-Informaci%C3%B3n-EGSI.pdf

National Institute of Standards and Technology, NIST. “NIST Cibersecurity Framework”. Tomado de: https://www.nist.gov/document/frameworkesmellrev20181102mncleanpdf Pág. 20.

We Live Security, ESET. “Cómo desarrollar y aplicar un programa de seguridad de la información”. Tomado de: https://www.welivesecurity.com/la-es/2017/01/11/desarrollo-programa-de-seguridad-informacion/

# ANEXOS

# ANEXO 1

# CASO DE NEGOCIO

# Entregable 1 – Caso de Negocio del Proyecto

## Introducción

El presente documento tiene como objetivo presentar un breve resumen del estado actual de la empresa, así como señalar como la implementación de un programa de seguridad de la información mejorará algunas de las necesidades de la empresa en base a su crecimiento y expansión de actividades.

## Objetivo del Proyecto

El objetivo principal del proyecto es implementar un programa de seguridad de la información, basado en marcos de referencia como ISO 27001 y 27002 para brindar lineamientos y políticas de seguridad actualizadas; así como identificar bases para un gobierno de IT dentro de la organización.

## Alcance del Proyecto

Como parte del alcance de la implementación de este proyecto contempla lo siguiente:

- Evaluar e identificar el estado actual de las políticas y controles de seguridad existentes.
- Evaluar e identificar los riesgos asociados a 1 activo de información crítico.
- Proponer políticas y controles que mejoren la seguridad de la información en relación a los activos críticos de información.
- Proponer políticas de seguimiento y mejoras que permitan medir y evaluar la gestión de la seguridad y su alineación con los objetivos del negocio.

## Expectativas del Proyecto

Se busca con la propuesta de implementación del programa de seguridad de la información y la actualización del SGSI alcanzar y cubrir las siguientes necesidades de la empresa:

- Establecer un sistema de gestión de seguridad de la información que funcione, se mantenga en el tiempo y se evalué con apoyo externo para su mejora.
- Definir políticas y métodos de protección de la información que administra la empresa basado en la Confidencialidad, Integridad y Disponibilidad y considerando en los casos que amerita la Privacidad.
- Establecer el cumplimiento efectivo de las regulaciones y obligaciones relacionadas a la seguridad de la información para las unidades de negocio.

## Beneficios de implementar el proyecto

Como parte de los beneficios implementar un Programa de seguridad están:

- Minimizar los riesgos asociados a los activos críticos, así como el impacto de estos riesgos; lo que ayuda a una mejor entrega de servicios a otras empresas.
- Entregar servicios de tecnología al cliente interno y externo, en donde se tenga en cuenta temas de seguridad de la información.

- Respaldar el alcance de los objetivos del negocio basado en una inversión adecuada en soluciones IT y alineando estas con las necesidades actuales y futuras de la empresa.
- Mejorar la gestión de activos y procesos relacionados a IT, por medio de políticas y procesos más apegados a la realidad de las empresas en el tiempo.
- Reforzar la imagen empresarial al incluir características de seguridad en la entrega de servicios a los clientes potenciales.

**Fases del proyecto**

Estas son las fases contempladas en el proyecto:

1. Análisis y Diagnóstico del SGSI Actual
2. Clasificación de los tipos de la información y los activos de Información
3. Inventario de Activos de Información
4. Análisis de amenazas y vulnerabilidades de los activos críticos seleccionados
5. Elaboración de Documentos Claves del SGSI
6. Operación


*Figura 1. Diagrama de fases del proyecto*

La fase de Operación se ejecutará una vez que las 5 primeras fases se encuentren aprobadas por la gerencia con la documentación y entregables a presentarse.

**Entregables del Proyecto**

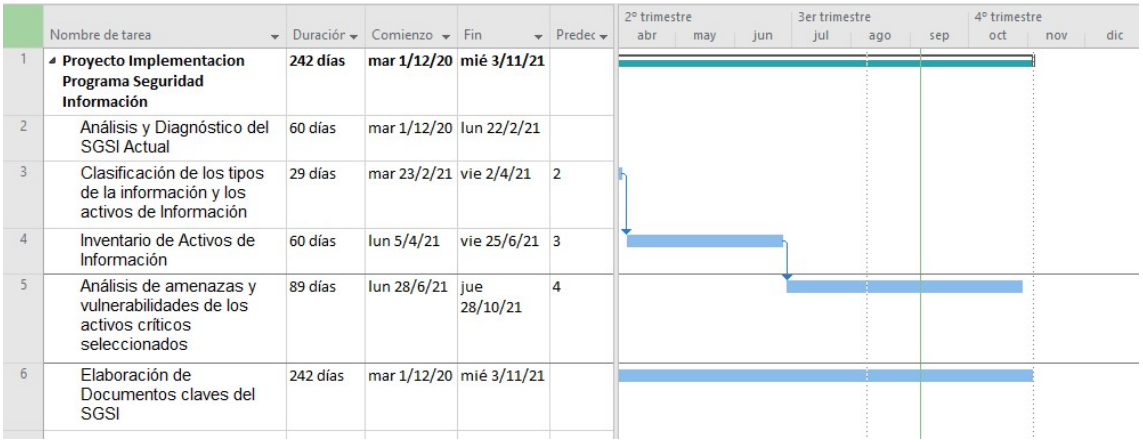
Como parte de los entregables del proyecto considerarán los siguientes entregables:

- Informe de Evaluación del estado actual de la Gestión del SGSI
- Clasificación de los tipos de Información
- Activos de Información críticos identificados y clasificados
- Análisis de amenazas y vulnerabilidades de un activo de información crítico

- Documento que incluye objetivo, políticas de alto nivel, roles y Responsabilidades de alto nivel, Procesos clave.
- Programa de mejora continua del SGSI incluyendo los proyectos, planes de acción definidos

## Cronograma del Proyecto

En la figura 2 se adjunta el cronograma del proyecto, que incluyen las 5 primeras fases del proyecto.



| | Nombre de tarea | Duración | Comienzo | Fin | Predec |
|---|---|---|---|---|---|
| 1 | **Proyecto Implementacion Programa Seguridad Información** | **242 días** | **mar 1/12/20** | **mié 3/11/21** | |
| 2 | Análisis y Diagnóstico del SGSI Actual | 60 días | mar 1/12/20 | lun 22/2/21 | |
| 3 | Clasificación de los tipos de la información y los activos de Información | 29 días | mar 23/2/21 | vie 2/4/21 | 2 |
| 4 | Inventario de Activos de Información | 60 días | lun 5/4/21 | vie 25/6/21 | 3 |
| 5 | Análisis de amenazas y vulnerabilidades de los activos críticos seleccionados | 89 días | lun 28/6/21 | jue 28/10/21 | 4 |
| 6 | Elaboración de Documentos claves del SGSI | 242 días | mar 1/12/20 | mié 3/11/21 | |



*Figura 2. Cronograma Inicial del proyecto*

Este cronograma contempla 242 días en donde se ejecutarán cada una de las fases y se harán las revisiones respectivas con los Gerentes Técnico y Gerente General de la empresa.

## Premisas del Proyecto

Para el presente proyecto se han considerado las siguientes premisas:

- La disposición de los socios para actualizar el SGSI e implementar un programa de seguridad acorde a las necesidades de la empresa.
- El acceso a la información existente referente a la documentación de seguridad definida anteriormente.
- La disponibilidad de reuniones con el Gerente técnico actual y el Gerente General de 2 horas por semana para consultas.

## Limitaciones del Proyecto

Para el presente proyecto se han considerado las siguientes limitaciones:

- El personal que trabaja en el área de TI que estarían a cargo del programa tienen poca experiencia en temas de seguridad de la información.
- Existe un presupuesto limitado para las inversiones en tecnología y seguridad de la información.

**Costos relacionados a la Implementación del Proyecto**

Para que el proyecto pueda cumplir con los objetivos establecidos, se han identificado algunos recursos que ayudarán a conseguir los objetivos que persigue la implementación del programa de seguridad de la información.

| Recurso | Costo Anual |
|---|---|
| Personal encargado de las políticas de seguridad de la información y soporte de políticas de seguridad para empresa. 1 Recurso | $ 12000 |
| Auditoría externa respecto al SGSI | $ 3000 |
| Inversión en tecnología de seguridad de la información | $ 8000 |
| Consultor Informático para revisión semestral | $4000 |
| Licencia para Software de Seguimiento de SGSI | $3500 |

*Tabla 1. Estimación de Costos anual del proyecto*

El cálculo de los recursos se lo ha hecho anualmente, tomando en consideración actividades que ayuden al SGSI a mantenerse y mejorar en el tiempo, así como un responsable de mantener y seguir las actividades de seguridad dentro de la empresa.

**Características del negocio, la organización, activos y tecnologías.**

Como contexto inicial empresa que se encarga de brindar soluciones tecnológicas para implementación y operación de Centros de Atención a clientes, mejora de plataformas de Call centers e incorporación de la atención de canales digitales como parte del servicio al cliente que ofrecen otras empresas. La estructura de la empresa anteriormente descrita se la puede observar en la figura 3.

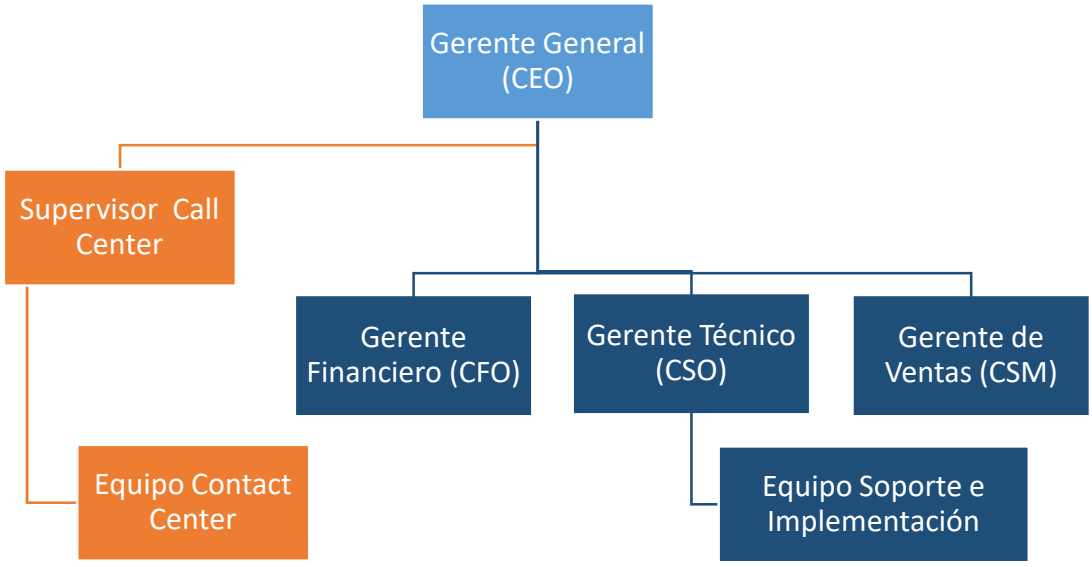



*Figura 3. Estructura Organizacional de la empresa seleccionada para este caso*

En este esquema organizacional los cuadros de color azul representan a la estructura base de la empresa mientras que los cuadro en color naranja representan a una unidad de negocio que se basa en brindar servicios de contact center como un servicio.

Ambas partes comparten dos procesos de funcionamiento, estos son la implementación y la gestión financiera.

**Proceso de Funcionamiento de la Empresa**

En esta sección se mostrarán los procesos descritos para cada una de las unidades de negocios, las cuales laboran de forma independiente, pero responden al mismo gerente.

En las tablas 2 y 3 se muestran los procesos junto a los responsables dentro de las unidades de negocio.

| **Proceso** | **Responsable** |
|---|---|
| Facturación | CFO/CEO |
| Operación Contact Center | Supervisor Call Center |
| Ventas | CFO/CEO |

*Tabla 2. Procesos Empresariales de la Unidad Naranja*

| **Proceso** | **Responsable** |
|---|---|
| Facturación | CFO |
| Contabilidad | CFO |
| Soporte e Implementación | CSO / Equipo Soporte |
| Ventas | CSM/CEO |
| Compras e Importaciones | CSM/ Equipo Soporte |
| Manejo RRHH | CSO / Equipo Soporte |

*Tabla 3. Procesos Empresariales de la Unidad Azul*

Para identificar el ecosistema de funcionamiento de la empresa a nivel tecnológico, se muestra en la figura 4 el esquema de red de la infraestructura actual.

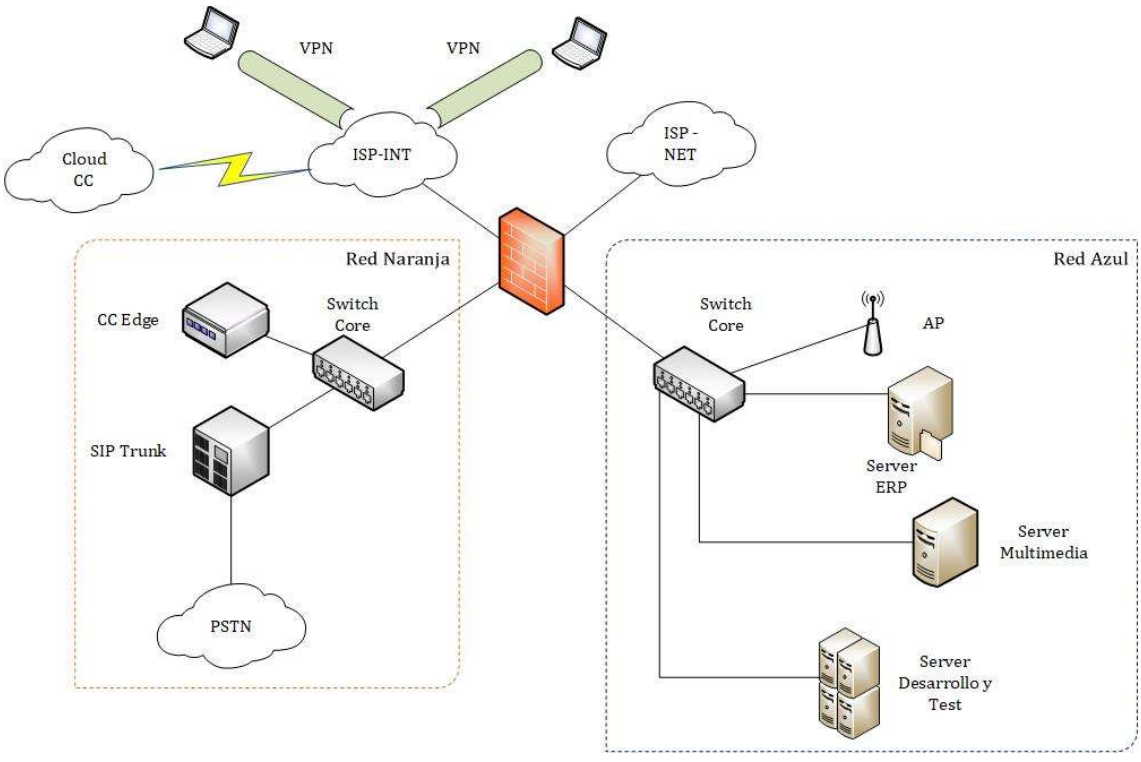



*Figura 4. Esquema de Red de la infraestructura*

Al estar ambas unidades de negocio en una misma infraestructura, estas se encuentran aisladas por medio de un firewall. Cada unidad de negocio cuenta con un proveedor de internet independiente.

Para el caso del proceso de ventas y facturación de ambas unidades, este proceso se soporta en un servidor que hace las funciones de ERP y Facturación Electrónica.

El proceso de Operaciones de Contact Center se soporta en tecnología cloud y los asesores acceden vía VPN debido a las limitaciones de la pandemia del año 2020.

Del lado de la unidad base, la mayoría de los servicios internos se utilizan desde el cloud, y los activos físicos que se manejan son equipos de comunicación y los servidores ERP, Testing y Desarrollo y un server que hace de Central IP para funcionamiento interno y pruebas.

**Antecedentes Empresariales**

En el siguiente listado se menciona algunas particularidades de la empresa:

- Desde inicios del año 2021, estas 2 unidades de negocio han incorporado sus actividades sobre el mismo datacenter, por lo que compartirán el esquema de red y funcionamiento sobre algunos componentes tecnológicos.
- Para la segunda unidad es importante brindar el servicio de contact center y que su disponibilidad en atención del mismo sea lo más apegado al contrato de servicios que actualmente maneja.
- Al momento la unidad base generó hace 4 años un SGSI, sin embargo, no se han establecido un seguimiento adecuado del SGSI, el proceso de mejoras no se ha aplicado acorde a la normativa.
- La operación del SGSI es poco supervisada y no esta formalizado del todo.
- En el caso de la segunda unidad de negocio se debe incluir en el cumplimiento de las políticas que se establezcan en el programa de seguridad de la información.
- Se ha aprobado la ley de protección de datos personales en Ecuador y como parte de actividades de la segunda unidad, es necesario mejorar la seguridad de la información referente al tratamiento de los datos personales de la cartera de clientes de los clientes de la segunda empresa.

.

# ANEXO 2

# EVALUACIÓN DEL SGSI ACTUAL

# Entregable 2 - Definición de Metodología de Evaluación  y Evaluación del SGSI

Para poder arrancar con la definición de seguridad que lleva la empresa al momento, es necesario definir en qué punto se encuentra la empresa respecto al manejo de la seguridad de la organización en sus diferentes actividades. Para ello, es necesario definir marcos de referencia y escalas de medición para definir acciones de mejora al estado de la empresa.

Este documento se ha elaborado basado en el marco de referencia ISO 27001/ISO 27002 y especifican las secciones de ISO 27001, y una sección para la evaluación de todo el listado de la ISO 27002. También unsa una escala de medición de madurez basado en Cobit 2019 y adaptado que se indica en la pestaña de Resumen.

Las pestañas denominadas como "Resumen ISO 27001" y "Resumen ISO 27002" muestran el resultado global del la evaluación.

Las pestañas denominadas "Sección_X" contiene las evaluaciones por sección referente a las secciones de la ISO 27001.

La pestaña denominada "Anexo A" contiene la evaluación en global de la ISO 27002.

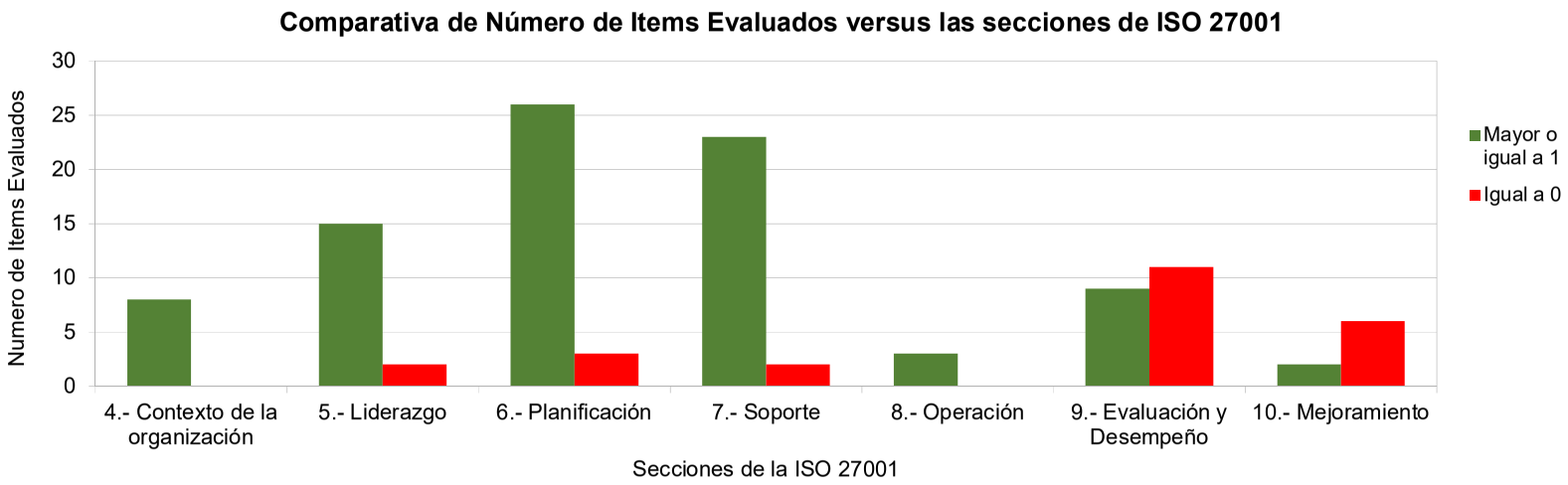
La Pestaña denominada "Planes de acción contiene todos los planes de acción referente a la mejora del SGSI.

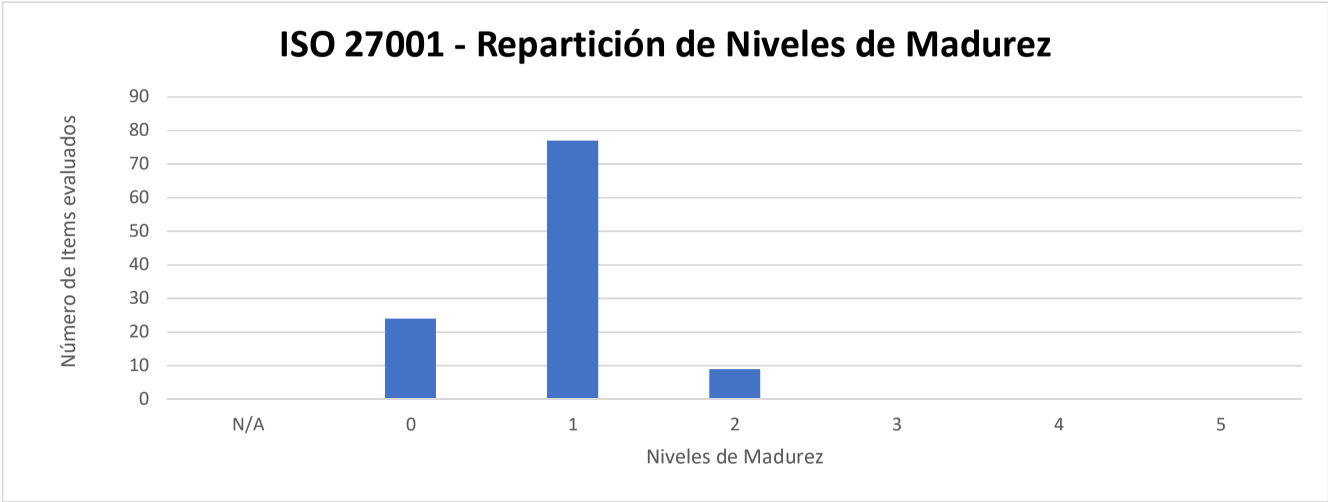
# Evaluación de Madurez respecto a los controles definidos en la ISO 27001

| Dominio | Promedio | Nro. Items | Mayor o igual a 1 | Igual a 0 |
|---|---|---|---|---|
| 4.- Contexto de la organización | 1.13 | 8 | 8 | 0 |
| 5.- Liderazgo | 1.06 | 17 | 15 | 2 |
| 6.- Planificación | 0.90 | 29 | 26 | 3 |
| 7.- Soporte | 0.90 | 25 | 23 | 2 |
| 8.- Operación | 1.00 | 3 | 3 | 0 |
| 9.- Evaluación y Desempeño | 0.45 | 20 | 9 | 11 |
| 10.- Mejoramiento | 0.25 | 8 | 2 | 6 |

**Tabla de Valores - Alcance**

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 0 |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. | 24 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. | 77 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. | 9 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. | 0 |


Comparativa de Número de Items Evaluados versus las secciones de ISO 27001
Numero de Items Evaluados
30
25
20
15
10
5
0
4.- Contexto de la organización
5.- Liderazgo
6.- Planificación
7.- Soporte
8.- Operación
9.- Evaluación y Desempeño
10.- Mejoramiento
Secciones de la ISO 27001
Mayor o igual a 1
Igual a 0

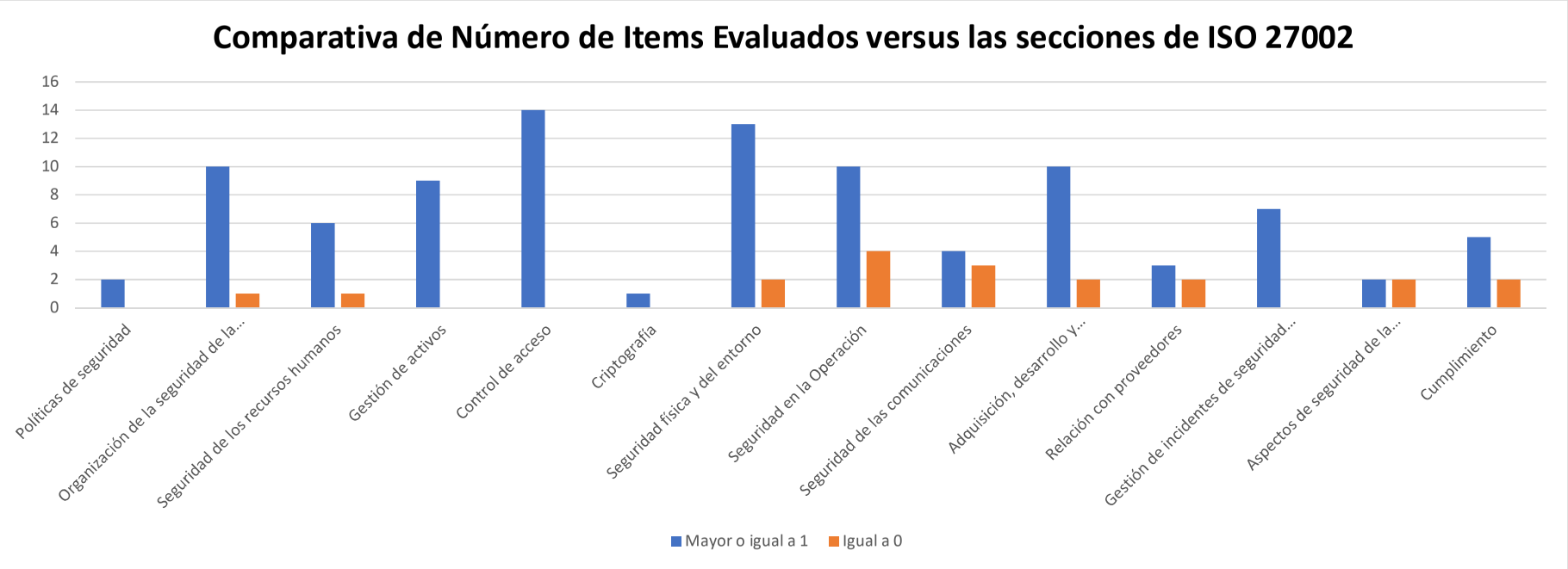

ISO 27001 - Repartición de Niveles de Madurez
Número de Items evaluados
90
80
70
60
50
40
30
20
10
0
N/A
0
1
2
3
4
5
Niveles de Madurez

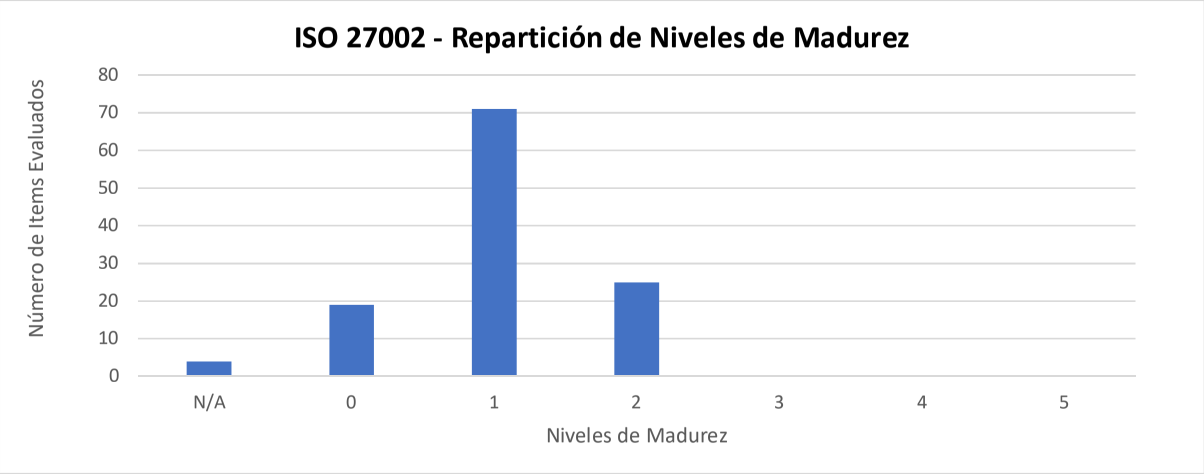
# Evaluación de Madurez respecto a los controles definidos en la ISO 27002

| Dominio | Promedio | Nro. Items | Mayor o igual a 1 | Igual a 0 | No Aplica |
|---|---|---|---|---|---|
| Políticas de seguridad | 1.00 | 2 | 2 | 0 | 0 |
| Organización de la seguridad de la Información | 1.27 | 11 | 10 | 1 | 0 |
| Seguridad de los recursos humanos | 0.86 | 7 | 6 | 1 | 0 |
| Gestión de activos | 1.33 | 10 | 9 | 0 | 1 |
| Control de acceso | 1.29 | 14 | 14 | 0 | 0 |
| Criptografía | 2.00 | 2 | 1 | 0 | 1 |
| Seguridad física y del entorno | 1.07 | 15 | 13 | 2 | 0 |
| Seguridad en la Operación | 1.00 | 14 | 10 | 4 | 0 |
| Seguridad de las comunicaciones | 0.86 | 7 | 4 | 3 | 0 |
| Adquisición, desarrollo y mantenimiento de los sistemas de información | 1.00 | 13 | 10 | 2 | 1 |
| Relación con proveedores | 0.80 | 5 | 3 | 2 | 0 |
| Gestión de incidentes de seguridad de la información | 1.00 | 7 | 7 | 0 | 0 |
| Aspectos de seguridad de la información para la gestión de la continuidad de negocio | 0.50 | 4 | 2 | 2 | 0 |
| Cumplimiento | 0.86 | 8 | 5 | 2 | 1 |

**Tabla de Valores - Alcance**

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 4 |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. | 19 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. | 71 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. | 25 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. | 0 |


Comparativa de Número de Items Evaluados versus las secciones de ISO 27002
16
14
12
10
8
6
4
2
0
Políticas de seguridad
Organización de la seguridad de la...
Seguridad de los recursos humanos
Gestión de activos
Control de acceso
Criptografía
Seguridad física y del entorno
Seguridad en la Operación
Seguridad de las comunicaciones
Adquisición, desarrollo y...
Relación con proveedores
Gestión de incidentes de seguridad...
Aspectos de seguridad de la...
Cumplimiento
Mayor o igual a 1
Igual a 0

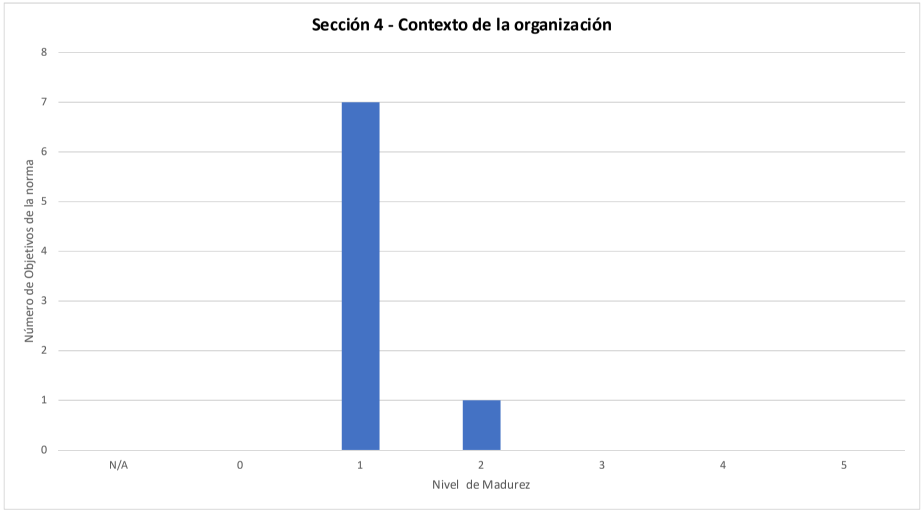

ISO 27002 - Repartición de Niveles de Madurez
Número de Items Evaluados
80
70
60
50
40
30
20
10
0
N/A
0
1
2
3
4
5
Niveles de Madurez

| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Código del plan de Acción |
|---|---|---|---|---|---|
| **4** | **Contexto de la organización** | | | | |
| **4.1** | **Comprensión de la organización y de su contexto** | | | | |
| 4.1 | La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información. | 1 | La organización ha definido parcialmente las cuestiones internas, debido a que se han adquirido nuevos contratos y obligaciones | Actualizar las cuestiones internas y externas referente al SGSI tomando en cuenta los nuevos contratos y obligaciones de la empresa | SGSI-4-1-a |
| **4.2** | **Comprensión de las necesidades y expectativas de las partes interesadas** | | | | |
| 4.2 | La organización debe determinar: | | | | |
| 4.2 (a) | las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información; y | 1 | La definición de las partes interesadas para el SGSI se encuentra desactualizada | Actualizar la definición de las partes interesadas del SGSI tomando en contexto la realidad actual de la empresa | SGSI-4-1-a |
| 4.2 (b) | los requisitos de estas partes interesadas que son relevantes para la seguridad de la información. | 1 | Los requisitos definidos actualmente no cubren todas las partes interesadas que son relevantes para el SGSI | Actualizar los requisitos de las partes interesadas del SGSI tomando en contexto la realidad actual de la empresa | SGSI-4-1-a |
| **4.3** | **Determinación del alcance del sistema de gestión de la seguridad de la información** | | | | |
| 4.3 | La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: | | | | |
| 4.3 (a) | las cuestiones externas e internas referidas en el apartado 4.1; | 1 | La organización ha definido parcialmente las cuestiones internas, debido a que se han adquirido nuevos contratos y obligaciones | Actualizar las cuestiones internas y externas referente al SGSI tomando en cuenta los nuevos contratos y obligaciones de la empresa | SGSI-4-1-a |
| 4.3 (b) | los requisitos referidos en el apartado 4.2; | 1 | Los requisitos definidos actualmente no cubren todas las partes interesadas que son relevantes para el SGSI | Actualizar los requisitos de las partes interesadas del SGSI tomando en contexto la realidad actual de la empresa | SGSI-4-1-a |
| 4.3 (c) | las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones. | 2 | Se cuenta con una definición de interfaces y dependencias entre la organización y otras organizaciones pero se encuentra desactualizada. | Reforzar y actualizar la definición de interfaces y dependencias entre la organización y otras organizaciones. | SGSI-4-1-a |
| 4.3 | El alcance debe estar disponible como información documentada. | 1 | El alcance se encuentra documentado, sin embargo no se encuentra actualizado. | Actualizar la documentación referente al alcance del SGSI. | SGSI-4-1-a |
| **4.4** | **Sistema de gestión de la seguridad de la información** | | | | |
| 4.4 | La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma internacional. | 1 | La organización ha establecido e implementado parcialmente un SGSI, no se ha ido mejorando y ajustando el SGSI en el tiempo. | Actualizar y reforzar el SGSI para que sea establecido acorde a las necesidades actuales de la empresa, implementado con la realidad de la empresa, así como mantener y proveer una retroalimentación para la mejora continua. | SGSI-4-2-a |

| Categoría | Total |
|---|---|
| N/A | 0 |
| 0 | 0 |
| 1 | 7 |
| 2 | 1 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 1.13 |

**Resumen de la sección 4 - Evaluacion del SGSI con ISO 27001**



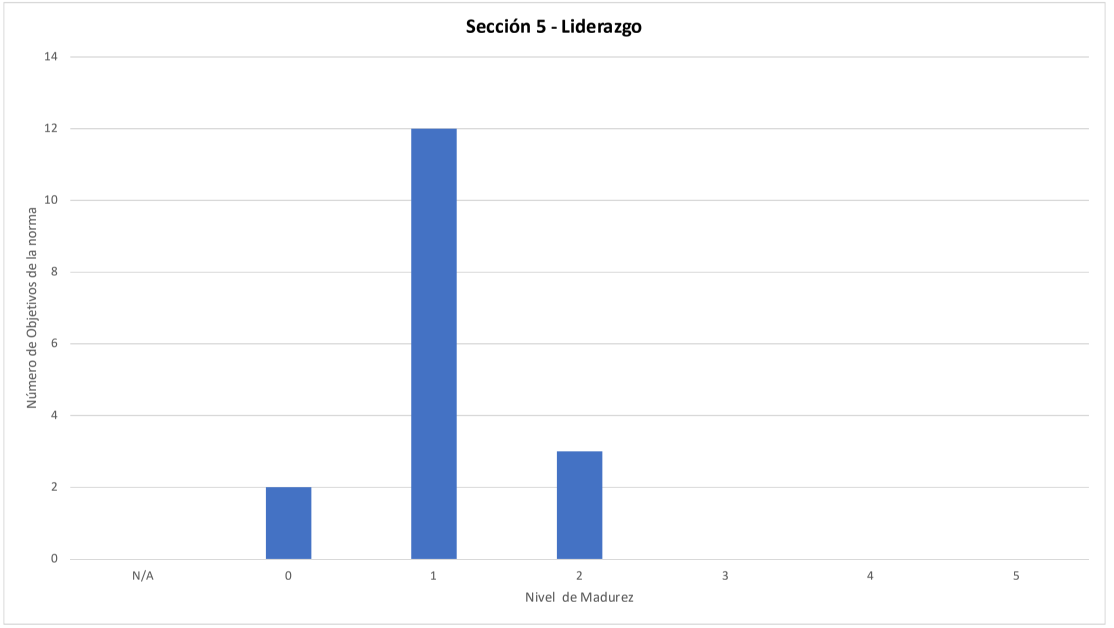
| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Codigo del Plan de Acción |
|---|---|---|---|---|---|
| **5** | **Liderazgo** | | | | |
| **5.1** | **Liderazgo y compromiso** | | | | |
| 5.1 | La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información: | | | | |
| 5.1 (a) | asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización; | 1 | Se estableció una politica de seguridad y sus objetivos, estos actualmente no son compatibles con la dirección estratégica de la organización | Ajustar la política de seguridad y sus objetivos para que estos sean compatibles con la dirección estratégica de la organización. | SGSI-5-1-a |
| 5.1 (b) | asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización; | 1 | El SGSI no se encuentra integrado enlos procesos actuales de la organización. | Incorporar el nuevo SGSI con los procesos actuales de la organización. | SGSI-5-1-a |
| 5.1 (c) | asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles; | 2 | El SGSI actual cuenta con recursos para las actividades, sin embargo no cubre todas las actividades de la empresa. | Reforzar y actualizar la asignación de recursos necesarios para cubrir las actividades de la empresa. | SGSI-5-1-a |
| 5.1 (d) | comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información; | 1 | El SGSI y su aplicación se ha comunicado en muy pocas ocasiones a la organización | Crear un plan de comunicación sobre el seguimiento de las actividades referentes al SGSI y sus ajustes. | SGSI-5-1-b |
| 5.1 (e) | asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos; | 2 | EL SGSI tiene evidencia de conseguir pocos de los resultados previstos.en las politicas de su SGSI | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan factores de medición | SGSI-5-1-c |
| 5.1 (f) | dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información; | 2 | El SGSI tiene instrucciones para una parte del seguimiento de las actividades. | Actualizar las instrucciones de las acciones conforme se definan en los controles del SGSI | SGSI-5-1-c |
| 5.1 (g) | promoviendo la mejora continua; y | 0 | No existe evidencia del que el SGSI haya tenido mejora continua. | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan análisis de métricas | SGSI-5-1-c |
| 5.1 (h) | apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad. | 1 | El SGSI únicamente apoya al área de TI para la toma de decisiones respecto a la seguridad. | Definir un plan de comunicación de las medidas y controles implementados en el SGSI a las otras areas de la empresa | SGSI-5-1-c |
| **5.2** | **Política** | | | | |
| 5.2 | La alta dirección debe establecer una política de seguridad de la información que: | | | | |
| 5.2 (a) | sea adecuada al propósito de la organización; | 1 | Se estableció una politica de seguridad y sus objetivos, estos actualmente son adecuados parcialmente con el propósito de la organización | Ajustar la política de seguridad y sus objetivos para que estos sean compatibles con la dirección estratégica de la organización | SGSI-5-1-a |
| 5.2 (b) | incluya objetivos de seguridad de la información (véase 6.2) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información; | 1 | Se ha identificado que se tienen algunos lineamientos basados en la ISO 27002 | Reforzar la definición de las políticas de seguridad del programa basadas en ISO 27002 | SGSI-6-1-d |
| 5.2 (c) | incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e | 1 | Para la definición del SGSI actual se incluyo el compromiso de cumplir con los requisitos aplicables a ese momento respecto a la seguridad de la información. | Actualizar y generar un nuevo documento de compromiso de cumplimiento de requisitos aplicables respecto a la seguridad de la información. | SGSI-5-2-a |
| 5.2 (d) | incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información. | 0 | No se evidencia que se haya ejecutado un compromiso de mejora continua | Generar un documento de constancia sobre el cumplimiento del compomiso de mejora continua del SGSI. | SGSI-5-2-a |
| 5.2 | La política de seguridad de la información debe: | | | | |
| 5.2 (e) | estar disponible como información documentada; | 1 | La información del SGSI que se encuentra documentada no se encuentra actualizada. | Generar un plan de documentación del SGSI que incluya versionamiento y actualizaciones periodicas | SGSI-5-2-b |
| 5.2 (f) | comunicarse dentro de la organización; y | 1 | Las politicas de seguridad del SGSI se han comunicado en contadas ocasiones. | Generar un plan de comunicación sobre las políticas que tiene el SGSI en la empresa y definir un calendario de comunicación | SGSI-5-2-c |

| | | | | | |
|---|---|---|---|---|---|
| 5.2 (g) | estar disponible para las partes interesadas, según sea apropiado. | 1 | La documentación del SGSI se encuentra disponible unicamente bajo pedido. | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | SGSI-5-2-d |
| **5.3** | **Roles, responsabilidades y autoridades en la organización** | | | | |
| 5.3 | La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización. La alta dirección debe asignar la responsabilidad y autoridad para: | | | | |
| 5.3 (a) | asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional; e | 1 | El SGSI con el que cuenta la empresa no se encuentra alineado completamente a los requisitos de la norma internacional | Realizar una revisión interna luego de 6 meses de haberse implementado el nuevo SGSI en la organización.para definir el estado del SGSI | SGSI-5-3-a |
| 5.3 (b) | informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información. | 1 | Los avances de la gestión del SGSI era informados esporadicamente, además no se realizo un seguimiento de mejoras del SGSI | Incluir en el plan de comunicación de los resultados del SGSI a la alta dirección. | SGSI-5-2-c |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 2 |
| 1 | 12 |
| 2 | 3 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 1.06 |

## Resumen de la sección 5 - Evaluación del SGSI con ISO 27001



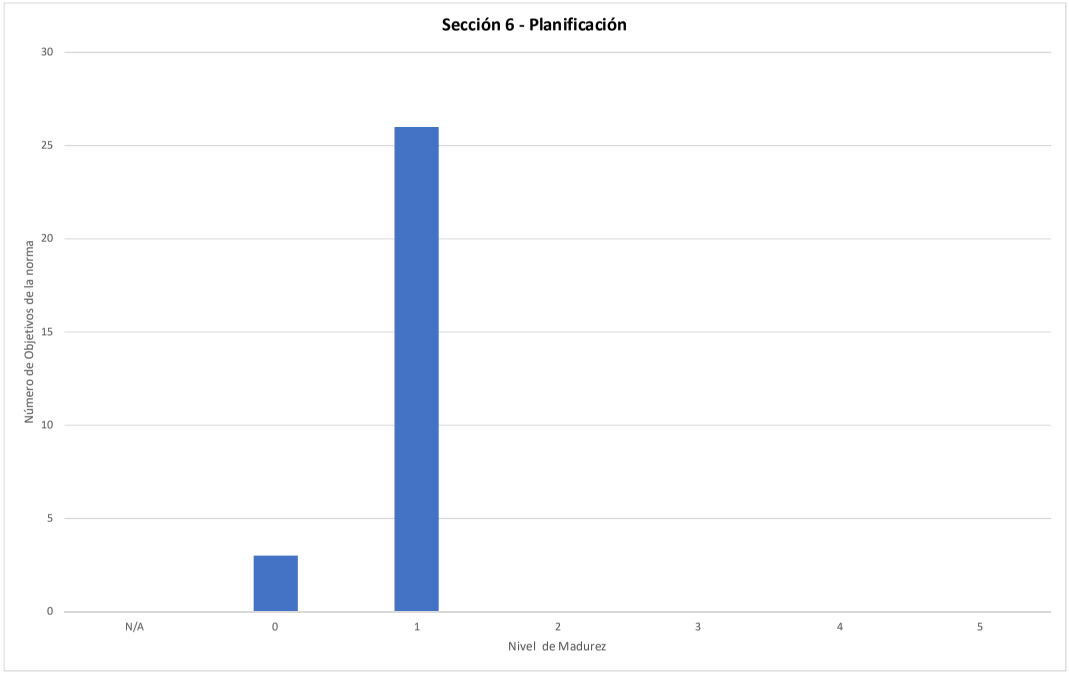
| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Codigo del Plan de Acción |
|---|---|---|---|---|---|
| **6** | **Planificación** | | | | |
| **6.1** | **Acciones para tratar los riesgos y oportunidades** | | | | |
| **6.1.1** | **Consideraciones generales** | | | | |
| 6.1.1 | Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de: | | | | |
| 6.1.1 (a) | asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos | 1 | EL SGSI tiene evidencia de conseguir pocos de los resultados previstos.en las politicas de su SGSI | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan factores de medición | SGSI-5-1-c |
| 6.1.1 (b) | prevenir o reducir efectos indeseados; y | 1 | La definición de prevención o reducción de efectos indeseados no se encuentra actualizada. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.1 (c) | lograr la mejora continua. | 0 | No se ha definido objetivos para alcanzar la mejora continua | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan análisis de métricas | SGSI-5-1-c |
| 6.1.1 | La organización debe planificar: | | | | |
| 6.1.1 (d) | las acciones para tratar estos riesgos y oportunidades; y | 1 | La definición de acciones para trater los riesgos y oportnuidades se encuentra desacualizada | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| 6.1.1 (e) | la manera de:<br>1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y<br>2) evaluar la eficacia de estas acciones. | 1 | La forma de integrar las acciones a los proceso del SGSI se encuentran poco definidos y no existe evaluación de eficacia | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| **6.1.2** | **Apreciación de riesgos de seguridad de la información** | | | | |
| 6.1.2 | La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que: | | | | |
| 6.1.2(a) | establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:<br>1) los criterios de aceptación de los riesgos, y<br>2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información; | 1 | Los criterios sobre riesgos en seguridad de la información se encuentran desactualizados | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.2(b) | asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables; | 1 | Las mediciones que se ejecutan a los riesgos se encuentran poco definidas y no existe evaluación de la eficacia | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| 6.1.2(c) | identifique los riesgos de seguridad de la información:<br>1) llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,<br>2) identificando a los dueños de los riesgos; | 1 | La definición existente de los riesgos se encuentra desactualizada, no se han definido dueños de los riesgos. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.2(d) | analice los riesgos de seguridad de la información:<br>1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,<br>2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),<br>3) determinando los niveles de riesgo; | 1 | La definición existente de los riesgos se encuentra desactualizada, no se han definido adecuadamente los niveles de riesgo. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.2(e) | la manera de:<br>1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y<br>2) evaluar la eficacia de estas acciones. | 1 | La forma de integrar las acciones a los proceso del SGSI se encuentran poco definidos y no existe evaluación de eficacia | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| 6.1.2 | La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información. | 1 | La documentación sobre la apreciación de riesgos se encuentra incompleta y desactualizada | Definir una política de manejo de documentación sobre los riesgos que se consideraron para el SGSI. | SGSI-6-1-c |
| **6.1.3** | **Tratamiento de los riesgos de seguridad de la información** | | | | |
| 6.1.3 | La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para: | | | | |
| 6.1.3(a) | seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos; | 1 | La definición existente de los riesgos se encuentra desactualizada, no se han definido adecuadamente la apreciación de riesgos. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.3(b) | determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información; | 1 | El listado de controles con los que cuenta la organización se encuentran desactualizados. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| 6.1.3(c) | comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios; | 1 | El listado de controles con los que cuenta la organización se encuentran incompletos | Reforzar la definición de los controles necesarios dentro de la empresa y apegar los controles al anexo A. | SGSI-6-1-d |

| | | | | | |
|---|---|---|---|---|---|
| 6.1.3(d) | elaborar una “Declaración de Aplicabilidad” que contenga:<br>– los controles necesarios [véase 6.1.3 b) y c)];<br>– la justificación de las inclusiones;<br>– si los controles necesarios están implementados o no; y<br>– la justificación de las exclusiones de cualquiera de los controles del anexo A. | 1 | La declaración de aplicabilidad se encuentra incompleta, existen inconsistencias en las justificaciones de algunos controles. | Reforzar la declaración de aplicabilidad conforme a las nuevas responsabilidades de la empresa. | SGSI-6-1-e |
| 6.1.3(e) | formular un plan de tratamiento de riesgos de seguridad de la información; y | 1 | El plan de tratamientos de riesgo actual se encuentra desactualizado y no se encuentra acorde a las necesidades de la empresa. | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| 6.1.3(f) | obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos. | 1 | El plan de tratamientos de riesgo actual no cuenta con la aceptación del plan de tratamiento de riesgos | Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |
| 6.1.3 | La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información. | 1 | La documentación sobre la apreciación de riesgos se encuentra impcompleta y descatualizada | Definir un plan de manejo de documentación del SGSI | SGSI-6-1-c |
| **6.2** | **Objetivos de seguridad de la información y planificación para su consecución** | | | | |
| 6.2 | La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deben: | | | | |
| 6.2 (a) | ser coherentes con la política de seguridad de la información; | 1 | Los objetivos de seguridad de la información se encuentran definidos, pero no guardan una estrecha relación con la política de seguridad de la infromación | Definir nuevos objetivos de seguridad que se encuentren acordes a las políticas de seguridad de la información. | SGSI-6-2-a |
| 6.2 (b) | ser medibles (si es posible); | 1 | Las mediciones de los objetivos de seguridad no se encuentran homologadas con factores de medición. Solo pocos controles son medibles. | Definir nuevos factores de medición de los objetivos de seguridad | SGSI-6-2-a |
| 6.2 (c) | tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos; | 1 | El plan de tratamientos de riesgo actual se encuentra desactualizado y no se encuentra acorde a las necesidades de la empresa. De igual manera la apreciación de riesgos se encuentra desactualizada. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos. Definir un plan de seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-a<br>SGSI-6-1-b |
| 6.2 (d) | ser comunicados; y | 1 | Las políticas de seguridad, así como sus objetivos del SGSI se han comunicado en contadas ocasiones. | Generar un plan de comunicación sobre las políticas que tiene el SGSI en la empresa y definir un calendario de comunicación | SGSI-5-2-c |
| 6.2 (e) | ser actualizados, según sea apropiado. | 0 | No existe evidencia de que los objetivos de seguridad de la información hayan sido actualizados. | Definir un plan de actualización de los objetivos de seguridad de la información basado en las mediciones a realizarse | SGSI-6-2-a |
| 6.2 | La organización debe conservar información documentada sobre los objetivos de seguridad de la información. | 1 | La documentación sobre la apreciación de riesgos se encuentra impcompleta y descatualizada | Definir un plan de manejo de documentación del SGSI | SGSI-6-1-c |
| 6.2 | Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar: | | | | |
| 6.2 (f) | lo que se va a hacer; | 1 | La definición de las acciones para cumplir con los objetivos de la información se encuentra desactualizada. | Actualizar la planificación existente incluyendo las acciones necesarias para alcanzar los objetivos de seguridad de la información | SGSI-6-2-b |
| 6.2 (g) | qué recursos se requerirán; | 1 | La definición de los recursos necesarios para cumplir con los objetivos de la información se encuentra desactualizado. | Actualizar la planificación existente incluyendo los recursos necesarios para alcanzar los objetivos de seguridad de la información | |
| 6.2 (h) | quién será responsable; | 1 | La definición del personal responsable para dar seguimiento a los objetivos de la información se encuentra desactualizado. | Actualizar la planificación existente incluyendo la asignación del personal para alcanzar los objetivos de seguridad de la información | |
| 6.2 (i) | cuándo se finalizará; y | 1 | La definición de un cronograma o calendario de seguimientode los objetivos de información se encuentra desactualizada | Actualizar la planificación existente incluyendo periodos de tiempos o calendarios para alcanzar los objetivos de seguridad de la información | |
| 6.2 (j) | cómo se evaluarán los resultados. | 0 | No existe una definición de evaluación del resultado del alcance de los objetivos de seguridad de la información | Incluir en la planificación métricas para la evaluación de resultados respecto al cumplimiento de objetivos de seguridad de la información | |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 3 |
| 1 | 26 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 0.90 |

**Resumen de la sección 6 - Evaluación del SGSI con ISO 27001**



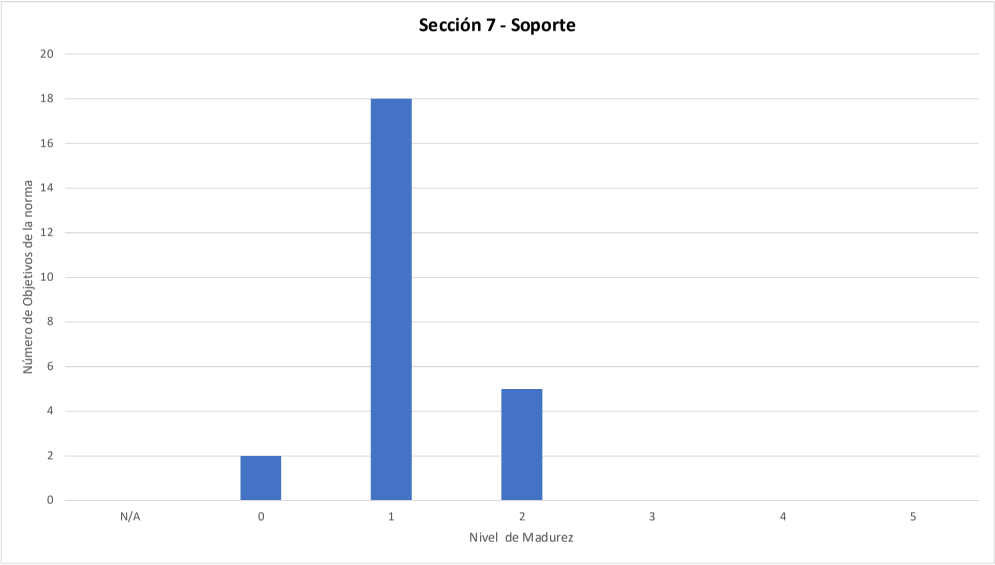
| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Código del Plan de Acción |
|---|---|---|---|---|---|
| **7** | **Soporte** | | | | |
| **7.1** | **Recursos** | | | | |
| 7.1 | La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información. | 1 | La definición de los recursos necesarios esta desactualizada a las nuevas necesidadesde la empresa | Reforzar y Actualizar los recursos necesarios para cumplir con el nuevo SGSI. | SGSI-7-1-a |
| **7.2** | **Competencia** | | | | |
| 7.2 | La organización debe: | | | | |
| 7.2 (a) | determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y | 1 | No todo el personal técnico a cargo del departamento de TI tiene formación en seguridad de la información | Definir un plan de asignación de responsabilidades referente a la participación en las actividades del SGSI | SGSI-7-2-a |
| 7.2 (b) | asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas; | 1 | Pocos miembros del personal que participa en el departamento de TI tienen experiencia en seguridad de la información | Incluir asignación de responsabilidades acorde a su experiencia en temas de TI y seguridad de la información. | |
| 7.2 (c) | cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y | 0 | No existen planes de formación de recursos respecto a seguridad de la información. | Definir un plan de formación del personal de seguridad de la información en base a sus responsabilidades. | |
| 7.2 (d) | conservar la información documentada apropiada, como evidencia de la competencia. | 2 | La documentación del personal del departamento de TI se encuentra documentada tales como certificaciones y Hoja de Vida | Incluir en la documentación cursos, capacitaciones o asistencias a charlas sobre seguridad de la información | |
| **7.3** | **Concienciación** | | | | |
| 7.3 | Las personas que trabajan bajo el control de la organización deben ser conscientes de: | | | | |
| 7.3(a) | la política de la seguridad de la información; | 1 | No se ha difundido las politicas de seguridad de la información a todas las áreas de la empresa. | Definir un plan de concienciación sobre las políticas y los objetivos de seguridad de la información, así como sus beneficios y las implicaciones de no cumplir con los objetivos. | SGSI-7-3-a |
| 7.3(b) | su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; | 1 | En las difusiones realizadas no se han señalado todos los beneficios que se obtienen al implementar las politicas de seguridad de la información. | | |
| 7.3(c) | las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información. | 1 | En las difusiones realizadas no se han señalado todas las implicaciones de no cumplir las politicas de seguridad de la información. | | |
| **7.4** | **Comunicación** | | | | |
| 7.4 | La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan: | | | | |
| 7.4 (a) | el contenido de la comunicación; | 1 | El contenido de la comunicación que se habia realizado se encuentra incompleto y desactualizado. | Elaborar un esquema de comunicación que incluya que se debe comunicar, cuando comunicar, a quien comunicar, quien debe comunicar y que procesos se deben utilizar para comunicar. | SGSI-7-4-a |
| 7.4 (b) | cuándo comunicar; | 1 | Se han definido fechas de comunicación basadas en eventos reactivos | | |
| 7.4 (c) | a quién comunicar; | 1 | La comunicación de las necesidades del SGSI se han comunicado a ciertas áreas de la empresa | | |
| 7.4 (d) | quién debe comunicar; | 2 | Se habia definido que la comunicación la haga el Gerente Técnico de la empresa | | |

| | | | | | |
|---|---|---|---|---|---|
| 7.4 (e) | los procesos por los que debe efectuarse la comunicación. | 1 | Se han definido unicamente el proceso de envio de correos como unico medio de comunicación. | | |
| **7.5** | **Información documentada** | | | | |
| **7.5.1** | **Consideraciones generales** | | | | |
| 7.5.1 | El sistema de gestión de la seguridad de la información de la organización debe incluir: | | | | |
| 7.5.1 (a) | la información documentada requerida por esta norma internacional; | 1 | El SGSI con el que cuenta la empresa no se encuentra alineado completamente a los requisitos de la norma internacional | Realizar una revisión interna luego de de 3 meses de haberse implementado el nuevo SGSI en la organización.para definir el estado del SGSI | SGSI-5-3-a |
| 7.5.1 (b) | la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información. | 0 | No se ha definido un listado de documentación que sea definida como necesaria para la eficacia del SGSI | Definir un listado de documentación necesaria para medir la eficacia del SGSI. | SGSI-7-5-a |
| **7.5.2** | **Creación y actualización** | | | | |
| 7.5.2 | Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente: | | | | |
| 7.5.2 (a) | la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia); | 1 | Se ha definido un esquema de identificación con titulo y autor de la documentación, no hay versionamiento | Definir un reglamento sobre el formato de la documentación y los requisitos minimos que esta documentación debe tener. | SGSI-7-5-b |
| 7.5.2 (b) | el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico); | 1 | Se ha identificado que la documentación cuenta en algunos casos con gráficos, pero se encuentra descatualizada. | Definir un reglamento sobre el contenido de la documentación, así como su actualización. | |
| 7.5.2 (c) | la revisión y aprobación con respecto a la idoneidad y adecuación. | 2 | La documentación ha pasado por un proceso de aprobación con respecto a la idoneidad y su adecuación | Reforzar el proceso de aprobación manteniendo la revisión de idoneidad y adecuación. | |
| **7.5.3** | **Control de la información documentada** | | | | |
| 7.5.3 | La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional se debe controlar para asegurarse que: | | | | |
| 7.5.3 (a) | esté disponible y preparada para su uso, dónde y cuándo se necesite; | 1 | La documentación del SGSI se encuentra disponible unicamente bajo pedido. | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | SGSI-5-2-d |
| 7.5.3 (b) | esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad). | 1 | La documentación del SGSI se encuentra protegida unicamente contra perdida de confidencialidad, no se ha considerado el uso inadecuado ni la perdida de integridad | Definir un plan de protección de la documentación que incluya acciones en caso de perdida de confidencialidad, el uso inadecuado y la perdida de integridad. | SGSI-7-5-c |
| 7.5.3 | Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable: | | | | |
| 7.5.3 (c) | distribución, acceso, recuperación y uso; | 1 | la documentación del SGSI no se ha distribuido adecuadamente entre todas las areas de la empresa. Se maneja el acceso a la documentación por medio de solicitudes. | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | SGSI-5-2-d |
| 7.5.3 (d) | almacenamiento y preservación, incluida la preservación de la legibilidad; | 2 | La documentación del SGSI actual se ha almacenado en varios sitios y se preservado, sin embargo es necesario definir y unificar las áreas en donde se va a almacenar esta información | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | SGSI-5-2-d |
| 7.5.3 (e) | control de cambios (por ejemplo, control de versión); | 1 | Parte de la documentación del SGSI maneja versionamiento. | Incluir en el plan de manejo de documentación del SGSI la sección de versionamiento | SGSI-5-2-b |
| 7.5.3 (f) | retención y disposición. | 1 | La retención de la documentacion del SGSI se ejecuta, el manejo de la disposición de la documentación se encuentra incompleto | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | SGSI-5-2-d |
| 7.5.3 | La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información se debe identificar y controlar, según sea adecuado. | 2 | La documentación de origen externo que participa en el SGSI se encuentra identificada y controlada | Incluir en el plan de almacenamiento las instrucciones para la identificación de la documentación externa. | SGSI-5-2-d |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 2 |
| 1 | 18 |
| 2 | 5 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 1.12 |

## Resumen de la sección 7 - Evaluación del SGSI con ISO 27001

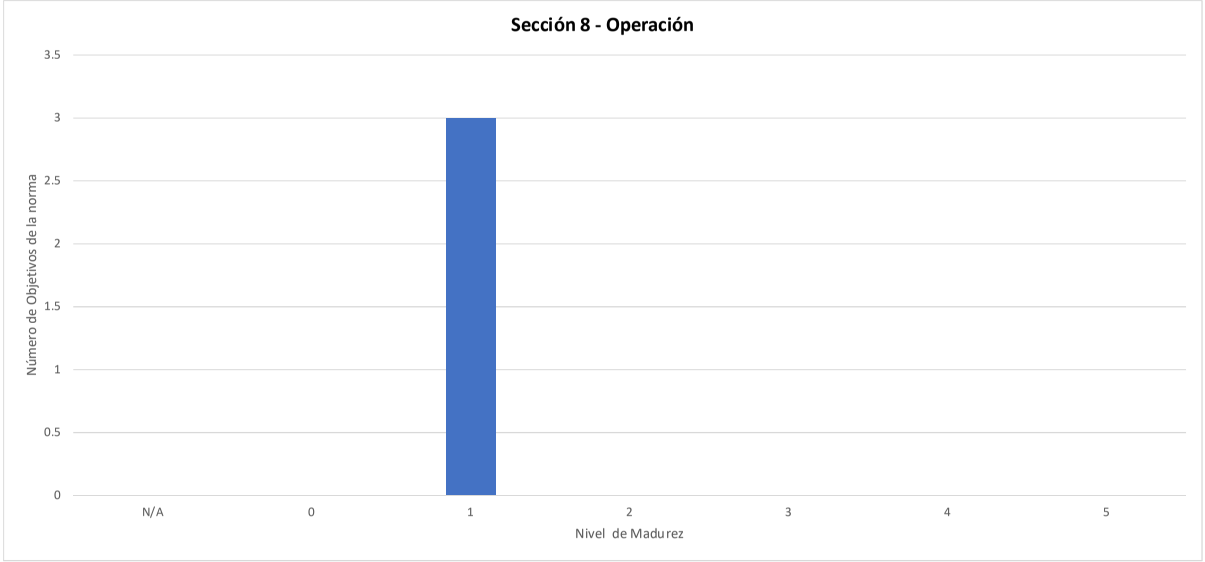


| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Código de Plan de Acción |
|---|---|---|---|---|---|
| **8** | **Operación** | | | | |
| **8.1** | **Planificación y control operacional** | | | | |
| 8.1 | La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado 6.1. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinados en el apartado 6.2. | 1 | La empresa ha planificado e implementado parte de los procesos necesarios para cumplir con los requisitos de seguridad de la información. Los planes paea alcanzar los objetivos de seguridad de la información se encuentran desactualizados | Actualizar la planificación existente incluyendo las acciones necesarias para alcanzar los objetivos de seguridad de la información | SGSI-6-2-b |
| **8.2** | **Apreciación de los riesgos de seguridad de la información** | | | | |
| 8.2 | La organización debe efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2a. La organización debe conservar información documentada de los resultados de las apreciaciones de riesgos de seguridad de información. | 1 | Los criterios sobre riesgos en seguridad de la información se encuentran desactualizados. La documentación sobre la apreciación de riesgos se encuentra incompleta y desactualizada | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos | SGSI-6-1-a |
| **8.3** | **Tratamiento de los riesgos de seguridad de la información** | | | | |
| 8.3 | La organización debe implementar el plan de tratamiento de los riesgos de seguridad de la información. La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información. | 1 | El plan de tratamientos de riesgo actual se encuentra desactualizado y no se encuentra acorde a las necesidades de la empresa. | Definir un plan seguimiento y mejora de tratamiento de riesgos | SGSI-6-1-b |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 0 |
| 1 | 3 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 1.00 |

## Resumen de la sección 8 - Evaluación del SGSI con ISO 27001



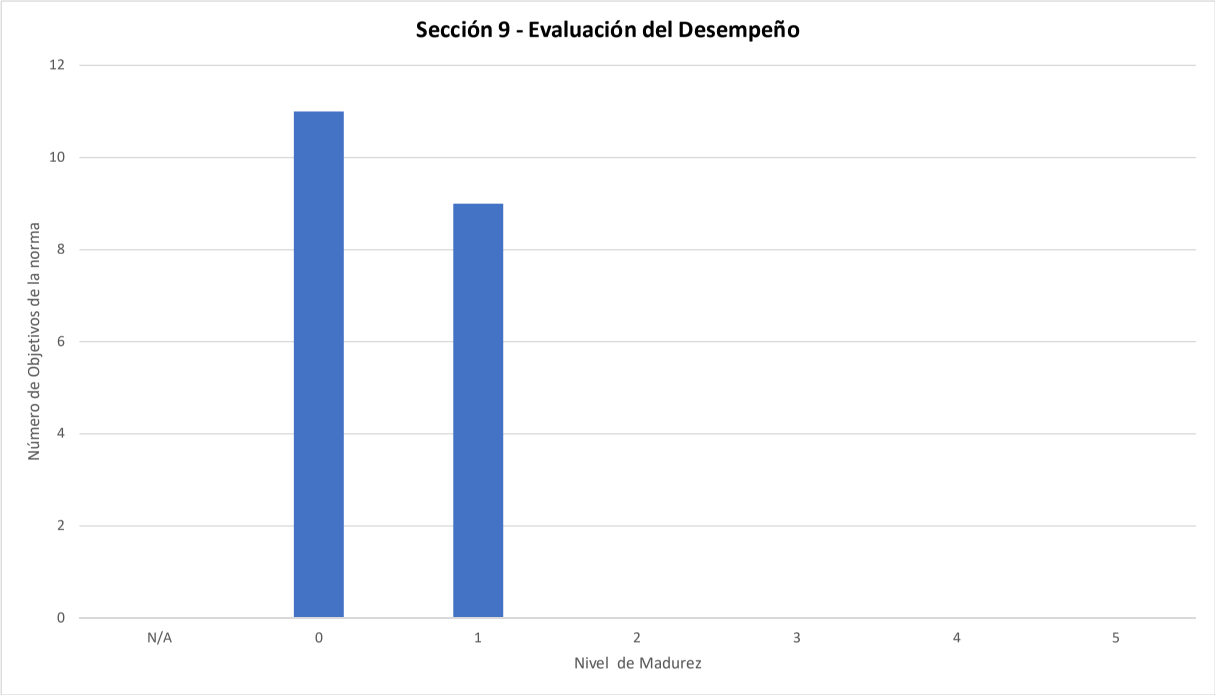
| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Codigo del Plan de Acción |
|---|---|---|---|---|---|
| **9** | **Evaluación del desempeño** | | | | |
| **9.1** | **Seguimiento, medición, análisis y evaluación** | | | | |
| 9.1 | La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. La organización debe determinar: | | | | |
| 9.1 (a) | a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información; | 1 | El SGSI tiene evidencia de conseguir pocos de los resultados previstos.en las politicas de su SGSI | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan análisis de métricas | SGSI-5-1-c |
| 9.1 (b) | los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos; | 1 | El SGSI tiene evidencia de conseguir pocos de los resultados previstos.en las politicas de su SGSI | | |
| 9.1 (c) | cuándo se deben llevar a cabo el seguimiento y la medición; | 1 | Se habia definido que el seguimiento y la medicónción la haga el Gerente Técnico de la empresa | | |
| 9.1 (d) | quién debe hacer el seguimiento y la medición; | 0 | No existe evidencia del que el SGSI haya tenido mejora continua. | | |
| 9.1 (e) | cuándo se deben analizar y evaluar los resultados del seguimiento y la medición; | 0 | No existe evidencia del que el SGSI haya tenido mejora continua. | | |
| 9.1 (f) | quién debe analizar y evaluar esos resultados. | 0 | No se ha definido un responsable para realizar el análisis y evaluación de estos riesgos | Definir un plan de asignación de responsabilidades referente a la participación en las actividades del SGSI. | SGSI-7-2-a |
| **9.2** | **Auditoria Interna** | | | | |
| 9.2 | La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información: | | | | |
| 9.2 (a) | cumple con:<br>1) los requisitos propios de la organización para su sistema de gestión de la seguridad de la información,<br>2) los requisitos de esta norma internacional, | 1 | El SGSI con el que cuenta la empresa no se encuentra alineado completamente a los requisitos de la norma internacional | Realizar una revisión interna luego de de 3 meses de haberse implementado el nuevo SGSI en la organización.para definir el estado del SGSI | SGSI-5-3-a |
| 9.2 (b) | está implementado y mantenido de manera eficaz. | 1 | La organización ha establecido e implementado parcialmente un SGSI, no se ha ido mejorando y ajustando el SGSI en el tiempo. | Actualizar y reforzar el SGSI para que sea establecido acorde a las necesidades actuales de la empresa, implementado con la realidad de la empresa, así como mantener y proveer una retroalimentación para la mejora continua. | SGSI-4-2-a |
| 9.2 | La organización debe: | | | | |
| 9.2 (c) | planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas; | 0 | No se han definido auditorias respecto a seguridad de la información | | |
| 9.2 (d) | para cada auditoría, definir sus criterios y su alcance; | 0 | No se ha definido alcances de la auditoria de seguridad de la información | | |

| | | | | | |
|---|---|---|---|---|---|
| 9.2 (e) | seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; | 0 | No se han seleccionado auditores o una empresa de auditoria para los temas de seguridad de la información. | Definir un plan de auditoria para el SGSI, sus politicas y sus resultados | SGSI-9-2-a |
| 9.2 (f) | asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías; y | 0 | No se han definido auditorias respecto a seguridad de la información | | |
| 9.2 (g) | conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta. | 0 | No se han definido auditorias respecto a seguridad de la información | | |
| **9.3** | **Revisión por la dirección** | | | | |
| 9.3 | La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. La revisión por la dirección debe incluir consideraciones sobre: | | | | |
| 9.3 (a) | el estado de las acciones desde anteriores revisiones por la dirección; | 1 | Se han definido pocas revisiones, sin embargo no se han definido cambios en dichas revisiones | Acoplar al plan de seguimiento de la eficacia del SGSI el seguimiento de las acciones definidas por la dirección | SGSI-5-1-c |
| 9.3 (b) | los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información; | 1 | Se han definido pocas revisiones, sin embargo no se han definido cambios en dichas revisiones | Acoplar al plan de seguimiento de la eficacia del SGSI los cambios en las cuestiones internas y externas que sean pertinentes al sistema. | SGSI-5-1-c |
| 9.3 (c) | la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a:<br>1) no conformidades y acciones correctivas,<br>2) seguimiento y resultados de las mediciones,<br>3) resultados de auditoría, y<br>4) el cumplimiento de los objetivos de seguridad de la información, | 0 | No se han definido auditorias respecto a seguridad de la información | Definir un plan de acción respecto a los resultados de la auditoria, así como el tratamiento de las no conformidade, las acciones correctivas. | SGSI-9-2-a |
| 9.3 (d) | los comentarios provenientes de las partes interesadas; | 1 | Los comentarios provenientes de las partes interesadas se exponen pero no se documentan. | Revisar si los comentarios de las partes interesadas se alinean a los requisitos definidos y a la mejora continua y documentar estos comentarios | SGSI-5-1-c |
| 9.3 (e) | los resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos; y | 1 | La definición existente de los riesgos se encuentra desactualizada, no se han definido adecuadamente los niveles de riesgo. | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos. | SGSI-6-1-a |
| 9.3 (f) | las oportunidades de mejora continua. | 0 | No se ha realizado las definiciones de mejoras continuas sobre el SGSI | Incluir las mejoras en la documentación sobre las mejoras basadas en la auditoria | SGSI-5-1-c |
| 9.3 | Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información. La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. | 0 | No se ha realizado las definiciones de mejoras continuas sobre el SGSI | Incluir un listado de los documentos relacionados con las mejoras continuas que se definan. | SGSI-5-1-c |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 11 |
| 1 | 9 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 0.45 |

## Resumen de la sección 9 - Evaluación del SGSI con ISO 27001

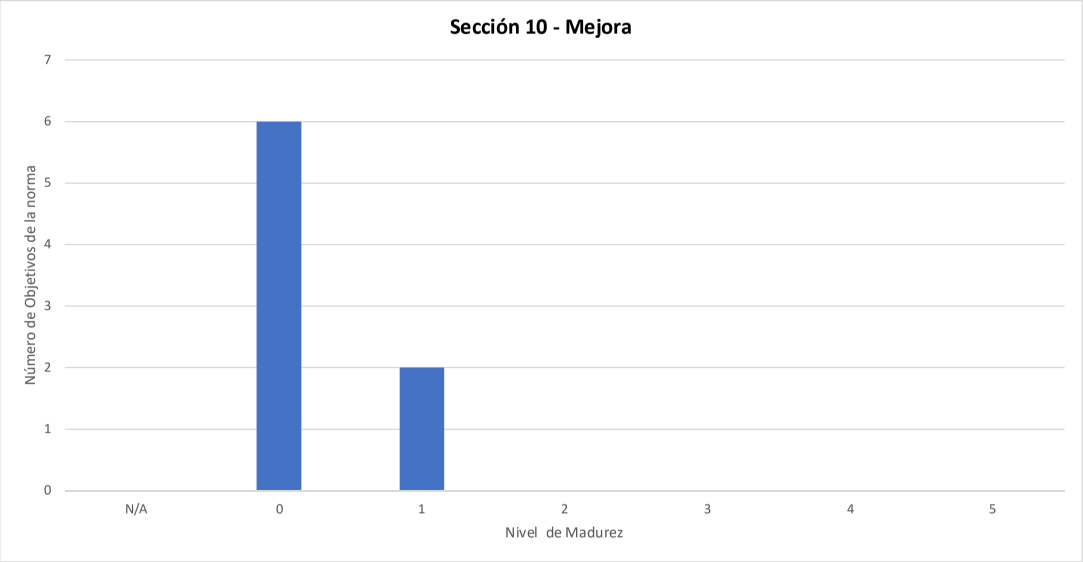


| Control de ISO /IEC 27001 | Requerimientos obligatorios para el SGSI | Valoración | Estado Actual | Planes de Acción | Codigo del plan de Acción |
|---|---|---|---|---|---|
| **10** | **Mejora** | | | | |
| **10.1** | **No confirmidades y acciones correctivas** | | | | |
| 10.1 | Cuando ocurra una no conformidad, la organización debe: | | | | |
| 10.1 (a) | reaccionar a la no conformidad y realizar lo siguiente:<br>1) tomar acción para controlarlo y corregirlo; y<br>2) afrontar con las consecuencias | 0 | No se ha definido acciones a tomarse en cuenta en relaciónal manejo de una no conformidad en una auditoria de seguridad de la información | Incluir en la documentación de las auditorias del SGSI, un proceso para manejo de no conformidades y su tratamiento | SGSI-9-2-a |
| 10.1 (b) | evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir,<br>ni ocurra en otra parte, mediante:<br>1) la revisión de la no conformidad,<br>2) la determinación de las causas de la no conformidad, y<br>3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir; | 0 | No se ha definido acciones a tomarse en cuenta en relaciónal manejo de una no conformidad en una auditoria de seguridad de la información | Incluir en la documentación de las auditorias del SGSI, un proceso para manejo de no conformidades y su tratamiento | SGSI-9-2-a |
| 10.1 (c) | Determinar e implementar las acciones preventivas necesarias | 1 | Se ha definido acciones preventivas iniciales, pero no se ha realizado la medición de su efectividad | Incluir en el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se detallen las acciones preventivas necesarias | SGSI-5-1-c |
| 10.1 (d) | Revisar las acciones preventivas tomadas y su efectividad | 0 | Se ha definido acciones preventivas iniciales, pero no se ha realizado la medición de su efectividad | Medir y documentar los resultados obtenidos en el plan de seguimiento de la eficacia de los controles previsto en el SGSI. | SGSI-5-1-c |
| 10.1 (e) | realizar cambios al SGSI si es necesario | 1 | Se ha llevado un registro insuficiente de los cambios realizados en el SGSI | Registrar los cambios que se realicen en el plan de seguimiento de la eficacia de los controles previsto en el SGSI. | SGSI-5-1-c |
| 10.1 | Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas. La organización debe conservar información documentada, como evidencia de: | | | | |
| 10.1 (f) | la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo; y | 0 | No se ha definido acciones a tomarse en cuenta en relación al manejo de una no conformidad en una auditoria de seguridad de la información | Incluir en la documentación de las auditorias del SGSI, un proceso para manejo de no conformidades y su tratamiento. | SGSI-9-2-a |
| 10.1 (g) | los resultados de cualquier acción correctiva. | 0 | No se ha definido acciones a tomarse en cuenta en relación al manejo de una no conformidad en una auditoria de seguridad de la información | Incluir en la documentación de las auditorias del SGSI, un proceso para manejo de no conformidades y su tratamiento. | SGSI-9-2-a |
| **10.2** | **Mejoramiento Continuo** | | | | |
| 10.2 | La organización debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, resultados de las auditorías, el análisis de los eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección | 0 | No se evidencia que se haya ejecutado un compromiso de mejora continua | Generar un documento de compromiso de cumplimiento de mejora continua del SGSI. | SGSI-5-2-a |

| Categoria | Total |
|---|---|
| N/A | 0 |
| 0 | 6 |
| 1 | 2 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 0.25 |

## Resumen de la sección 10 - Evaluación del SGSI con ISO 27001



| Numeral | Dominio o descripción | Valoración | Estado Actual | Planes de Acción | Código del plan de Acción |
|---|---|---|---|---|---|
| **A.5** | **Políticas de seguridad** | | | | |
| **A.5.1** | **Directrices de gestión de la seguridad de la información** | | | | |
| A.5.1.1 | Documento de la política de seguridad de la información. | 1 | Existe un documento de políticas de seguridad de la información pero se encuentra desactualizado | Actualizar el documento de la política de seguridad de la información. | SGSI-A1-A5-1-1 |
| A.5.1.2 | Revisión de la política de seguridad de la información. | 1 | Se han realizado pocas revisiones y ajustes sobre la política de seguridad de la información | Definir un cronograma de revisión de las políticas de seguridad de la información. | SGSI-A1-A5-1-1 |
| **A.6** | **Organización de la seguridad de la Información** | | | | |
| **A.6.1** | **Organización Interna** | | | | |
| A.6.1.1 | Compromiso de la dirección con la seguridad de la información | 2 | Se ha definido el compromiso respectivo para dar seguimiento y evaluación de las políticas de seguridad de la información | Generar un plan de asignación interna respecto a la definición, seguimiento y mantenimiento de las políticas de seguridad de la información. | SGSI-A1-A6-1-1 |
| A.6.1.2 | Coordinación de la seguridad de la información. | 1 | Existe poca coordinación respecto a la coordinación y seguimiento de la aplicación de coordinación para temas | Definir la asignación de responsabilidades para la coordinación de la seguridad de la información | SGSI-A1-A6-1-1 |
| A.6.1.3 | Asignación de responsabilidades para la seguridad de la información. | 1 | La asignación interna para el seguimiento y mantenimiento de las políticas de seguridad de la información | Definir la asignación de responsabilidades para la coordinación de la seguridad de la información | SGSI-A1-A6-1-1 |
| A.6.1.4 | Procesos de autorización para los servicios de procesamiento de información. | 1 | No todos los procesamientos de información conllevan una autorización | Definir una política de procesamiento de información que incluya autorizaciones | SGSI-A1-A6-1-2 |
| A.6.1.5 | Acuerdos sobre confidencialidad | 2 | La empresa maneja acuerdos de confidencialidad con sus empleados y proveedores | Reforzar la documentación sobre los acuerdos de confidencialidad con clientes y proveedores | SGSI-A1-A6-1-3 |
| A.6.1.6 | Contacto con las autoridades | 2 | Existe un contacto entre el personal de IT y las autoridades de la empresa | Definir una política de contacto con las autoridades para los temas de seguridad de la empresa. | SGSI-A1-A6-1-4 |
| A.6.1.7 | Contacto con grupos de interés especiales | 2 | Existe contacto con grupos de interés especiales para la institución | Definir una política de contacto con grupos de interés especiales en los temas de seguridad de la información. | SGSI-A1-A6-1-5 |
| A.6.1.8 | Revisión independiente de la seguridad de la información | 0 | No se ha definido revisiones independientes sobre seguridad de la información | Incluir en el plan de auditoria del SGSI, la auditoria de las políticas de seguridad de la información | SGSI-9-2-a |
| **A.6.2** | **Dispositivos para movilidad y teletrabajo.** | | | | |
| A.6.2.1 | Identificación de los riesgos relacionados con las partes externas | 1 | Se han identificado pocos riesgos respecto a las partes externas | Definir un análisis de riesgos referente al trato con partes externas, clientes, proveedores y terceras partes. | SGSI-A1-A6-2-1 |
| A.6.2.2 | Consideraciones de la seguridad cuando se trata con los clientes | 1 | Se han identificado pocos riesgos respecto al trato con los clientes | | |

| | | | | | |
|---|---|---|---|---|---|
| A.6.2.3 | Consideraciones de la seguridad en los acuerdos con terceras partes | 1 | Se han identificado pocos riesgos respecto a los acuerdos con los terceros | | |
| **A.7** | **Seguridad de los recursos humanos** | | | | |
| **A.7.1** | **Antes de la contratación.** | | | | |
| A.7.1.1 | Roles y responsabilidades | 1 | Los roles y responsabilidades se encuentran identificados pero no se encuentra documentados | Generar una política de contratación en donde se documenten los roles y responsabilidades de los cargos de la empresa, así como los perfiles de acceso a la información en base a ese cargo. | SGSI-A1-A7-1-1 |
| A.7.1.2 | Selección | 1 | En la gran mayoría de procesos de selección no se incluyen como competencias del puesto el conocimiento de seguridad de la información. | Incluir en la política de contratación, los parámetros de selección de personal y que se incluya el requerimiento de habilidades tales como conocimiento de seguridad de la información | |
| A.7.1.3 | Términos y condiciones laborales | 1 | Los términos y condiciones laborales no se encuentran documentadas a detalle en los contratos y solo se señalan verbalmente. Existe únicamente un acuerdo de confidencialidad al inicio de la contratación. | Incluir en la política de contratación de personal los términos y condiciones laborales respecto al alcance de la información que ese cargo manejará y la seguridad de la información asociada con estos términos | |
| **A.7.2** | **Durante la contratación** | | | | |
| A.7.2.1 | Responsabilidades de la dirección | 1 | Los procesos de responsabilidad de la dirección se encuentran poco delineados y la documentación existente es insuficiente. | En la política de contratación de personal incluir la definición de responsabilidades de la dirección del personal y el acceso a la información | SGSI-A1-A7-1-1 |
| A.7.2.2 | Educación, formación y concientización sobre la seguridad de la información | 1 | No existe un proceso o documentación que haga referencia a la seguridad de la información que manejan los empleados. Existe únicamente un acuerdo de confidencialidad al inicio de la contratación. | Incluir en la política de contratación la necesidad de habilidades como conocimiento de seguridad de la información o capacitaciones para el personal que no tenga estas habilidades | |
| A.7.2.3 | Proceso disciplinario | 0 | No existe documentado un proceso disciplinario respecto a fallas o negligencia respecto a seguridad de la información | Incluir en la política de contratación una sección referente al proceso disciplinario | |
| **A.7.3** | **Cese o cambio de puesto de trabajo** | | | | |
| A.7.3.1 | Responsabilidades en la terminación | 1 | Se ejecutan tareas de forma intuitiva, no existe una política o practica bien definida. | En la política de contratación de personal incluir las tareas y actividades cuando una persona cesa funciones dentro de la empresa respecto a la información que manejaba ese colaborador | SGSI-A1-A7-1-1 |
| **A.8** | **Gestión de activos** | | | | |
| **A.8.1** | **Responsabilidad de los bienes** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| A.8.1.1 | Inventario de activos | 1 | El inventario de activos se encuentra desactualizado al momento | Actualizar el inventario tecnológico e incluir la fecha de adquisición de ese activo tecnológico. | SGSI-A1-A8-1-1 |
| A.8.1.2 | Propiedad de los activos | 2 | Cuando se entregan activos a los colaboradores/clientes se generan actas de entrega y recepción señalando al dueño del activo | Incluir una bitácora de entregas de activos tecnológicos a colaboradores. | SGSI-A1-A8-1-1 |
| A.8.1.3 | Uso aceptable de los activos | 1 | La definición de uso aceptable de los activos no se ha dado a en todos los empleados de la empresa | Definir una política de uso aceptable de los activos tecnológicos de la empresa. | SGSI-A1-A8-1-2 |
| A.8.1.4 | Devolución de activos | 2 | Cuando se entregan activos a los colaboradores/clientes se generan actas de entrega y recepción señalando al dueño del activo | Incluir una bitácora de devoluciones de activos tecnológicos hechas por los colaboradores | SGSI-A1-A8-1-1 |
| **A.8.2** | **Clasificación de la Información** | | | | |
| A.8.2.1 | Directrices de clasificación | 1 | Existe una directriz para clasificación de información únicamente en el área comercial | Documentar la directriz de clasificación de información existente y ampliarla a las demás áreas de la empresa. | SGSI-A1-A8-2-1 |
| A.8.2.2 | Etiquetado y manejo de información | 1 | Existe un etiquetado en el manejo de información física, sin embargo eso no se lo ha llevado a la documentación digital. | Documentar la directriz sobre el etiquetado de la información y ampliarlo a la documentación digital. | SGSI-A1-A8-2-1 |
| A.8.2.3 | Manipulación de activos | 1 | Se tiene delineado que usuarios pueden acceder a que activos de información pero esa información no se encuentra documentada y parametrizada en base a la relación laboral del usuario | Documentar los permisos de los usuarios y sus accesos regulares hacia que equipos tecnológicos en base a su rol en la empresa. | SGSI-A1-A8-2-1 |
| **A.8.3** | **Manejo de los soportes de almacenamiento** | | | | |
| A.8.3.1 | Gestión de soportes extraíbles | 1 | Se tiene implementado gestión de medios extraíbles únicamente en una unidad del negocio. También se manejan respaldos en medios extraíbles | Extender la política de gestión medios extraíbles y soportes de almacenamiento a toda la organización en base a las necesidades de la empresa. | SGSI-A1-A8-2-2 |
| A.8.3.2 | Eliminación de soportes | 2 | Se cuenta con un procedimiento detallado para la sanitización de datos y eliminación de soportes tecnológicos | Incluir el procedimiento en la política de gestión de medios extraibles y soportes, definiendo el uso de herramientas y consideraciones mas actualizadas sobre sanitización de medios | SGSI-A1-A8-2-2 |
| A.8.3.3 | Soportes físicos en tránsito | N/A | No se manejan casos de soportes físicos de almacenamiento en tránsito | No se manejan casos de soportes físicos de almacenamiento en tránsito | |
| **A.9** | **Control de acceso** | | | | |
| **A.9.1** | **Requisitos de negocio para el control de accesos.** | | | | |
| A.9.1.1 | Política de control de acceso | 1 | Se ha definido una política de control de acceso básica utilizando un usuario y contraseña sobre el medio de conexión | Se debe definir una política de control de acceso a recursos | SGSI-A1-A9-1-1 |

| | | | | | |
|---|---|---|---|---|---|
| A.9.1.2 | Acceso a las redes y a los servicios de red | 1 | Se ha definido una política de control de acceso básica utilizando un usuario y contraseña sobre el medio de conexión | utilizando usuarios temporales y autenticacion temporal. | SGSI-A1-A9-1-1 |
| **A.9.2** | **Gestión de acceso de usuario** | | | | |
| A.9.2.1 | Registro y baja de usuario | 1 | Existe un proceso y evidencia de creación y eliminación de usuarios, sin embargo no se lleva una bitácora de esas actividades. | Generar una política de gestion de usuarios y contraseñas en donde se señalen los lineamientos de seguridad de los usuarios y contraseñas. | SGSI-A1-A9-2-1 |
| A.9.2.2 | Provisión de acceso de usuario | 1 | Una vez creado el usuario solicitado, se procede a entregar las credenciales de acceso al usuario en específico. | | |
| A.9.2.3 | Gestión de privilegios de acceso | 1 | Se manejan los privilegios acorde a las indicaciones de la creación de usuarios, no se tiene una definición de usuarios y privielgios avanzada. | | |
| A.9.2.4 | Gestión de la información secreta de autenticación de los usuarios | 2 | Las contraseñas de los usuarios se almacenan en un cloud externo. | | |
| A.9.2.5 | Revisión de los derechos de acceso de usuario | 1 | Solo ciertos accesos son revisados para cada usuario y su uso no se encuentra documentado. | | |
| A.9.2.6 | Retirada o reasignación de los derechos de acceso | 1 | Si un empleado deja la empresa o su rol cambia se procede a modificar sus permisos de acceso. No hay bitacoras de estos movimientos | | |
| **A.9.3** | **Responsabilidades del usuario** | | | | |
| A.9.3.1 | Uso de la información secreta de autenticación | 1 | Únicamente para la autenticación se ha implementado el uso de usuario y contraseña | Definir una política de uso de esquemas de autenticación mas robustas como uso de biométrica o doble factor de autenticación. | SGSI-A1-A9-3-1 |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones.** | | | | |
| A.9.4.1 | Restricción del acceso a la información | 2 | Existe una restricción de acceso para algunos de los recursos de la empresa en base a usuarios y perfiles. | Definir una política de restricción de acceso a sistemas y aplicaciones basada en permisos y usuarios. | SGSI-A1-A9-4-1 |
| A.9.4.2 | Procedimientos seguros de inicio de sesión | 2 | Los inicios de sesión se realizan a traves de protocolos seguros como NTLM y HTTPS | | |
| A.9.4.3 | Gestión de contraseñas de usuario. | 2 | Se tiene el uso de contraseñas temporales para los usuarios y los cambios de contraseña unicamente los hace el administrador de IT | | |
| A.9.4.4 | Uso de utilidades con privilegios del sistema | 1 | Se ha configurado para que pocas aplicaciones lleven seguridad de ejecución con privilegios de usuario. | Definir una política de uso de software y permisos de sistema operativo dependiendo de los usuarios. | SGSI-A1-A9-4-2 |

| | | | | | |
|---|---|---|---|---|---|
| A.9.4.5 | Control de acceso al código fuente de los programas. | 1 | El acceso al código fuente se encuentra delimitado pero no se almacena en los servidores de la empresa. | Definir una política de protección de acceso al repositorio de código fuente de los programas entregados. | SGSI-A1-A9-4-3 |
| **A.10** | **Criptografía** | | | | |
| **A.10.1** | **Controles criptográficos** | | | | |
| A.10.1.1 | Política de uso de los controles criptográficos | N/A | No se manejan controles criptográficos | No se manejan controles criptográficos | |
| A.10.1.2 | Gestión de claves | 2 | Las claves de acceso a los servicios IT se encuentran almacenadas localmente y remotamente, solo el personal de IT tiene acceso a estas claves | Crear una nueva política de gestión de claves en donde se incluyan las prácticas de seguridad ya existentes y nuevas consideraciones de seguridad. | SGSI-A1-A10-1-1 |
| **A.11** | **Seguridad física y del entorno** | | | | |
| **A.11.1** | **Áreas seguras** | | | | |
| A.11.1.1 | Perímetro de seguridad física. | 1 | Por normas del edificio se ha definido un perímetro de seguridad física en cada oficina | Definir una política de acceso, seguridad física de la oficina y sus diferentes áreas para colaboradores y proveedores. | SGSI-A1-A11-1-1 |
| A.11.1.2 | Controles físicos de entrada. | 2 | Se cuentan en el edificio con controles físicos tales como puertas con tarjetas electromagneticas, guardiania, camaras de vigilancia | | |
| A.11.1.3 | Seguridad de oficinas, despachos y recursos. | 2 | El acceso a los despachos y anaqueles que contiene información importante se encuentran con llaves, de igual manera las oficinas y are ade equipos. | | |
| A.11.1.4 | Protección contra las amenazas externas y ambientales. | 1 | Existen implementadas algunas medidas de protección contra amenazas externas y ambientales provistas por el edificio en donde funciona la empresa | | |
| A.11.1.5 | El trabajo en áreas seguras. | 1 | Se ha definido áreas seguras para los trabajadores, sin emabrgo la distribución actual necesita tener en cuenta lineamientos de seguridad y señaleticas | | |
| A.11.1.6 | Áreas de acceso público, carga y descarga. | 1 | Se cuenta con un área para acceso al publico, sin embargo esta cerca del cuarto de equipos. | | |
| **A.11.2** | **Seguridad de los equipos** | | | | |
| A.11.2.1 | Emplazamiento y protección de equipos. | 1 | Los equipos de IT se encuentran emplazados en un Data Center con restricciones de acceso. | Incluir en la política de acceso, seguridad física de la oficina las protecciones que deben tener considerados los equipos informáticos y de IT. | SGSI-A1-A11-2-1 |
| A.11.2.2 | Instalaciones de suministro. | 2 | El suministro electrico se encuentra cubierto con un UPS acorde al Data Center, adicionalmente el edificio cuenta con una planta de energia en caso de fallas | Definir un plan de mantenimiento y mejora respecto a la instalación de suministro y sus contingencias como el UPS | SGSI-A1-A11-2-2 |

| | | | | | |
|---|---|---|---|---|---|
| A.11.2.3 | Seguridad del cableado. | 1 | El cableado con el que se cuenta es antiguo. Al momento no todas las secciones del cableado se encuentran en buen estado, no estan organizadas correctamente | Definir un plan de actualización, mantenimiento del cableado estructurado y organización en los rack del data center. | SGSI-A1-A11-2-3 |
| A.11.2.4 | Mantenimiento de los equipos. | 1 | Los equipos de comunicaciones tienen planes de mantenimientos anuales. Los servidores y otros equipos no cuentan con planes de mantenimiento. | Definir un plan de mantenimiento, actualización y reasignación de equipos y medios dentro y fuera de la empresa e incluir garantias o seguros. | SGSI-A1-A11-2-4 |
| A.11.2.5 | Salida de activos fuera de las dependencias de la empresa. | 1 | Se cuenta con un procedimiento para cuando los activos de la empresa salen fuera de la dependencia de la empresa. Los equipos no cuentan con seguros/garantias. | | |
| A.11.2.6 | Seguridad de los equipos y activos fuera de las instalaciones. | 0 | No se cuenta con garantias/seguros para los equipos informáticos | | |
| A.11.2.7 | Reutilización o retirada segura de dispositivos de almacenamiento. | 1 | Se tiene delimitado una política de reutilización de medios y dispositivos de almacenamientos cuando esten soportados | Actualizar y reforzar la política de reutilización de medios e incluir procedimientos para la retirada segura de dispositivos de almacenamiento. | SGSI-A1-A11-2-5 |
| A.11.2.8 | Equipo informático de usuario desatendido. | 1 | Para el trabajo en oficina se cuentan con recomendaciones de seguridad, sin embargo no estan difundidas y socializadas en toda la empresa. | Definir una política para el manejo de equipos informáticos de usuarios desatendidos y adicionar una política de puesto de trabajo despejado y bloqueo de pantalla de forma automática. | SGSI-A1-A11-2-6 |
| A.11.2.9 | Política de puesto de trabajo despejado y bloqueo de pantalla. | 0 | No se cuenta con políticas de puesto de trabajo despejado y bloqueo de pantalla | | |
| **A.12** | **Seguridad en la Operación** | | | | |
| **A.12.1** | **Responsabilidades y procedimientos de operación** | | | | |
| A.12.1.1 | Documentación de procedimientos de operación. | 1 | Existe poca documentación sobre los procedimientos de operación de la empresa. | Definir una política de documentación de la operación tales como apagado/encendido de equipos. Gestion de cambios y Gestión de capacidades | SGSI-A1-A12-1-1 |
| A.12.1.2 | Gestión de cambios. | 1 | La gestión de cambios unicamente se lo hace en casos especiales cuando hay cambios en la infraestructura. Esta gestión de cambios no se documenta correctamente. | | |

| | | | | | |
|---|---|---|---|---|---|
| A.12.1.3 | Gestión de capacidades. | 1 | La gestión de capacidades se realiza de forma reactiva, la expansión de capacidades se maneja en peridos largos dentro de la empresa (2-3 años) | | |
| A.12.1.4 | Separación de entornos de desarrollo, prueba y producción. | 2 | En la empresa se cuentan con entornos de desarrollo y pruebas localmente. Los ambientes de producción se publican en servidores en cloud | Actualizar la definición de la separación de los ambientes de desarrollo, prueba y producción con herramientas de automatización. | SGSI-A1-A12-2-1 |
| **A.12.2** | **Protección contra código malicioso** | | | | |
| A.12.2.1 | Validación de los datos de entrada | 2 | En los desarrollos realizados se valida los datos de entrada y la inyección de código | Incluir en la política de seguridad en la operación lineamientos sobre nuevos métodos de ataques y como manejarlos | SGSI-A1-A12-2-1 |
| **A.12.3** | **Copias de seguridad** | | | | |
| A.12.3.1 | Copias de seguridad de la información | 1 | Se generan copias de seguridad de la información de forma irregular | Establecer una política de copias de seguridad para los activos de mayor importancia. | SGSI-A1-A12-3-1 |
| **A12.4** | **Registros y supervisión** | | | | |
| A12.4.1 | Registro de eventos | 0 | No se generan procesos relacionados a los logs de los componentes ni su almacenamiento y revisión | Definir una política de tratamiento, almacenamiento y revisión de logs de los equipos IT de la empresa. Incluir la sincronocidad de tiempo en sus procedimientos. | SGSI-A1-A12-4-1 |
| A12.4.2 | Protección de la información del registro | 0 | Los logs de los equipos no se descargan ni se almacenan en algún repositorio | | |
| A12.4.3 | Registros de administradores y usuarios | 1 | En los servidores y algunos equipos IT se almacenan las actividades ejecutadas por los administradores y se conservan detro de los equipos | | |
| A12.4.4 | Sincronización del reloj | 2 | En los equipos IT se realiza la sincronización de la fecha y hora por medio de servidores NTP publicos | | |
| **A12.5** | **Control del software en ambientes operacionales** | | | | |
| A12.5.1 | Instalación del software en ambientes operacionales | 2 | El software que se utilizan en la empresa es licenciado y se encuentra previamente probado y validado. Se tienen en cuenta una política local de actualizaciones de componentes y librerias de software | Reforzar y actualizar la política de adquisición de software para uso empresarial con el fin mantener el software empresarial lo mas estable posible y actualizado. | SGSI-A1-A12-5-1 |
| **A12.6** | **Gestión de la vulnerabilidad técnica** | | | | |
| A12.6.1 | Gestión de las vulnerabilidades técnicas | 0 | No se hace gestión de vulnerabilidades técnicas respecto a los componentes de software y hardware. | Definir un plan de hardening semestral de los equipos informáticos que permitan parchar las vulnerabilidades | SGSI-A1-A12-6-1 |

| | | | | | |
|---|---|---|---|---|---|
| A12.6.2 | Restricción en la instalación de software | 1 | La restricción de instalación de software se maneja a nivel de servidores, en el caso de los usuarios de equipos de escritorio no se lleva ese control | Definir un plan de control de roles y permisos de usuario a nivel del sistema operativo para evitar instalación de software sin autorización. | SGSI-A1-A9-4-2 |
| **A12.7** | **Consideraciones sobre la auditoria de sistemas de información** | | | | |
| A12.7.1 | Controles de auditoría de sistemas de información | 0 | No se ha realizado una auditoria sobre el SGSI y las políticas de seguridad existentes | Definir un plan de auditoria para el SGSI, sus políticas y sus resultados | SGSI-9-2-a |
| **A13** | **Seguridad de las comunicaciones** | | | | |
| **A13.1** | **Gestión de la seguridad de las redes** | | | | |
| A13.1.1 | Controles de red | 2 | Actualmente existen controles de red para separar las unidades de negocio a traves del firewall. | Definir una política de diseño, implementación y operación de una red redundante y con medidas de seguridad acorde a las necesidades de la empresa. | SGSI-A1-A13-1-1 |
| A13.1.2 | Seguridad de los servicios de red | 1 | Se han implementado protocolos de seguridad parcialmente en los servicios de red | | |
| A13.1.3 | Segregación en redes | 1 | Existe segregación de redes unicamente por el firewall. | | |
| **A13.2** | **Intercambio de información** | | | | |
| A13.2.1 | Políticas y procedimientos de intercambio de información | 0 | No se ha definido una política de intercambio de información. | Definir una política de intercambio de información y mensajería electrónica. | SGSI-A1-A13-2-1 |
| A13.2.2 | Acuerdos de intercambio de información | 0 | No se ha definido un acuerdo de intercambio de información entre la empresa y sus clientes/proveedores. | | |
| A13.2.3 | Mensajería electrónica | 0 | No se ha definido políticas de uso aceptable para la mensajeria electrónica de la empresa. | | |
| A13.2.4 | Acuerdos de confidencialidad o no revelación | 2 | Se manejan acuerdos de confidencialidad con los proveedores y empleados.Asi mismo la empresa firma contratos de confidencialidad con sus clientes. | Reforzar el manejo de acuerdos de confidencialidad y generar una bitácora de acuerdos activos de la empresa. | SGSI-A1-A6-1-3 |
| **A14** | **Adquisición, desarrollo y mantenimiento de los sistemas de información** | | | | |
| **A14.1** | **Requisitos de seguridad en los sistemas de información** | | | | |
| A14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | 2 | En la mayoria de ocasiones se consieran los requisitos de seguridad en los sistemas de información como pruebas de errores, vulnerabilidades, etc | Definir una política de implementación de seguridad en servidores que alberguen sistemas de información. | SGSI-A1-A14-1-1 |
| A14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | 2 | En las fases de implementación se aseguran las aplicaciones que se publican hacia redes publicas con algunos mecanismos de seguridad | | |
| A14.1.3 | Protección de las transacciones de servicios de aplicaciones | 1 | Existen procedimientos para asegurar las transacciones de servicios de aplicaciones | | |

| | | | | | |
|---|---|---|---|---|---|
| **A14.2** | **Seguridad en el desarrollo y en los procesos de soporte** | | | | |
| A14.2.1 | Política de desarrollo seguro | 1 | No existe definida una política de desarrollo seguro denytro de la empresa, si no que se siguen algunas recomendaciones sobre desarrollo seguro | Definir una política de desarrollo seguro para la empresa basada en principios de ingenieria de sistemas seguros. | SGSI-A1-A14-2-1 |
| A14.2.2 | Procedimiento de control de cambios en sistemas | 1 | Se ejecutan control de cambios en ocasiones, en donde se hacen cambios mayores sobre los sistemas existentes. Existen registros de cambios de más de un año. | Definir una política de control de cambios en los sistemas de la empresa que incluyan cambios en funcionalidad, en sus librerias, en su entorno de desarrollo o en paquetes de software. | SGSI-A1-A14-2-2 |
| A14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | 1 | Cuando existen actualizaciones a nivel del sistema operativo, solo se revisan las aplicaciones que ofrecen un servicio o se levantan automáticamente | | |
| A14.2.4 | Restricciones a los cambios en los paquetes de software | 1 | Solo se ejecutan cambios en los paquetes de software cuando se van a realizar actualización de librerias. No hay una restricción definida | | |
| A14.2.5 | Principios de ingeniería de sistemas seguros | 1 | Para el desarrollo de sistemas se toman en cuenta algunos principios de ingenieria de desarrollo seguro. | Definir una política de desarrollo seguro para la empresa basada en principios de ingenieria de sistemas seguros. | SGSI-A1-A14-2-1 |
| A14.2.6 | Entorno de desarrollo seguro | 0 | El entorno de desarrollo no tiene definidas medidas de seguridad configuradas. | Definir una política de aseguramiento del entorno de desarrollo. | SGSI-A1-A14-2-3 |
| A14.2.7 | Externalización del desarrollo de software | N/A | No se externaliza el desarrollo de sistemas en la empresa | No se externaliza el desarrollo de sistemas en la empresa | |
| A14.2.8 | Pruebas funcionales de seguridad de sistemas | 0 | No se realiza pruebas funcionales de seguridad en los sistemas desarrollados | Definir un procedimiento para ejecutar pruebas funcionales de seguridad en los sistemas desarrollados. | SGSI-A1-A14-2-4 |
| A14.2.9 | Pruebas de aceptación de sistemas | 1 | Los desarrollos que se ejecutan llevan pruebas de aceptación del sistema basado en los requisitos del sistema levantados inicialmente | Definir una política de pruebas de aceptación basada en cumplimiento de requisitos y normas de seguridad. | SGSI-A1-A14-2-5 |
| **A14.3** | **Datos de prueba** | | | | |
| A14.3.1 | Protección de los datos de prueba | 1 | Los datos de prueba que se utilizan no como manejar y proteger datos de prueba tienen una protección adecuada. | Definir una política de tratamiento de datos de pruebas, su procesamiento y privacidad en caso de ser datos personales. | SGSI-A1-A14-3-1 |
| **A15** | **Relación con proveedores** | | | | |
| **A15.1** | **Seguridad en las relaciones con proveedores** | | | | |
| A15.1.1 | Política de seguridad de la información en las relaciones con los proveedores | 2 | Se maneja un conjunto de normas y buenas practicas en el manejo de politicas de seguridad y firma de acuerdos de confidencialidad. | Reforzar el manejo de acuerdos de confidencialidad y generar una bitácora de acuerdos activos de la empresa. | SGSI-A1-A13-2-2 |

| | | | | | |
|---|---|---|---|---|---|
| A15.1.2 | Requisitos de seguridad en contratos con terceros | 0 | No se ha definido un acuerdo de intercambio de información entre la empresa y terceros | Incluir en la política de intercambio de información y mensajería electrónica. | SGSI-A1-A13-2-1 |
| A15.1.3 | Cadena de suministro de tecnología de la información y de las comunicaciones | 1 | Se ha definido algunos proveedores regulares de la empresa en temas de servicios o componentes IT. | Definir una política de gestión de suministros IT, comunicaciones y servicios de IT | SGSI-A1-A15-2-1 |
| **A15.2** | **Gestión de la provisión de servicios del proveedor** | | | | |
| A15.2.1 | Control y revisión de la provisión de servicios del proveedor | 1 | Se lleva un control de provisión de servicio en algunos de los proveedores que se tiene contratado al momento | Definir una política de control de los servicios contratados con los proveedores en base a disponibilidad de servicio y cumplimiento del SLA. | SGSI-A1-A15-2-1 |
| A15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | 0 | No se ha establecido planes o políticas referentes a la provisión del servicio del proveedor | | |
| **A16** | **Gestión de incidentes de seguridad de la información** | | | | |
| **A16.1** | **Gestión de incidentes de seguridad de la información y mejoras** | | | | |
| A16.1.1 | Responsabilidades y procedimientos | 1 | Se ha definido la responsabilidad y procedimientos de seguridad de la empresa al departamento IT | Definir una política de gestión de incidentes de seguridad de la información que incluya procedimientos de analisis, recopilación y mejora continua. | SGSI-A1-A16-1-1 |
| A16.1.2 | Notificación de los eventos de seguridad de la información | 1 | En caso de existir un evento de seguridad de la información, la notificación del evento se la haría por parte del Gerente técnico con Autorización del Gerente General | | |
| A16.1.3 | Notificación de puntos débiles de la seguridad | 1 | El Gerente técnico identifica los puntos débiles de la seguridad de forma reactiva, y sin periodicidad | | |
| A16.1.4 | Evaluación y decisión sobre los eventos de seguridad de información | 1 | En caso de existir un evento de seguridad de la información, la evaluación y decisión sobre evento se la haría por parte de los Gerentes General y Técnico. | | |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | 1 | En caso de existir un evento de seguridad de la información, la respuesta a incidentes de seguridad se lo hace bajo la habilidad del personal de IT, no hay procesos de respuesta a incidentes. | | |
| A16.1.6 | Aprendizaje de los incidentes de seguridad de la información | 1 | Luego de los incidentes de seguridad de la información se documentan los procesos que se ejecutaron para solventar el incidente de seguridad. Luego de eso este procedimiento no lleva seguimiento ni actualización. | | |

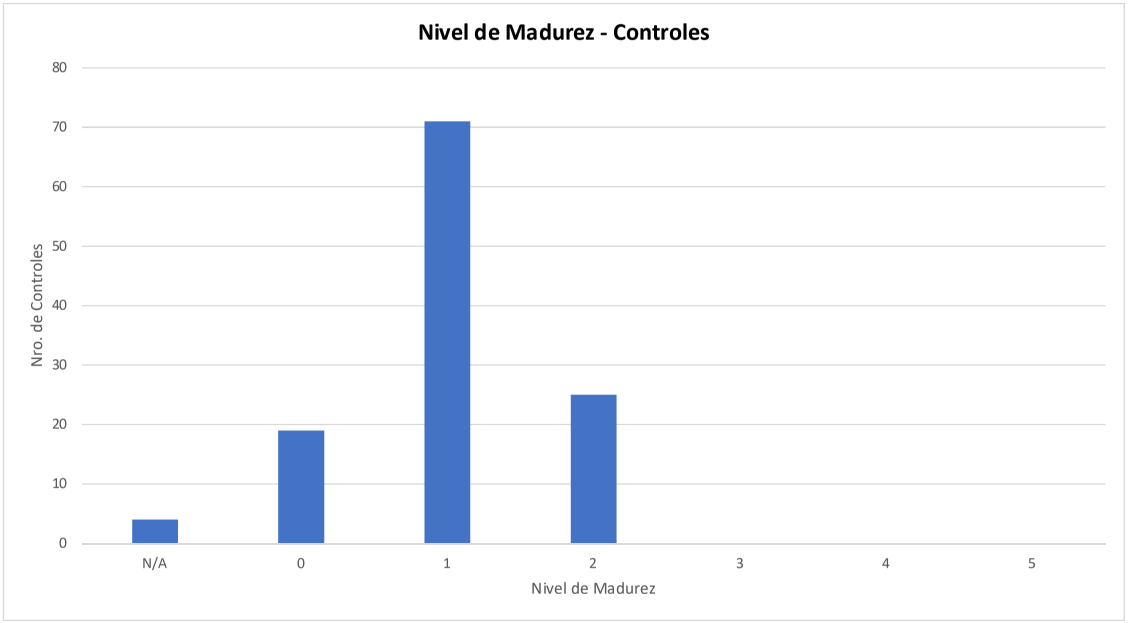
| | | | | | |
|---|---|---|---|---|---|
| A16.1.7 | Recopilación de evidencias | 1 | La recopilación de evidencias se lo hace de forma reactiva y a modo de diagnostico de los eventos de seguridad. Esta recopilación no sigue algun proceso o buena práctica. | | |
| **A17** | **Aspectos de seguridad de la información para la gestión de la continuidad de negocio** | | | | |
| **A17.1** | **Continuidad de la seguridad de la información** | | | | |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | 1 | La continuidad de la seguridad de la información no esta contemplada en sus esquemas de funcionamiento actuales | Definir un plan de continuidad de la seguridad de la información, sus controles, su revisión, ajuste y mejora continua. | SGSI-A1-A17-1-1 |
| A17.1.2 | Implementar la continuidad de la seguridad de la información | 0 | Al momento no se encuentra implementada continuidad en la seguridad de la información | | |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | 0 | No se ha definido planes de seguimiento de la continuidad de la seguridad de la información | | |
| **A17.2** | **Redundancias** | | | | |
| A17.2.1 | Disponibilidad de los recursos de tratamiento de la información | 1 | Existen pocos componentes tecnológicos que cuentan con componentes y/o esquemas de redundancia | Definir un proyecto para reforzar y mejorar los esquemas existentes en los componentes que se consideren como críticos. | SGSI-A1-A17-2-1 |
| **A18** | **Cumplimiento** | | | | |
| **A18.1** | **Cumplimiento de los requisitos legales y contractuales** | | | | |
| A18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | 2 | La empresa cuenta con una conformación bajo la ley y cumple con la legislación aplicable | Realizar una auditoria externa para identificar puntos de mejora respecto al cumplimiento legal y requisitos contractuales. | SGSI-A1-A18-1-1 |
| A18.1.2 | Derechos de Propiedad Intelectual (DPI) | 0 | Los desarrollos de software elaborados por la empresa no se amaparan bajo derechos de propiedad Intelectual | Definir una política para registro de derechos de propiedad intelectual en el caso de los desarrollos que se manejan dentro de la empresa. | SGSI-A1-A18-1-2 |
| A18.1.3 | Protección de los registros de la organización | 1 | La mayoria de los registros de la organización cuentan con respaldo físico y pocos de estos componentes tienen respaldo digital. Los registros físicos cuentan con protecciones básicas. | Definir una política de protección de los registros de la organización y reforzar las medidas de seguridad de estos registros. | SGSI-A1-A18-1-3 |
| A18.1.4 | Protección y privacidad de la información de carácter personal | 1 | Como parte de politicas de la empresa, se mantienen definiciones sobre la privacidad y protección de la información de carácter personal. | Definir una política de protección y privacidad de la información de carácter personal. | SGSI-A1-A18-1-4 |
| A18.1.5 | Regulación de los controles criptográficos | N/A | No se manejan controles criptográficos | No se manejan controles criptográficos | |
| **A18.2** | **Revisiones de la seguridad de la información** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| A18.2.1 | Revisión independiente de la seguridad de la información | 0 | No se ha realizado una auditoria sobre el SGSI y las políticas de seguridad existentes | Definir un plan de auditoria para el SGSI, sus políticas y sus resultados | SGSI-9-2-a |
| A18.2.2 | Cumplimiento de las políticas y normas de seguridad | 1 | El conjunto de políticas sigue con la estructura de la norma, sin embargo no se han realizado mejoras significativas a las políticas | | |
| A18.2.3 | Comprobación del cumplimiento técnico | 1 | Se ha seguido el esquema de políticas pero no se han hecho mediciones de la efectividad y cumplimiento de las políticas | | |

| Categoria | Total |
|---|---|
| N/A | 4 |
| 0 | 19 |
| 1 | 71 |
| 2 | 25 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

| Promedio |
|---|
| 1.05 |

## Resumen de la sección Anexo A - Evaluación del SGSI con ISO 27002



| Código Plan | Plan de Acción | Categoria del Proyecto | Fuente | Objetivos del Plan de Acción | Desarrollo del Plan | Fecha Inicio | Fecha Fin |
|---|---|---|---|---|---|---|---|
| SGSI-4-1-a | Actualizar la definición de las partes interesadas del SGSI tomando en contexto la realidad actual de la empresa | Cumplimiento Norma | Análisis SGSI | Actualizar la definición de las partes interesadas para brindar un mejor conocimiento de la organización y su contexto. | Actualizar la definición de las partes interesadas, los requisitos de las partes interesadas y el contexto interno y externo de la empresa. Reforzar y actualizar la definición de interfaces y dependencias con otras organizaciones. Actualizar la documentación referente al alcance del SGSI. | 1/12/2021 | 30/12/2021 |
| SGSI-4-2-a | Actualizar el SGSI para cubrir las necesidades actuales de la empresa | Cumplimiento Norma | Análisis SGSI | Actualizar y reforzar el SGSI para que sea establecido acorde a las necesidades actuales de la empresa. | Definir las necesidades actuales de la empresa, definir como el SGSI aopya a las actividades de la empresa. Definir un procedimiento para mantener y proveer una retroalimentación para la mejora continua en cuanto a cubrir las necesidades de la empresa por medio del SGSI. | 1/12/2021 | 30/12/2021 |
| SGSI-5-1-a | Ajustar la política de seguridad y sus objetivos para que estos sean compatibles con la dirección estratégica de la organización. | Refuerzo | Análisis SGSI | Revisar y reforzar las políticas de seguridad, sus objetivos y que estas políticas esten alineadas a los objetivos de la organización. | Actualizar los objetivos empresariales. Actualizar el lsitado de políticas de seguridad. Definir una matriz entre los objetivos de la empresa y las políticas de seguridad de la información. | 1/4/2022 | 1/5/2022 |
| SGSI-5-1-b | Crear un plan de comunicación sobre el seguimiento de las actividades referentes al SGSI y sus ajustes. | Cumplimiento Norma | Análisis SGSI | Crear un plan de comunicaciones que informe de las actividades respecto al SGSI y sus avances. | Crear un cronograma de comunicaciones. Definir las actividades a ser comunicadas. Definir los responsables de comunicar estos avances. Definir un plan de aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 |
| SGSI-5-1-c | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan factores de medición. | Mejora Continua | Análisis SGSI | Actualizat el plan de segumiento de la eficacia de los controles definidos el SGSI. | Definir las métricas que se asociarán a los controles. Definir los umbrales de las métricas. Definir la periodicidad de cuando se tomen las mediciones. Definir un formato de documentación de las mediciones. Medir y documentar los resultados obtenidos en el plan de seguimiento de la eficacia de los controles previsto en el SGSI. Incluir un listado de los documentos relacionados con las mejoras continuas que se definan. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-5-2-a | Generar un documento de compromiso de cumplimiento de mejora continua del SGSI. | Mejora Continua | Análisis SGSI | Actualizar y generar un nuevo documento de compromiso de cumplimiento de requisitos aplicables respecto a la seguridad de la información. Se debe incluir comprobación del cumplimiento del compromiso. | Generar un nuevo documento de compromiso de cumplimiento de requisitos aplicables respecto a la seguridad de la información. Generar un formato de constancia sobre el cumplimiento del compomiso de mejora continua del SGSI. | 1/12/2021 | 30/12/2021 |
| SGSI-5-2-b | Generar un plan de documentación del SGSI que incluya versionamiento y actualizaciones periodicas | Cumplimiento Norma | Análisis SGSI | Definir un plan de documentación para el manejo de la documentación del SGSI. | Definir un sistema de versionamiento de esta documentación. Definir los responsables de los cambios de la documentación. Definir el proceso de aprobación de la documentación. | 1/7/2022 | 1/9/2022 |
| SGSI-5-2-c | Generar un plan de comunicación sobre las políticas que tiene el SGSI en la empresa y definir un calendario de comunicación | Cumplimiento Norma | Análisis SGSI | Crear un plan de comunicaciones que informe de las políticas definidas en el SGSI, así como su aplicación dentro de la empresa. | Crear un cronograma de comunicaciones. Definir las actividades a ser comunicadas. Definir los responsables de comunicar estos avances. Definir un plan de aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 |
| SGSI-5-2-d | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | Cumplimiento Norma | Análisis SGSI | Definir un plan de almacenamiento de la documentación del SGSI dentro de la organización. | Definir la ubicación en donde se va a almacenar la documentación del SGSI. Definir los permisos de lectura/escritura que les serán asignados a los diferentes miembros de la organización. Definir los planes de respaldos de la documentación. Incluir en el plan de almacenamiento las instrucciones para la identificación de la documentación externa | 1/7/2022 | 1/9/2022 |
| SGSI-5-3-a | Realizar una revisión interna luego de 6 meses de haberse implementado el nuevo SGSI en la organización.para definir el estado del SGSI | Mejora Continua | Análisis SGSI | Definir un plan de revisión interna luego de haberse modificado el SGSI para definir un nuevo estado del SGSI. | Definir un cronograma de revisiones internas para actualizar el estado del SGSI. Definir los responsables de la revisión del SGSI. Definir el formato de presentación del estado del SGSI. | 1/6/2022 | 1/7/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-6-1-a | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos. | Refuerzo | Análisis SGSI | Actualizar el listado de riesgos considerados para la operación de la empresa en base a la situación actual de la empresa. | Levantar los riesgos asociados a la operación del call center. Definir el apetito al riesgo con respecto a las nuevas actividades a ejecutarse. Definir los riesgos asociados al trabajo en las nuevas condiciones. | 1/12/2021 | 30/12/2021 |
| SGSI-6-1-b | Definir un plan de seguimiento y mejora de tratamiento de riesgos. | Mejora Continua | Análisis SGSI | Al identificarse el listado de riesgos, se debe definir como se hará seguimiento a la gestión de riesgos y se definirá como generar mejora continua en esta gestión de riesgos. | Se debe definir planes de tratamiento de riesgos. Se debe definir planes de medición de la gestión de riesgos. Se deben definir un cronograma de revisión de las métricas. Se deben definir planes de mejora en base a las métricas detectadas. | 1/1/2022 | 28/2/2022 |
| SGSI-6-1-c | Definir una política de manejo de documentación sobre los riesgos que se consideraron para el SGSI. | Cumplimiento Norma | Análisis SGSI | Definir como se realizará el manejo de la documentación referente a la gestión del riesgo, su tratamiento y la medición de sus metricas, asi como la documentación de las oportunidades de mejora continua. | Se debe definir los formatos para documentar los riesgos, los planes de tratamiento de riesgos. Se debe definir los formatos sobre los informes de medición de los riesgos. Se debe definir el formato de la documentación de las oportnuidades de mejora o cambios sobre los riesgos. | 1/1/2022 | 28/2/2022 |
| SGSI-6-1-d | Reforzar la definición de los controles necesarios dentro de la empresa y apegar los controles al anexo A. | Refuerzo | Análisis SGSI | Actualizar la definición de las políticas del Anexo A para ajustarlos con las nuevas definiciones de la empresa en cuanto a sus actividades. | Realizar un levantamiento de los controles definidos dentro de la empresa. Evaluar si los controles cumplemn con los objetivos de la empresa. Definir nuevos controles en caso de no tener controles implementados. Tomar en consideración la actualización de la declaración de aplicabilidad. | 1/4/2022 | 1/6/2022 |
| SGSI-6-1-e | Reforzar la declaración de aplicabilidad conforme a las nuevas responsabilidades de la empresa. | Refuerzo | Análisis SGSI | Actualizar la política de aplicabilidad sobre los controles del Anexo A que se utilizarán para la evaluación de la empresa en base a sus objetivos y actividades. | Actualizar la política de aplicabilidad considerando las nuevas actividades de la empresa. | 1/4/2022 | 1/6/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-6-2-a | Definir nuevos objetivos de seguridad que se encuentren acordes a las políticas de seguridad de la información. | Refuerzo | Análisis SGSI | Actualizar la definición de los objetivos de seguridad en base a las nuevas actividades de la empresa e incluir nuevos objetivos de seguridad. | Evaluar los objetivos de seguridad que se deben obtener con las nuevas actividades de la empresa. Definir las métricas para evaluar el avance del cumplimiento de los nuevos objetivos de seguridad. | 1/12/2021 | 30/12/2021 |
| SGSI-6-2-b | Actualizar la planificación existente incluyendo las acciones necesarias para alcanzar los objetivos de seguridad de la información. | Refuerzo | Análisis SGSI | Actualizar la planificación sobre las actividades, evaluaciones y seguimiento existente. | Con los nuevos objetivos de seguridad definidos, se debe ajustar las actividades, políticas, procesos necesarios para cumplir con estas nuevos objetivos y se debe definir una estimación de tiempo para dichas actividades. | 1/12/2021 | 30/12/2021 |
| SGSI-7-1-a | Reforzar y Actualizar los recursos necesarios para cumplir con el nuevo SGSI. | Prevención | Análisis SGSI | Definir que recursos adicionales se necesitan para cumplor con los nuevos objetivos de seguridad. | Definir los recursos en equipamiento IT necesario para el cumplimiento de objetivos. Definir los esquemas de funcionamiento de los componentes IT: | 1/1/2022 | 28/2/2022 |
| SGSI-7-2-a | Definir un plan de asignación de responsabilidades referente a la participación en las actividades del SGSI | Prevención | Análisis SGSI | Definir un plan de asignación de actividades y sus responsables, tomando en cuenta las actividades definidas para el SGSI. | Definir el personal técnico que estará a cargo de la gestión de los equipos IT. Definir los responsables del seguimiento, ajuste de configuraciones en los activos de IT. Definir responsables para la medición del alcance de los objetivos de seguridad de la información. | 1/1/2022 | 28/2/2022 |
| SGSI-7-3-a | Definir un plan de concienciación sobre las políticas y los objetivos de seguridad de la información, así como sus beneficios y las implicaciones de no cumplir con los objetivos. | Prevención | Análisis SGSI | Definir un plan de concienciamiento dentro de la organización sobre la importancia de la seguridad de la información, el SGSI y sus políticas y las mediciones que se realizarán para el SGSI. | Definir el contenido de la concienciaciión. Definir el número de sesiones necesarias para la concienciamiento. Definir los responsables y el auditorio de las charlas. Definir acciones adicionales para fomentar la concienciación como envio de emails sobre consejos de seguridad. | 1/4/2022 | 1/6/2022 |
| SGSI-7-4-a | Elaborar un esquema de comunicación que incluya que se debe comunicar, cuando comunicar, a quien comunicar, quien debe comunicar y que procesos se deben utilizar para comunicar. | Cumplimiento Norma | Análisis SGSI | Se debe definir un esquema para el manejo de las comunicaciones que involucre la generación de un proceso de comunicación. | Se debe definir los responsables de hacer las comunicaciones. Se debe definir el formato de las comunicaciones. Se debe definir el proceso de comunicación. Se debe definir los responsables de la elaboración y aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-7-5-a | Definir un listado de documentación necesaria para medir la eficacia del SGSI. | Cumplimiento Norma | Análisis SGSI | Definir un listado de los documentos/informes necesarios que incluyan métricas y que ayuden a realizar la medición de las actividades del SGSI. | Definir los informes necesarios para medir el cumplimiento y desempeño del SGSI. Definir el calendario de entrega de los informes para consolidación. Definir un cronograma para entregar la consolidación. | 1/7/2022 | 1/9/2022 |
| SGSI-7-5-b | Definir un reglamento sobre el formato de la documentación y los requisitos minimos que esta documentación debe tener. | Cumplimiento Norma | Análisis SGSI | Definir las acaracteristicas respecto a la documentación y su contenido, y que esta documentación cumpla requisitos mínimos para el uso en le SGSI. | Definir un listado de campos que llos formatos deben tener. Definir un reglamento sobre el contenido de la documentación, así como su actualización. Reforzar el proceso de aprobación manteniendo la revisión de idoneidad y adecuación. | 1/7/2022 | 1/9/2022 |
| SGSI-7-5-c | Definir un plan de protección de la documentación que incluya acciones en caso de perdida de confidencialidad, el uso inadecuado y la perdida de integridad. | Implementación | Análisis SGSI | Definir un plan para proteger la documentación del SGSI y definir acciones en caso de que se pierda la confidencialidad, la integridad y el uso inadecuado. | Definir esquemas para proteger la documentación . Definir escenarios para determinar acciones para el uso indebido, perdida de confidencialidad y perdida de integridad. Documentar estos planes. | 1/7/2022 | 1/9/2022 |
| SGSI-9-2-a | Definir un plan de auditoria para el SGSI, sus politicas y sus resultados | Implementación | Análisis SGSI | Definir los lineamientos sobre las auditorias internas y externas, asi como el tratamiento a las observaciones y no conformidades en el SGSI y las políticas de seguridad de la información. | Definir un cronograma para las auditorias internas, auditorias externas. Definir un plan de acción respecto a los resultados de la auditoria, así como el tratamiento de las no conformidades, las acciones correctivas del SGSI y de las políticas de seguridad de la información. | 1/4/2022 | 1/6/2022 |
| SGSI-A1-A5-1-1 | Actualizar el documento de la política de seguridad de la información. | Refuerzo | Análisis SGSI - Anexo A | Actualizar las politicas de seguridad de la información considerando la definición actualizada de los objetivos de seguridad de la información. | Obtener los nuevos objetivos de seguridad de la información. Actualizar las políticas de seguridad de la información para que estas ayuden al cumplimiento de los objetivos de seguridad de la información. Definir nuevas métricas para las políticas de seguridad de la información. | 1/1/2022 | 28/2/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A6-1-1 | Generar un plan de asignación interna respecto a la definición, seguimiento y mantenimiento de las políticas de seguridad de la información. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir la asignación de un responsable que coordine y supervise las actividades referente a las políticas de seguridad de la información y al seguimiento de las mismas. Definir el rol de Oficial de seguridad de la información y sus funciones. | Definir un coordinador de seguridad de la información. Definir las funciones del cargo de coordinador de seguridad de la información. | 1/1/2022 | 28/2/2022 |
| SGSI-A1-A6-1-2 | Definir una política de procesamiento de información que incluya autorizaciones. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir un proceso para autorizar cambios en las políticas de seguridad de la información, asi como cualquier cambio en IT que afecte a la seguridad de la información. | Definir un formato de autorizaciones para cambios que afecten a la sefuridad de la información. Definir un responsable para autorizar los cambios que afecten a las políticas de seguridad de la información o sus métricas. | 1/1/2022 | 28/2/2022 |
| SGSI-A1-A6-1-3 | Reforzar la documentación sobre los acuerdos de confidencialidad con clientes y proveedores. | Refuerzo | Análisis SGSI - Anexo A | Actualizar la documentación sobre los acuerdos de confidencialidad que se manejan con los clientes y proveedores. | Definir una bitácora o historial de los acuerdos de confindencialidad que se manejan con los clientes y proveedores. Actualizar los acuerdos de confidencialidad para que se ajusten a las nuevas necesidades de la empresa y a la ley vigente. | 1/1/2022 | 28/2/2022 |
| SGSI-A1-A6-1-4 | Definir una política de contacto con las autoridades para los temas de seguridad de la empresa. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir un cronograma de reuniones internas entre los encargados de seguridad de la información y las gerencias de la empresa. | Definir un cronograma para las revisiones de las gerencias respecto a la revisión de los avances de seguridad de la información. Definir un proceso de documentación de resumen de los temas tratados dentro de las reuniones. | 1/1/2022 | 28/2/2022 |
| SGSI-A1-A6-1-5 | Definir una política de contacto con grupos de interés especiales en los temas de seguridad de la información. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir los lineamientos para establecer contactos con grupos de interes especiales y generar un entendimiento común sobre seguridad de la infromación. | Definir un calendario para reuniones con los grupos de inyteres especiales. Definir un formato para documentar los temas tratados con los grupos de interes especiales. | 1/4/2022 | 1/6/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A6-2-1 | Definir un análisis de riesgos referente al trato con partes externas, clientes, proveedores y terceras partes. | Prevención | Análisis SGSI - Anexo A | Definir los riesgos para la empresa respecto al trato con partes externas, proveedores y terceras partes y que afecten a la seguridad de la información. | Definir los riesgos asociados a la interacción de la empresa con terceros. Definir las acciones referentes a la gestión de riesgos con terceros. Definir planes de acción para el tratamiento del riesgo. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A7-1-1 | Generar una política de contratación en donde se documenten los roles y responsabilidades de los cargos de la empresa, así como los perfiles de acceso a la información en base a ese cargo. | Implementación | Análisis SGSI - Anexo A | Definir una política de contratación en donde se definan los roles y responsabilidades de los empleados, asi como el nivel de acceso a la información de la empresa. | Definir una politica de acceso a la información basado en los cargos de la empresa. Incluir los requerimientos sobre conocimiento de seguridad de la información. Definir las responsabilidades frente a sus superiores sobre el manejo de la información. Definir un código disciplinario. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A8-1-1 | Actualizar el inventario tecnológico. | Refuerzo | Análisis SGSI - Anexo A | Actualizar el inventario tecnológico e incluir la fecha de adquisición de ese activo tecnológico. Definir el registro de los prestamos y devoluciones de los activos tecnológicos. | Definir una matriz de los activos tecnológicos que incluyan la fecha de adquisición. Definir los responsables de los activos de información que se hayna asignado. Definir formatos para asignación de activos. Definir formatos para devolución de activos. Definir bitácoras para registrar las devoluciones y prestamos. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A8-1-2 | Definir una política de uso aceptable de los activos tecnológicos de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir las consideraciones que se deben tener al utilizar equipos de IT provistos por la empresa. | Definir las condiciones de uso y los propositos de uso del equipamiento existente en la empresa. Automatizar en lo posible los controles que ayuden a que se cumplan con los lineamientos definidos de uso aceptable. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A8-2-1 | Documentar la directriz de clasificación de información existente y ampliarla a las demás áreas de la empresa. | Prevención | Análisis SGSI - Anexo A | Documentar la directriz de clasificación de información existente y ampliarla a las demás áreas de la empresa. Asi mismo definir esquemas de etiques para clasificar la información. | Actualizar la directriz de clasificación de información. Incluir las actividades de etiquetado de la información en base a categorías. Documentar los permisos de acceso de los usuarios en base a las directriz definida. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A8-2-2 | Extender la política de gestión medios extraíbles y soportes de almacenamiento a toda la organización en base a las necesidades de la empresa. | Refuerzo | Análisis SGSI - Anexo A | Extender la gestión de medios extraíbles y soportes de almacenamiento a toda la organización en base a las necesidades de la empresa. | Actualizar la política de gestión de medios extraibles y soportes de información para abarcar a toda la empresa. Definir procedimientos para limpiar y reutilizar medios extraibles. Definir procesos de limpieza de soportes de almacenamiento de información. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A9-1-1 | Se debe definir una política de control de acceso a recursos utilizando usuarios temporales y autenticacion temporal. | Prevención | Análisis SGSI - Anexo A | Definir una política de generación de usuarios temporales para acceder a los recursos de la empresa. | Definir procesos de compartición de documentos digitales, la duración del permiso, definir el tipo de información que se puede transmitir de esta forma. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A9-2-1 | Generar una política de gestion de usuarios y contraseñas. | Prevención | Análisis SGSI - Anexo A | Generar una política de gestion de usuarios y contraseñas en donde se señalen los lineamientos de seguridad de los usuarios y contraseñas. | Definir como se definiran los nombres de usuario dentro de la organización. Definir los esquemas de las contraseñas. Definir la periodicidad del cambio de contraseñas. | 1/4/2022 | 1/6/2022 |
| SGSI-A1-A9-3-1 | Definir una política de uso de esquemas de autenticación mas robustas como uso de biométrica o doble factor de autenticación. | Refuerzo | Análisis SGSI - Anexo A | Definir esquemas de autenticación mas robustos para el acceso a recursos que conlleven un mayor nivel de sensibilidad. | Definir que esquemas de autenticación adicionales se implementarán para el acceso a información clasificada como sensible o crítica. Definir que sistemas tendrán esta configuración. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A9-4-1 | Definir una política de restricción de acceso a sistemas y aplicaciones basada en permisos y usuarios. | Refuerzo | Análisis SGSI - Anexo A | Definir las consideraciones para que determinados usuarios puedan utilizar herramientas de la empresa, asi como delimitar el acceso a la información. | Definir el listado de usuarios existentes. Definir los permisos de los usuarios hacia las aplicaciones. Definir los permisos de los usuarios para el acceso a los recursos de la empresa. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A9-4-2 | Definir una política de uso de software y permisos de sistema operativo dependiendo de los usuarios. | Implementación | Análisis SGSI - Anexo A | Definir los permisos que cada usuario del sistema operativo puede ejecutar sobre el mismo. | Definir el formato y permisos de los usuarios del sistema operativo. Definir los perfiles de acceso que se asignara a cada persona de la empresa. Definir los roles que tendrán permiso de instalación de software en sus máquinas. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A9-4-3 | Definir una política de protección de acceso al repositorio de código fuente de los programas entregados. | Implementación | Análisis SGSI - Anexo A | Definir los permisos necesarios para los usuarios que acceden a los repositorios de código fuente en la empresa. | Definir medidas de control de acceso lógico al repositorio de codigo fuente basado en usuarios, contraseñas y permisos. Definir medidas de protección y respaldo del repositorio de códgo fuente. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A10-1-1 | Crear una nueva política de gestión de claves en donde se incluyan las prácticas de seguridad ya existentes y nuevas consideraciones de seguridad. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos sobre las contraseñas que se configurarán dentro de los equipos de IT de la organización y su gestión. | Definir un esquema de definición de contraseñas. Definir el listado de los equipos que utilizaran esta definición de contraseñas. Definir la periodicidad de las contraseñas. Definir un cronograma de actualización de contraseñas. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A11-1-1 | Definir una política de acceso, seguridad física de la oficina y sus diferentes áreas para colaboradores y proveedores. | Implementación | Análisis SGSI - Anexo A | Definir las consideraciones sobre seguridad física a las áreas sensibles de la emptresa en cuanto a seguridad de la información. | Reconocer las áreas sensibles en la empresa en cuanto a acceso a fuentes de información. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A11-2-1 | Incluir en la política de acceso, seguridad física de la oficina las protecciones que deben tener considerados los equipos informáticos y de IT. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos adicionales respecto a la consideración del aseguramiento de las áreas en donde funcionan o se almacenan equipos IT. | Definir los controles necesarios para asegurar las áreas en donde se almacene o procese información sensible de la empresa y que sean equipos de IT. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A11-2-2 | Definir un plan de mantenimiento y mejora respecto a la instalación de suministro y sus contingencias como el UPS. | Mejora Continua | Análisis SGSI - Anexo A | Definir las condiciones que se deben tener en cuenta para mantener funcional y operativo el suministro de energía electrica y sus medidas de contingencia. | Definir las condiciones de funcionamiento de los equipos IT de la empresa en cuanto a temas de energía. Definir un cronograma de mantenimiento de las contingencias de interrupción del suministro de energía electrica. Definir los niveles de funcionamiento adecuados del UPS. | 1/7/2022 | 1/9/2022 |
| SGSI-A1-A11-2-3 | Definir un plan de actualización, mantenimiento del cableado estructurado y organización en los rack del data center. | Mejora Continua | Análisis SGSI - Anexo A | Definir las condiciones que se deben tener en cuenta para mantener funcional y operativo la conectividad de la empresa y sus medidas de contingencia. | Definir las condiciones de funcionamiento del cableado estructurado. Definir la edad máxima del cableado de seguridad. Definir un plan de actualización y mantenimiento del cableado estructurado. Definir un esquema de peinado de los cables de energía y de red que se utilizan en el data center. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A11-2-4 | Definir un plan de mantenimiento, actualización y reasignación de equipos y medios; | Mejora Continua | Análisis SGSI - Anexo A | Definir los lineamientos para generar reasignación de equipos y componentes asignados al personal de la empresa. Definir una política para el mantenimiento de pólizas de los equipos. | Definir periodos de vida util de los equipos adquiridos. Definir esquemas de revisión y generación de informes del estado de los equipos. Definir su asignación dentro y fuera de la empresa e incluir garantias o seguros. | 1/5/2022 | 1/7/2022 |
| SGSI-A1-A11-2-5 | Actualizar y reforzar la política de reutilización de medios e incluir procedimientos para la retirada segura de dispositivos de almacenamiento. | Refuerzo | Análisis SGSI - Anexo A | Definir los lineamientos para la reutilización de medios de almacenamiento dentro y fuera de la empresa, asi como su reutilización. | Definir procesos para extraer medios de lamacenamiento de forma segura de componentes que cumplieron su vida util y se pueda reutilizar | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A11-2-6 | Definir una política para el manejo de equipos informáticos de usuarios desatendidos . | Prevención | Análisis SGSI - Anexo A | Definir una política para el manejo de equipos informáticos de usuarios desatendidos y adicionar una política de puesto de trabajo despejado y bloqueo de pantalla de forma automática. | Definir las condiciones que deben cumplirse para manejar equipos con usuarios desatendidos. Definir políticas de bloqueo de pantallas. Definir acciones cuando un colaborador va a dejar su puesto de trabajo momentaneamente. | 1/5/2022 | 1/7/2022 |
| SGSI-A1-A12-1-1 | Definir una política de documentación de la operación tales como apagado/encendido de equipos. Gestion de cambios y Gestión de capacidades | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir una política que defina los lineamientos de la operación de la empresa tales como apagado/encendido de equipos, la gestión de cambios en los equipos y la gestión de capacidades de los equipos. | Definir la planificación para el pagado, encendido de los equipos. Definir un plan para gestionar controles de cambio sobre los equipos que funcionan en el data center. Definir un esquema de monitoreo de las capacidades de los componentes de IT que funcionan en el data center. Definir un formato de evaluación de capacidades de los componentes del data center. Definir un proceso de aumento de capacidades. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A12-2-1 | Actualizar la definición de la separación de los ambientes de desarrollo, prueba y producción con herramientas de automatización. | Refuerzo | Análisis SGSI - Anexo A | Definir un esquema de trabajo contando con al menos 3 entornos para el desarrollo interno y el desarrollo de los productos. | Definir los requisitos necesarios para incorporar los ambientes de desarrollo y pruebas para el desarrollo en general y el ambiente de producción par el desarrollo interno. Definir las librerias, herramientas, SDK, plugins necesarios para habilitar dichos ambientes, definir que usuarios pueden acceder a dichos ambientes. | 1/7/2022 | 1/9/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A12-3-1 | Establecer una política de copias de seguridad para los activos de mayor importancia. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos para generar copias de seguridad de la información y configuración de los equipos de mayor importancia. | Identificar los equipos de los cuales se obtendrán copias de seguridad. Definir un cronograma de obtención de copias de respaldo. Definir donde se almacenarán estas copias de respaldo. | 1/6/2022 | 1/7/2022 |
| SGSI-A1-A12-4-1 | Definir una política de tratamiento, almacenamiento y revisión de logs de los equipos IT de la empresa. Incluir la sincronocidad de tiempo en sus procedimientos. | Refuerzo | Análisis SGSI - Anexo A | Definir los lineamientos, planes de acción y periodicidad del almacenamiento de los logs para sus análisis. | Definir el sitio de almacenamiento de los logs. Definir el tiempo de retención de los logs. Definir la periodicidad de cuando se respladen los logs. Definir el responsable de estas actividades. | 1/1/2022 | 31/12/2022 |
| SGSI-A1-A12-5-1 | Reforzar y actualizar la política de adquisición de software para uso empresarial con el fin mantener el software empresarial lo mas estable posible y actualizado. | Prevención | Análisis SGSI - Anexo A | Definir lineamientos respecto al software empresarial, su actualización y estabilización. | Definir el listado del software que se ocupa por la empresa. Definir la periodicidad de las actualizaciones. Definir los procesos para realizar la actualización del software y las pruebas de estabilización. | 1/1/2022 | 31/3/2022 |
| SGSI-A1-A12-6-1 | Definir un plan de hardening semestral de los equipos informáticos que permitan parchar las vulnerabilidades. | Prevención | Análisis SGSI - Anexo A | Definir las actividades necesarias para evaluar vulnerabilidades en los componentes críticos así como la peridicidad de estos análisis. | Definir los métodos o herramientas para el análisis de vulnerabilidades. Definir un cronograma de análisis. Definir los planes de acción en base a las vulnerabilidades que se encuentren. | 15/7/2022 | 30/8/2022 |
| SGSI-A1-A13-1-1 | Definir una política de diseño, implementación y operación de una red redundante y con medidas de seguridad acorde a las necesidades de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir un plan de diseño de la red empresarial, parametrizar su implementación y operación. | Definir el estado actual de la red. Definir los componentes necesarios para alcanzar el diseño de la red. Definir los lineamientos de operación de la red y configuraciones de seguridad. | 1/10/2022 | 1/12/2022 |
| SGSI-A1-A13-2-1 | Definir una política de intercambio de información y mensajería electrónica. | Implementación | Análisis SGSI - Anexo A | Definir un esquema de intercambio de información y mensajería electrónica teniendo en cuenta la confidencialidad, integridad, disponibilidad y privacidad. | Definir los lineamientos del intercambio de seguridad, su alcance y las aclaraciones respecto a la seguridad de la información al compartir información por mensajería electrónica. Definir ajustes que señalen estos cambios en la mensajería electrónica. | 1/1/2022 | 31/3/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A14-1-1 | Definir una política de implementación de seguridad en servidores que alberguen sistemas de información. | Mejora Continua | Análisis SGSI - Anexo A | Delimitar las necesidades de seguridad de la información en los servidores de la empresa basado en los lineamientos de confidencialidad, integridad y disponibilidad. | Definir los servidores a ser intervenidos. Definir las herramientas necesarias para implementar seguridad de la información en los servidores. Definir métricas que ayuden a indetificar la eficiencia de las herramientas. | 1/1/2022 | 31/3/2022 |
| SGSI-A1-A14-2-1 | Definir una política de desarrollo seguro para la empresa basada en principios de ingenieria de sistemas seguros. | Prevención | Análisis SGSI - Anexo A | Definir las consideraciones necesarias para generar desarrollos seguros dentro de la empresa basados en ingenieria de desarrollo seguro. | Definir los marcos de referencia a utilizarse. Definir las medidas de seguridad al momento de desarrollar. Definir las herramientas de seguridad para los entornos de desarrollo. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A14-2-2 | Definir una política de control de cambios en los sistemas de la empresa que incluyan cambios en funcionalidad, en sus librerias, en su entorno de desarrollo o en paquetes de software. | Prevención | Análisis SGSI - Anexo A | Definir una política de control de cambios para los sistemas de la empresa que incluyan cambios de funcionalidad, en el uso de librerias o dependencias o software adicionales. | Definir horarios para los trabajos en la infraestructura. Definir el procedimiento de registro del control de cambios. Definir los formatos para aprobaciones de cambios. Definir el proceso de aprobación de cambios. | 1/7/2022 | 1/8/2022 |
| SGSI-A1-A14-2-3 | Definir una política de aseguramiento del entorno de desarrollo. | Prevención | Análisis SGSI - Anexo A | Definir procesos, uso de herramientas y formatos para volver a los entornos de desarrollos ambientes seguros de desarrollo de software. | Definir procesos para asegurar el acceso al entorno de desarrollo. Definir herramientas informáticas para reforzar el entorno de desarrollo. Identificar componentes del entorno de desarrollo que mejoren la seguridad del desarrollo. Definir los usuarios y permisos del entorno de desarrollo. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A14-2-4 | Definir un procedimiento para ejecutar pruebas funcionales de seguridad en los sistemas desarrollados. | Implementación | Análisis SGSI - Anexo A | Definir procesos, herramientas y responsables para ejecutar pruebas funcionales de seguridad en el software que se desarrolla en la empresa. | Definir un marco de referencia o buenas prácticas a seguir para ejecutar pruebas funcionales de seguridad. Definir las pruebas funcionales de seguridad que se ejecutarian como parte de las pruebas funcionales. Definir los resultados esperados de las pruebas funcionales. | 1/10/2022 | 30/12/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A14-2-5 | Definir una política de pruebas de aceptación basada en cumplimiento de requisitos y normas de seguridad. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos para establecer pruebas de aceptación que consideren requisitos y normas de seguridad. | Definir un marco de referencia o buenas prácticas para aplicarse sobre las pruebas de aceptación. Seleccionar las pruebas aplicables a los desarrollos. Definir los requisitos e seguridad que se evaluaran en las pruebas de aceptación. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A14-3-1 | Definir una política de tratamiento de datos de pruebas, su procesamiento y privacidad en caso de ser datos personales. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir los lineamientos y consideraciones para el manejo de los datos de prueba y la privacidad de los mismos en caso de ser datos personales. | Definir documentación de autorización de uso de datos de prueba. Definir el proceso de pruebas tomando en cuenta los datos observados.Definir el manejo de los datos luego de la fase de pruebas. | 1/12/2021 | 30/12/2021 |
| SGSI-A1-A15-2-1 | Definir una política de control de los servicios contratados con los proveedores en base a disponibilidad de servicio y cumplimiento del SLA. | Mejora Continua | Análisis SGSI - Anexo A | Definir los objetivos sobre los servicios contratados referente a su disponibilidad durante un mes, asi como los procesos y herramientas que se utilizarán para estas mediciones. | Listar los SLA de los proveedores que tienen productos o servicios contratados con la empresa. Definir métodos de evaluación del cumplimiento de los SLA. Definir los esquemas de escalamiento que ofrece cada proveedor. | 1/5/2022 | 1/7/2022 |
| SGSI-A1-A16-1-1 | Definir una política de gestión de incidentes de seguridad de la información que incluya procedimientos de analisis, recopilación y mejora continua. | Implementación | Análisis SGSI - Anexo A | Definir procesos para manejar los incidentes de seguridad que pudiera manejar la empresa, estos procesos deben incluir procedimientos de análisis, recopilación, documentación y mejora continua. | Definir procesos para tratar incidentes de seguridad y activar esquemas de contingencia definidos. Definir un plan de comunicación a los clientes/proveedores afectados.Definir acciones de remediación para los incidentes detectados. | 1/1/2022 | 28/2/2022 |
| SGSI-A1-A17-1-1 | Definir un plan de continuidad de la seguridad de la información, sus controles, su revisión, ajuste y mejora continua. | Refuerzo | Análisis SGSI - Anexo A | Definir la continuidad de la seguridad de la información como parte de los esquemas de continuidad, identificar adicionalmente esquemas de revisión ajuste y mejora continua. | Definir los mecanismos de continuidad respecto a la seguridad que se implementarán en la empresa. Definir procesos de revisión de los procesos de continuidad. Definir las métricas sobre las medidas de continuidad. Definir planes de mejora en base de la evaluación de métricas. | 3/1/2022 | 28/2/2022 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SGSI-A1-A17-2-1 | Definir un proyecto para reforzar y mejorar los esquemas existentes en los componentes que se consideren como críticos. | Prevención | Análisis SGSI - Anexo A | Definir las necesidad de redundancia y alta disponibilidad para componentes de IT críticos, así como definir el tiempo que las adquisiciones se mantengan operativas en la empresa. | Definir la vida útil de los componentes IT. Definir la reutilización de los componentes IT si aplica. Definir un roadmap de adquisiciones como parte de las renovaciones de IT. | 3/1/2022 | 28/2/2022 |
| SGSI-A1-A18-1-1 | Realizar una auditoria externa para identificar puntos de mejora respecto al cumplimiento legal y requisitos contractuales. | Prevención | Análisis SGSI - Anexo A | Definir los objetivos que se persiguen con la auditoria externa respecto a la conformación de la empresa, el cumplimiento legal y los requisitos contractuales. | Definir el alcance de la auditoria. Definir que lineamientos de cumplimiento legal se buscan evaluar. Definir que areas de cumplimiento se van a evaluar. Seleccionar un proveedor de servicios de auditoria | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A18-1-2 | Definir una política para registro de derechos de propiedad intelectual en el caso de los desarrollos que se manejan dentro de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir los procesos para identificar y registrar los desarrollos que se hacen dentro de la empresa como propiedad intelectual. | Incluir en los procesos de venta de productos y servicios la sección de "Porpiedad Intelectual". Definir una bitácora de desarrollos efectuados por la empresa. Definir un proceso de registro de los desarrollos como parte de la propiedad intelectual de la empresa. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A18-1-3 | Definir una política de protección de los registros de la organización y reforzar las medidas de seguridad de estos registros. | Implementación | Análisis SGSI - Anexo A | Definir procesos para proteger los registros importantes de la empresa e identificar las medidas de seguridad que sean aplicables a la empresa. | Clasificar la información que maneja la empresa. Definir en que partes de la empresa se almacena esta información. Definir procesos para asegurar el acceso a la información y a los registros. | 1/10/2022 | 30/12/2022 |
| SGSI-A1-A18-1-4 | Definir una política de protección y privacidad de la información de carácter personal. | Implementación | Análisis SGSI - Anexo A | Definir los pasos necesarios para proteger los documentos o procesos empresariales que manejen información de carácter personal, asi como las medidas de protección de esta información. | Clasificar la información que maneja la empresa y los tipos de información en base a la privacidad. Definir procesos que permitan asegurar la privacidad en el manejo de la información.Definir procesos de manejo de información personal que contenga autorizaciones por parte de los encargados de procesar esa información o de los dueños de esa información. | 3/1/2022 | 28/2/2022 |

# ANEXO 3

# INFORME SOBRE LA EVALUACIÓN DEL SGSI

## Entregable 3 – Informe del Estado Actual del SGSI

### Introducción

El presente documento tiene como objetivo presentar un breve resumen del estado actual del SGSI y evaluar su madurez con base al análisis de la documentación existente en la empresa y ayudado por marcos de referencia de seguridad.

### Metodología de Trabajo

Para el proceso de evaluación del SGSI actual se ha contemplado utilizar las ISO 27001 y 27002 con el fin de evaluar el cumplimiento de sus ítems conforme a la calificación de la siguiente tabla:

| Valor | Efectividad | Significado | Descripción |
|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. |

*Tabla 1. Escala de medición utilizada para evaluar los ítems descritos en las secciones de la ISO 27001*

Esta evaluación se tomará en cuenta con la documentación presentada y revisión en conjunto. El resumen de cada unidad se presentará en este documento como un resumen de la “Evaluación de Madurez del ISO 27001 y 27002”

### Medición de la sección 4 – Contexto de la organización

Los ítems descritos en el marco de referencia del ISO 27001 con respecto a la sección 4 menciona como un SGSI interactúa con la organización, así como el análisis del alcance del SGSI.

La sección 4 hace referencia al entendimiento por parte de la organización de los problemas internos y externos que puedan afectar al alcance de los objetivos del SGSI.

En la figura 1 muestra el resultado de la medición de los ítems señalados en esta sección.

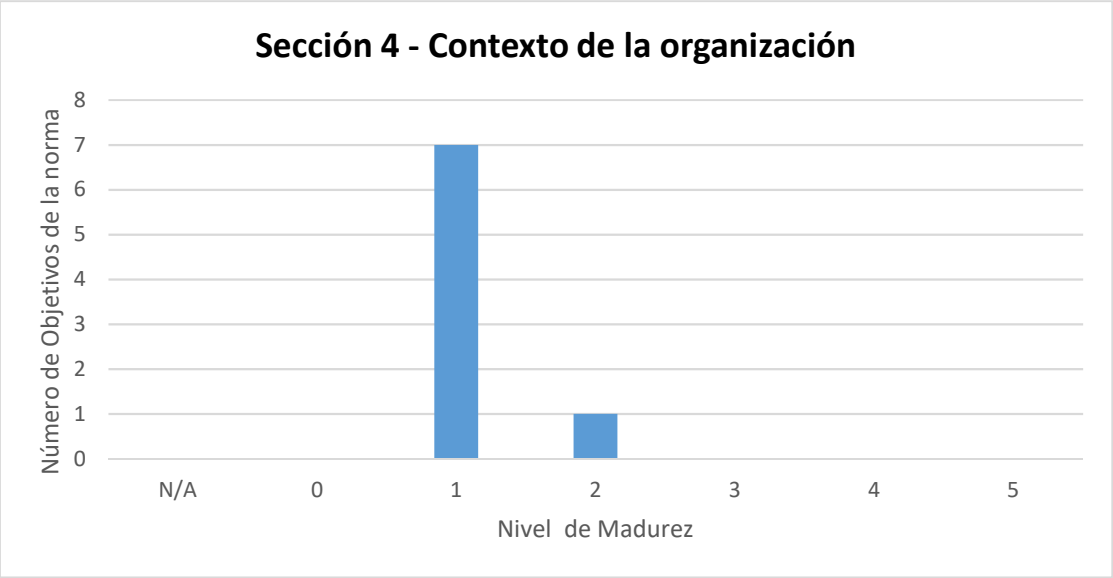



*Figura 1. Análisis de madurez de los ítems descritos en la sección 4 del ISO 27001*

Como se puede ver en la gráfica en mención, de los 8 ítems evaluados en esta sección 7 de estos ítems se encuentran en un nivel de madurez 1, mientras que existe uno solo con nivel de madurez 2.

La tendencia en esta sección es 1, por lo que se puede concluir que el contexto de la organización referente a la ISO 27001 se muestra con procedimientos inexistentes, sin una estructura repetible y basada en el esfuerzo personal.

**Medición de la sección 5 – Liderazgo**

La sección 5 hace referencia al liderazgo y compromiso de las autoridades con el cumplimiento de los objetivos y políticas establecidos en el SGSI. En la figura 2 se puede observar el resultado de la medición de los ítems señalados en esta sección.

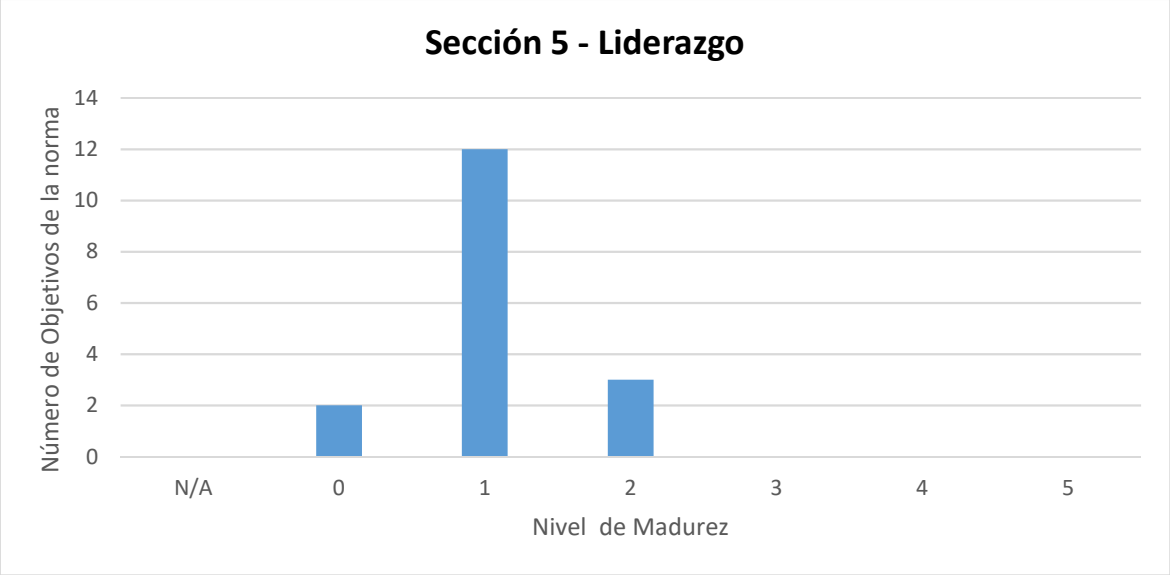



*Figura 2. Análisis de madurez de los ítems descritos en la sección 5 del ISO 27001*

Como se puede ver en la gráfica anterior, de los 17 ítems evaluados en esta sección 2 de esos ítems se encuentran con un nivel 0, es decir inexistente; 12 de estos ítems se

encuentran en un nivel de madurez 1, mientras que existen 3 con un nivel de madurez 2.

La tendencia en esta sección es 1, por lo que se puede concluir que el contexto del liderazgo de la organización referente a la ISO 27001 se muestra con procedimientos inexistentes, sin una estructura repetible y basada en el esfuerzo personal.

**Medición de la sección 6 – Liderazgo**

La sección 6 hace referencia a la planificación de actividades y recursos para alcanzar el cumplimiento de los objetivos establecidos, así como también evalúa el manejo de los riesgos dentro del SGSI. En la figura 3 se puede observar el resultado de la medición de los ítems señalados en esta sección.

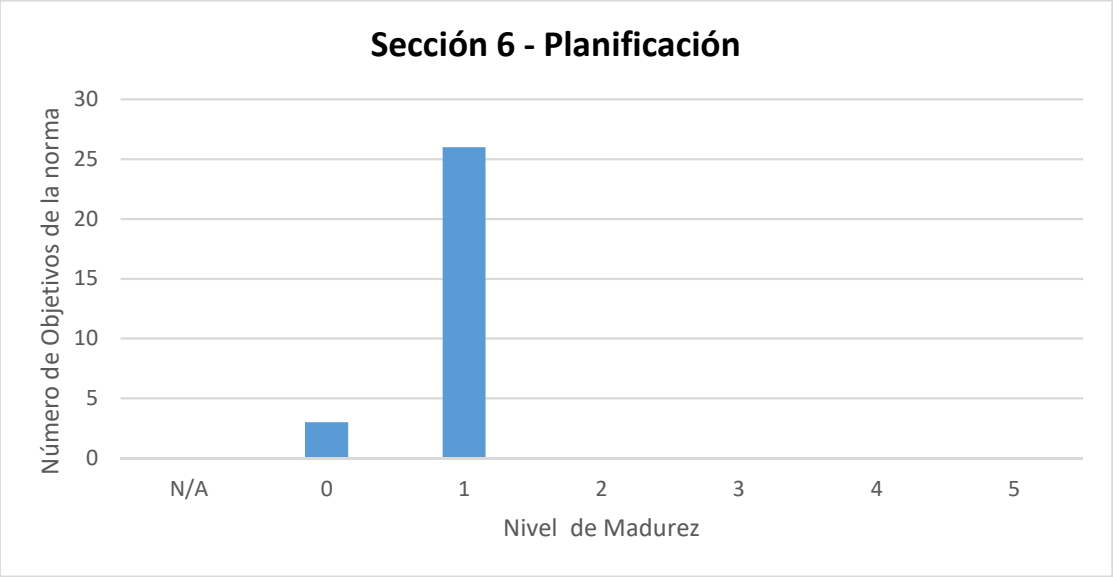



*Figura 3. Análisis de madurez de los ítems descritos en la sección 6 del ISO 27001*

Como se puede ver en la gráfica anterior, de los 29 ítems evaluados en esta sección 2 de esos ítems se encuentran con un nivel 0, es decir inexistente; los otros 27 ítems se encuentran en un nivel de madurez 1.

La tendencia en esta sección es 1, por lo que se puede concluir que el contexto del liderazgo de la organización referente a la ISO 27001 se muestra con procedimientos inexistentes, sin una estructura repetible y basada en el esfuerzo personal.

**Medición de la sección 7 – Soporte**

La sección 7 hace referencia al soporte que la organización brinda para llevar a cabo las actividades dentro del SGSI, entiéndase soporte a la provisión de recursos tales como presupuestos, recursos humanos, comunicación, así como la documentación. En la figura 4 se puede observar el resultado de la medición de los ítems señalados en esta sección.

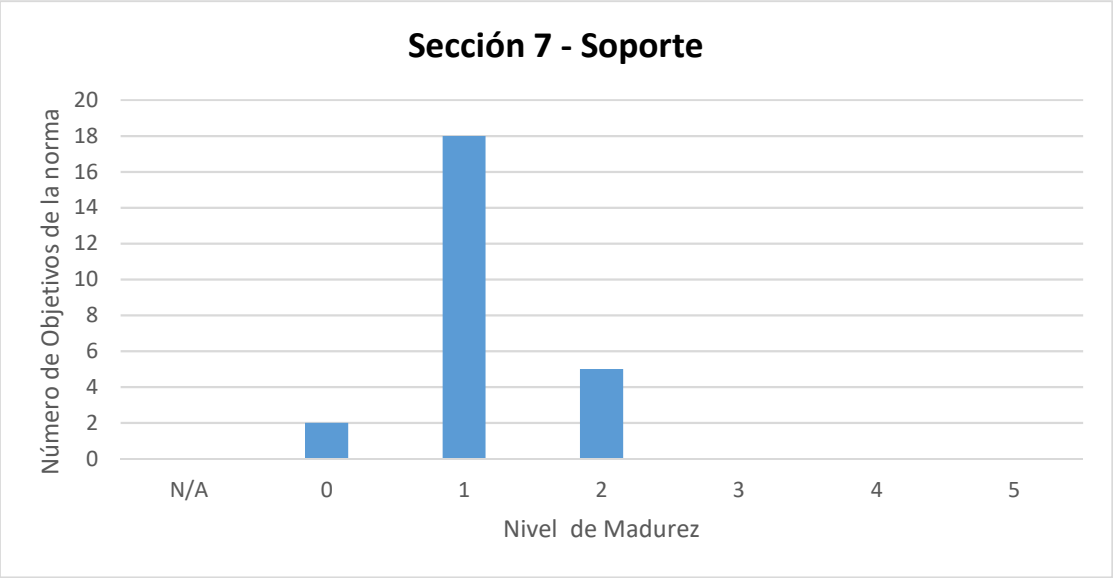



*Figura 4. Análisis de madurez de los ítems descritos en la sección 7 del ISO 27001*

Como se puede ver en la gráfica anterior, de los 25 ítems evaluados en esta sección 2 de esos ítems se encuentran con un nivel 0, es decir inexistente; 18 de estos ítems se encuentran en un nivel de madurez 1 y solo 5 cuentan con un nivel 2 de madurez.

De igual manera en esta sección el valor predominante de madurez es el 1, por lo que se puede concluir que el contexto de Recursos referente a la ISO 27001 se muestra con procedimientos inexistentes, sin una estructura repetible y basada en el esfuerzo personal.

**Medición de la sección 8 – Operación**

La sección 8 hace referencia a las consideraciones de la operación, su planificación y hace una revisión rápida de los temas de apreciación y tratamiento de riesgos. En la figura 5 se puede observar el resultado de la medición de los ítems señalados en esta sección.

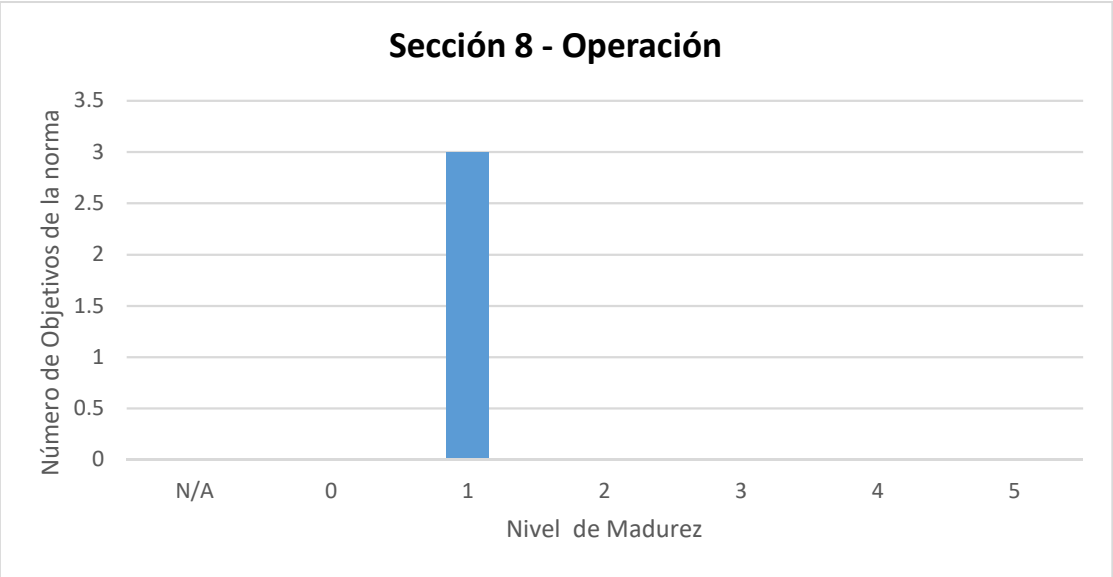



*Figura 5. Análisis de madurez de los ítems descritos en la sección 8 del ISO 27001*

En esta sección existen 3 ítems a evaluarse y en todos se asignó la calificación del nivel de madurez en 1. Siendo esta sección acreedora al nivel de madurez es el 1, puede concluir que el contexto de Operación referente a la ISO 27001 se muestra con procedimientos inexistentes, sin una estructura repetible y basada en el esfuerzo personal.

**Medición de la sección 9 – Evaluación del Desempeño**

La sección Evaluación del desempeño hace referencia a como la organización da seguimiento, monitorea, mide, analiza, audita internamente y la revisión de estos resultados por las autoridades de la organización. La figura 6 se puede observar el resultado de la medición de los ítems señalados en esta sección.

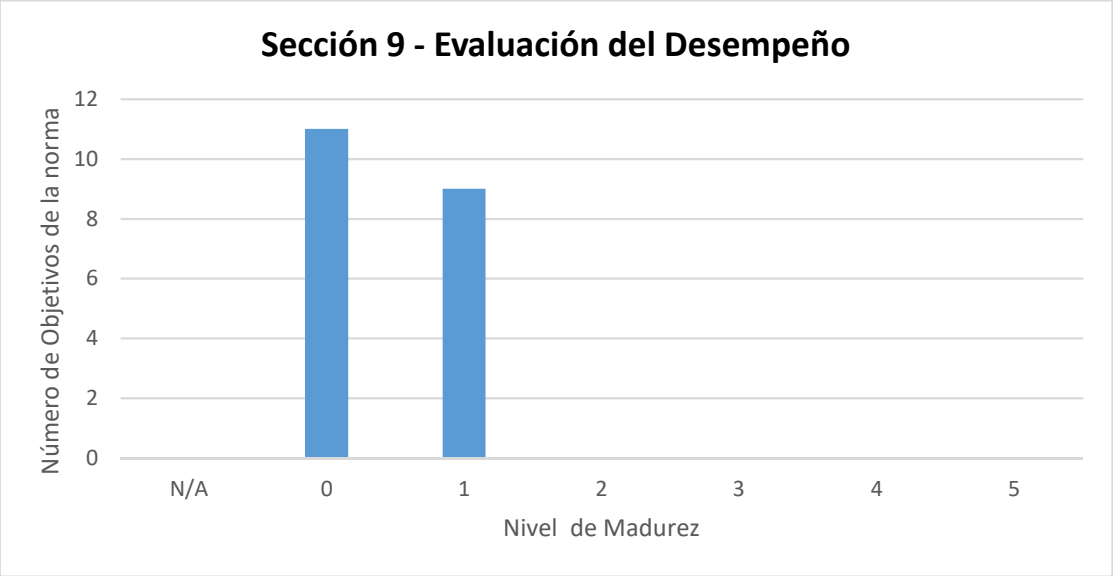



*Figura 6. Análisis de madurez de los ítems descritos en la sección 9 del ISO 27001*

En esta sección existen 20 ítems a evaluarse, de este número 11 ítems tienen una calificación de 0, que es decir inexistente y existen 9 ítems que tienen una calificación de madurez igual a 1. En este caso hay un número mayor de ítems con nivel de madurez 0, por lo que en esta sección se puede concluir que estos procesos son inexistentes y que están encaminados a levantarse posteriormente.

**Medición de la sección 10 – Mejora**

La última sección que se especifica en la norma ISO 27001 hace referencia a como la organización busca la mejora de su SGSI en base a las revisiones internas, y la colaboración de las otras secciones. Esta sección involucra mucho la auditoria externa y el tratamiento que se hace a las observaciones de estas auditorías. La figura 7 se puede observar el resultado de la medición de los ítems señalados en esta sección.

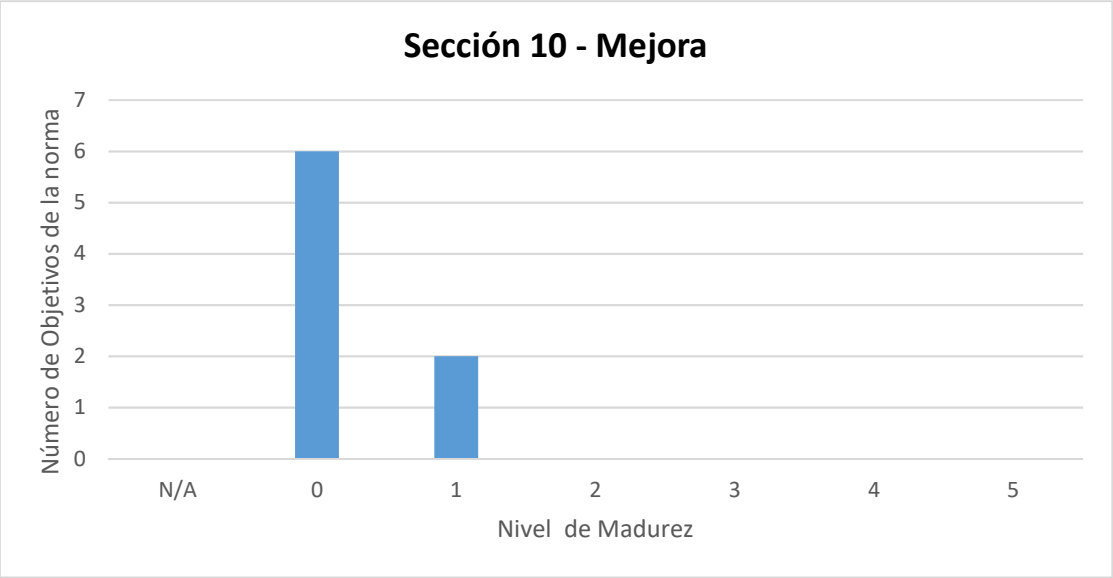



*Figura 7. Análisis de madurez de los ítems descritos en la sección 10 del ISO 27001*

En esta sección existen 8 ítems a evaluarse, de este número 6 ítems tienen una calificación de 0, que es decir inexistente y existen únicamente 2 ítems que tienen una calificación de madurez igual a 1. En este caso hay un número mayor de ítems con nivel de madurez 0, por lo que en esta sección se puede concluir que estos procesos son inexistentes y que están encaminados a levantarse posteriormente.

**Evaluación de la ISO 27001 en general**

Respecto a la evaluación de ítems en basados en el marco de referencia ISO 27001, se ha podido obtener los datos de la tabla 2 que muestran el número de ítems que fueron evaluados con las escalas de madurez previstas al inicio del documento.

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 0 |
| 0 | 0% | Inexistente | Inexistencia de cualquier proceso conocido. | 24 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos poco definidos o localizados en áreas concretas. Actividades no muy organizadas. | 77 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Se depende del conocimiento y experiencia individual. | 9 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir las actividades de los procesos mediante indicadores numéricos y estadísticos. Existen herramientas para mejorar el desempeño y calidad de los procesos. | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. Con base a criterios cuantitativos se determinan los ajustes a realizarse y se optimizan los procesos. | 0 |

*Tabla 2. Nivel de madurez medido en los ítems del marco de referencia ISO 27001*

Respecto a esta distribución la figura 8 se puede apreciar la distribución de los niveles de madurez versus el número de ítems evaluados dentro de ISO27001.

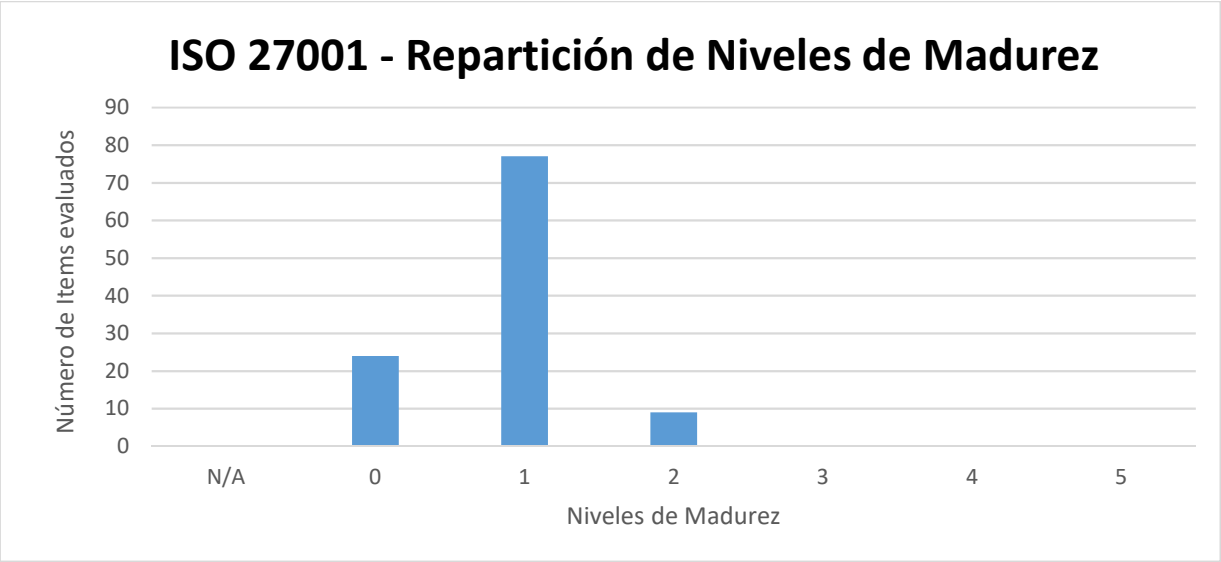



*Figura 8. Repartición de los Niveles de Madurez calificados en conjunto con en el marco de referencia ISO 27001*

La distribución muestra que existe una tendencia marcada a que los elementos analizados por ISO 27001 están en su mayoría en un nivel de madurez 1, seguidos por los ítems con niveles de madurez de 0 y finalmente unos pocos ítems con nivel de madurez 2. Cabe mencionarse que no existen políticas calificadas con un nivel de madurez 3 o superior.

Ahora, para poder determinar qué áreas o secciones son las que necesitan un mayor enfoque se ha definido la tabla 3, aquí se puede apreciar las áreas que necesitan un enfoque de completitud de los ítems del marco de referencia de la ISO 27001. Como existe una tendencia marcada de ítems evaluados con un nivel de madurez 1 o 2 se los agrupo en la columna llamada “Mayor o igual a 1”, por otro lado, la columna “Igual a 0” lleva el número de objetivos que han sido calificados con un 0. No existen ítems en esta parte que hayan sido calificados como “No Aplica” (N/A). la columna “Nro. Ítems” contiene el total de políticas que tiene asociada esa sección. Finalmente, la columna “Promedio” ha sido calculada como un promedio de los niveles de madurez de los controles asociados a esa sección.

| Dominio | Promedio | Nro. Ítems | Mayor o igual a 1 | Igual a 0 |
|---|---|---|---|---|
| 4.- Contexto de la organización | 1.13 | 8 | 8 | 0 |
| 5.- Liderazgo | 1.06 | 17 | 15 | 2 |
| 6.- Planificación | 0.90 | 29 | 26 | 3 |
| 7.- Soporte | 0.90 | 25 | 23 | 2 |
| 8.- Operación | 1.00 | 3 | 3 | 0 |
| 9.- Evaluación y Desempeño | 0.45 | 20 | 9 | 11 |
| 10.- Mejoramiento | 0.25 | 8 | 2 | 6 |

*Tabla 3. Distribución resumida de los niveles de madurez junto con las secciones del marco de referencia ISO 27001*

Para poder comprender mejor las áreas de enfoque, se puede visualizar los datos en una forma gráfica, tal como se expone en la figura 9.


*Figura 9. Comparativa de los ítems con madurez versus las secciones del marco de referencia ISO 27001*

En esta gráfica, se puede observar que las secciones 4, 5, 6, 7 y 8 muestran que cuentan ítems ya existentes; además se puede ver que en estas secciones el número de ítems que tienen niveles de madurez 0 son bajos. Por el contrario, en las secciones 9 y 10 existe un mayor número de ítems que fueron evaluados con un nivel de madurez de 0.

**Medición y Evaluación de los objetivos de la ISO 27002**

Para el caso de la evaluación de los objetivos descritos en el marco de referencia ISO 27002 se ha mantenido el mismo esquema de evaluación. En esta sección se hizo una evaluación de 119 puntos que hacen referencia a controles que pueden estar implementados dentro de la empresa en forma de políticas de seguridad que ayuden al complimiento de los ítems descrito en la ISO 27001. La tabla 3 muestra el número de ítems evaluados respecto a la escala de nivel de madurez vista al inicio.

| Valor | Efectividad | Significado | Descripción | Número |
|---|---|---|---|---|
| N/A | --- | No Aplicable | El control o política no aplica a la organización | 4 |
| 0 | 0% | Inexistente | Carencia completa de cualquier proceso conocido. | 19 |
| 1 | 10% | Inicial / Ad-hoc | Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales. | 71 |
| 2 | 30% | Reproducible, pero intuitivo | Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual | 25 |
| 3 | 65% | Proceso definido | La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados. | 0 |
| 4 | 85% | Gestionado y medible | Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia | 0 |
| 5 | 100% | Optimizado | Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos | 0 |

*Tabla 4. Nivel de madurez medido en los ítems del marco de referencia ISO 27002*

La distribución de la tabla 4 muestra una tendencia marcada en que existe un número alto en el nivel de madurez 1, seguido del número de políticas calificadas con un nivel de madurez 2, seguidas por las políticas calificadas con un nivel de madurez 0 y al final contando con únicamente 4 políticas que no aplican al contexto de la empresa. Esta distribución se la puede apreciar de forma más clara en la figura 10.

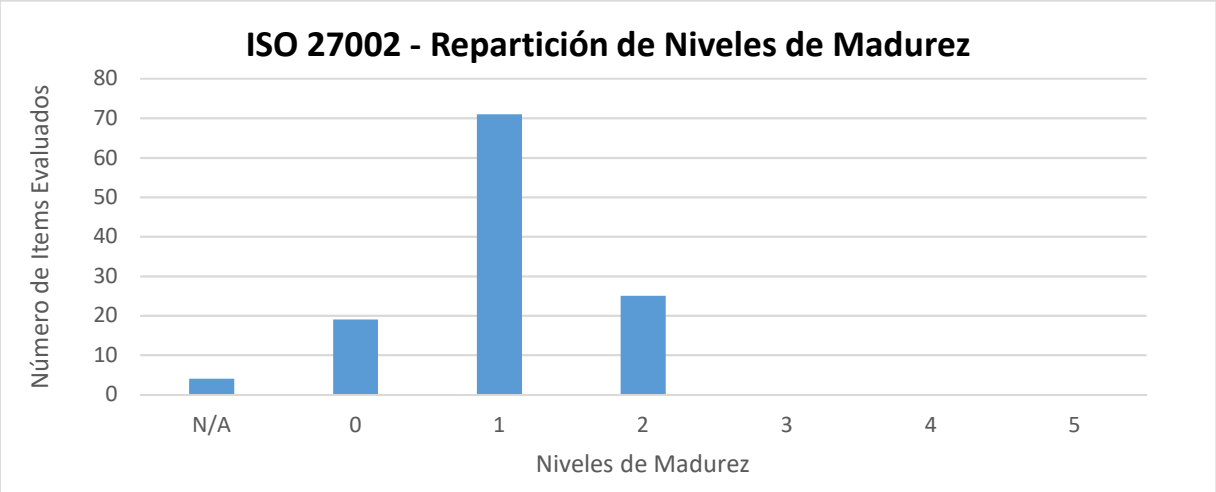



*Figura 8. Repartición de los niveles de Madurez basados en el marco de referencia ISO 27002*

Esta figura muestra la tendencia anteriormente mencionada, que hace referencia al predominio del número de políticas calificadas con un nivel de madurez 1. Cabe mencionarse que no existen políticas calificadas con un nivel de madurez 3 o superior.

Como siguiente punto en el análisis, se ha incluido la distribución de las calificaciones sobre cada una de las secciones de la ISO 27002. Al verificarse anteriormente que las calificaciones no pasan el nivel de madurez 3, se ha decidido unir el conteo de las políticas evaluadas con nivel 1 y 2 en la columna “Mayor o igual a 1”, mientras que en la columna “Igual a 0” se han contabilizado aquellas políticas cuyo nivel de madurez fue calificado como 0; la columna “Nro. Ítems” contiene el total de políticas que tiene asociada esa sección. Finalmente, la columna “Promedio” ha sido calculada como un promedio de los niveles de madurez de los controles asociados a esa sección. Esta distribución se lo puede ver en la tabla 5.

| Dominio | Promedio | Nro. Ítems | Mayor o igual a 1 | Igual a 0 | No Aplica |
|---|---|---|---|---|---|
| Políticas de seguridad | 1.00 | 2 | 2 | 0 | 0 |
| Organización de la seguridad de la Información | 1.27 | 11 | 10 | 1 | 0 |
| Seguridad de los recursos humanos | 0.86 | 7 | 6 | 1 | 0 |
| Gestión de activos | 1.33 | 10 | 9 | 0 | 1 |
| Control de acceso | 1.29 | 14 | 14 | 0 | 0 |
| Criptografía | 2.00 | 2 | 1 | 0 | 1 |
| Seguridad física y del entorno | 1.07 | 15 | 13 | 2 | 0 |
| Seguridad en la Operación | 1.00 | 14 | 10 | 4 | 0 |
| Seguridad de las comunicaciones | 0.86 | 7 | 4 | 3 | 0 |
| Adquisición, desarrollo y mantenimiento de los sistemas de información | 1.00 | 13 | 10 | 2 | 1 |
| Relación con proveedores | 0.80 | 5 | 3 | 2 | 0 |
| Gestión de incidentes de seguridad de la información | 1.00 | 7 | 7 | 0 | 0 |
| Aspectos de seguridad de la información para la gestión de la continuidad de negocio | 0.50 | 4 | 2 | 2 | 0 |
| Cumplimiento | 0.86 | 8 | 5 | 2 | 1 |

*Tabla 5. Distribución resumida de los niveles de madurez junto con las secciones del marco de referencia ISO 27002*

Para ver una distribución gráfica de esta tabla, se ha añadido la figura 11 que muestra la distribución de las secciones con las calificaciones obtenidas por sección.

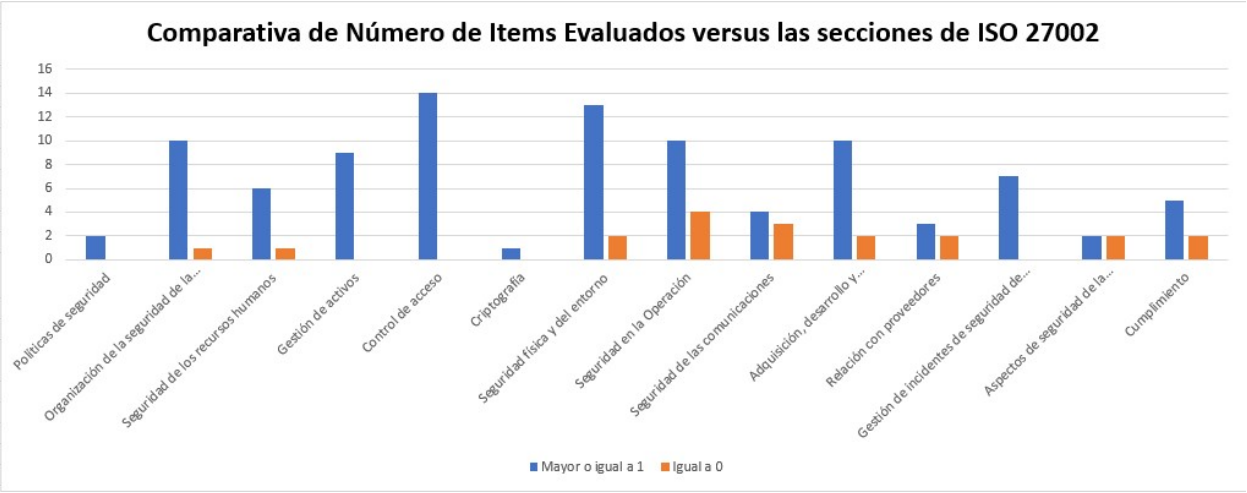



*Figura 11. Comparativa de los ítems con madurez versus las secciones del marco de referencia ISO 27002*

En esta gráfica se puede ver que la distribución de políticas evaluadas con un nivel de madurez de 1 o más se encuentra muy bien distribuida en todos los temas que maneja la ISO27002, en este caso no existe una sección con un número superior de políticas evaluadas con un nivel de madurez 0.

**Conclusiones respecto de la evaluación**

Respecto al análisis de los gráficos y las medidas tomadas se ha llegado a las siguientes conclusiones:

- Al realizarse las mediciones de madurez utilizando los ítems de los marcos de referencia ISO 27001/27002 se pudo evidenciar que su nivel de madurez mayoritariamente se encuentra en el nivel 1, por lo que los conceptos sobre seguridad de la información se encuentran en estados iniciales, por ende, es necesario cultivar mejores prácticas y definiciones sobre temas de seguridad de la información dentro de la empresa.
- Es importante señalar, que adicionalmente es necesario que la empresa tenga una revisión externa de los temas de seguridad a modo de consultorías para reforzar las prácticas y políticas e implementar prácticas que les hacen falta como el manejo de auditorías y el manejo de sus observaciones y no conformidades.
- Es necesario generar una capacitación y concienciación sobre la seguridad de la información dentro de la empresa y explicar los beneficios de la seguridad de la información en las operaciones del día a día de la empresa.

# Entregable 4 - Clasificación de la Información e Identificación de Activos Críticos

La fase de clasificación de la información comprende entender que información maneja la empresa y que tan sensible es esa información respecto al apetito al riesgo que ha definido la empresa. Es importante mencionar que para que las políticas de seguridad de la información y el tratamiento de los riesgos sea eficiente, es necesario conocer que se va a proteger y cuál sería el impacto de no proteger adecuadamente.

La fase de Inventario de activos de Información, hace alusión a que activos de información se manejan dentro de la empresa y guardan una estrecha relación con los Tipos de Información que se identificaron anteriormente. De este análisis se obtendrán los activos de información críticos, los cuales requieren un análisis de riesgos detallado.

La pestaña "Riesgos" contiene el modulador de Impacto de los Riesgos, la probabilidad y la escala de Severidad.

La pestaña "Ent. de Información con Riesgos" contiene la evaluación cuantitativa del Riesgo versus la afectación a la Confidencialidad, Integridad, Disponibilidad y Privacidad.

La pestaña "Ent. de Información - Crit" contiene la evaluación cualitativa del Riesgo versus la afectación a la Confidencialidad, Integridad, Disponibilidad y Privacidad y se define la criticidad de los tipos de información.

La pestaña "Inventario de Activos" contiene todos los activos de IT identificados por la empresa.

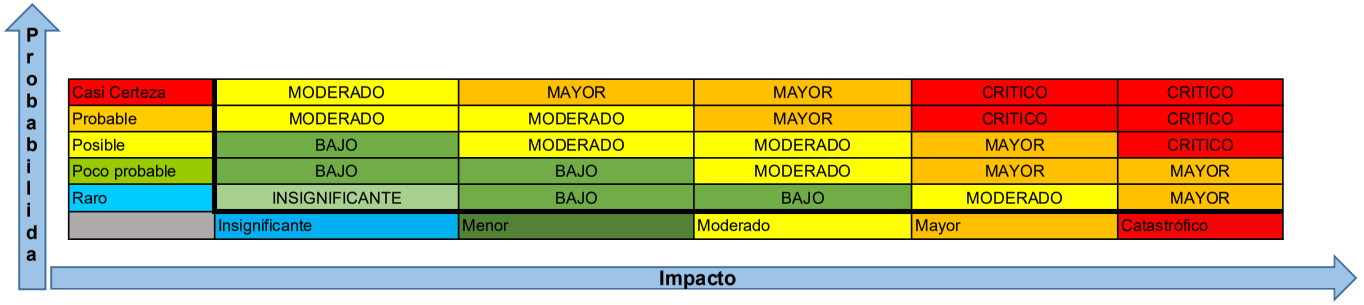
La pestaña "Activos" de Información" contiene los activos de IT más representativos junto con los tipos de información que procesan.

La pestaña "Definición de Activos Críticos" contiene los activos de información con los tipos de información y se añadieron la criticidad de los Tipos de Información, de los activos y los procesos que están involucrados en esos activos.

Finalmente, la pestaña "Resumen de Activos Críticos" muestra una tabla resumen que indica el número de Tipos de Información y el numero de Tipos de Información crítica que un activo de información maneja y su priorización.

| Impacto | | | | | |
|---|---|---|---|---|---|
| | **Escala numérica** | **Pérdidas Financieras** | **Interrupción de operaciones parciales y/o totales** | **Multas y Sanciones de los Organismos de Control** | **Perdida de Cartera** |
| Catastrófico | **5** | Perdidas mayores al 30% del ingreso neto | | Mayor a 3 sanciones al año | Perdida de 4 o más clientes |
| Mayor | **4** | Perdidas mayores al 15% y menores al 30% del ingreso neto | Perdida del servicio mayor a 8 horas y menor a 12 horas. | Mayor a 2 sanciones al año | Perdida de 2 o 3 clientes |
| Moderado | **3** | Perdidas mayores al 8% y menores al 15% del ingreso neto | Perdida del servicio mayor a 4 horas y menor a 8 horas | Mayor a 1 sanciones al año | Perdida de 1 cliente |
| Menor | **2** | Perdidas mayores al 3% y menores al 8% del ingreso neto | Perdida del servicio mayor a 2 horas y menor a 4 horas | | |
| Insignificante | **1** | Perdidas menores al 3% del ingreso neto | Perdida de servicio menor a 2 horas | | |

| Probabilidad | | |
|---|---|---|
| | **%** | **Descripción** |
| 5 | 100% | Casi Certeza |
| 4 | 85% | Probable |
| 3 | 50% | Posible |
| 2 | 25% | Poco probable |
| 1 | 5% | Raro |




| | | | | | |
|---|---|---|---|---|---|
| Casi Certeza | MODERADO | MAYOR | MAYOR | CRITICO | CRITICO |
| Probable | MODERADO | MODERADO | MAYOR | CRITICO | CRITICO |
| Posible | BAJO | MODERADO | MODERADO | MAYOR | CRITICO |
| Poco probable | BAJO | BAJO | MODERADO | MAYOR | MAYOR |
| Raro | INSIGNIFICANTE | BAJO | BAJO | MODERADO | MAYOR |
| | Insignificante | Menor | Moderado | Mayor | Catastrófico |

| Nro. | Nombre ENTIDAD | Nombre Tipo de Información | Descripción Tipo de Información | Pérdidas Financieras | Interrupción de operaciones parciales y/o totales | Multas y Sanciones de los Organismos de Control | Perdida de Cartera | Impacto Confidencialidad | Pérdidas Financieras | Interrupción de operaciones parciales y/o totales | Multas y Sanciones de los Organismos de Control | Perdida de Cartera | Impacto Integridad | Pérdidas Financieras | Interrupción de operaciones parciales y/o totales | Multas y Sanciones de los Organismos de Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Clientes | Información de contacto del cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. | 3 | 2 | 3 | 3 | Moderado | 2 | 2 | 2 | 3 | Moderado | 2 | 1 | 1 |
| 2 | | Información Financiera del Cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. | 3 | 2 | 4 | 4 | Mayor | 5 | 3 | 4 | 5 | Crítico | 3 | 3 | 2 |
| 3 | | Información de Prospecto del Cliente | Información para contacto con el cliente: Dirección Matriz, Número de teléfono convencional, número de teléfono celular, email. | 4 | 4 | 2 | 4 | Mayor | 2 | 3 | 2 | 3 | Moderado | 3 | 2 | 2 |
| 4 | Proveedores | Información de contacto del Proveedor | Información que permita contactar a los proveedores, ya sea de manera física o por medios tecnológicos, Ejemplo: País, ciudad, dirección física de la empresa, número de teléfono convencional/ celular, email, pagina web. | 3 | 3 | 3 | 3 | Moderado | 1 | 1 | 2 | 3 | Bajo | 2 | 2 | 1 |
| 5 | | Información Legal del Proveedor | Información que permita identificar al proveedor, si es persona natural o jurídica. Ejemplo: Registro de la constitución de la empresa, RUC, representante legal, accionistas. | 3 | 3 | 3 | 3 | Moderado | 3 | 2 | 3 | 3 | Moderado | 3 | 2 | 2 |
| 6 | | Información Financiera del Proveedor | Información referente a prestamos, deudas x pagar, deudas x cobrar; así como cuentas bancarias o formas de pago | 3 | 3 | 3 | 3 | Moderado | 3 | 3 | 3 | 3 | Moderado | 3 | 3 | 2 |
| 7 | Organización | Información de Contratos con el cliente | Información sobre productos o servicios que se hayan contratado con la empresa, así como los SLA y garantías. | 3 | 3 | 2 | 3 | Moderado | 3 | 3 | 3 | 3 | Moderado | 3 | 3 | 3 |
| 8 | | Información de conformación de la empresa | Información sobre la conformación de la empresa y su operación. Ejemplo: Conformación de la empresa, socios de la empresa, registro pymes, RUC. | 3 | 3 | 2 | 4 | Moderado | 3 | 3 | 3 | 3 | Moderado | 3 | 3 | 2 |
| 9 | | Información Financiera de la Empresa | Información referente a prestamos, diarios contables, pagos, reembolsos. Utilidades. | 4 | 3 | 3 | 4 | Mayor | 4 | 3 | 4 | 4 | Mayor | 4 | 4 | 2 |
| 10 | | Información Productos y Servicios de la Empresa | Información referente a productos y servicios ofertados por la empresa | 2 | 3 | 2 | 3 | Moderado | 2 | 2 | 1 | 3 | Bajo | 3 | 3 | 2 |
| 11 | | Información sobre actividades diarias de la empresa | Información referente a las actividades diarias de la empresa como informes de servicio técnico, cursos, demos, capacitaciones. | 2 | 3 | 2 | 1 | Bajo | 3 | 4 | 2 | 3 | Moderado | 3 | 4 | 2 |
| 12 | | Información Estrategia de la Empresa | Información referente a estrategia de ventas, oportunidades, proyectos en fase pre-venta | 4 | 4 | 3 | 4 | Mayor | 3 | 2 | 2 | 4 | Moderado | 3 | 3 | 2 |
| 13 | Cartera de los Clientes | Información de contacto de la cartera del cliente. | Información para contacto con la cartera del cliente: Cedula de Identidad, Dirección, Numero de teléfono convencional, numero de teléfono celular, email | 4 | 4 | 4 | 4 | Crítico | 2 | 3 | 4 | 5 | Mayor | 4 | 4 | 5 |
| 14 | | Información de adquisiciones de la cartera del cliente. | Información referente a los productos adquiridos por la cartera del cliente. Ej.: Contrato de Garantía, tipo vehículo, plazo de garantía, componentes vehículo. | 4 | 3 | 4 | 4 | Mayor | 3 | 3 | 4 | 3 | Mayor | 3 | 3 | 2 |
| 15 | | Información de Gestión del Servicio de Atención a Clientes | Información que permite medir la operación del centro de contacto de los clientes. Ejemplo: Llamadas al mes, numero de citas registradas, número de atenciones realizadas | 3 | 3 | 2 | 4 | Moderado | 4 | 3 | 2 | 3 | Moderado | 3 | 3 | 3 |
| 16 | | Información de Operación del Servicio Contratado | Información que permite gestionar el centro de contacto de los clientes. Ejemplo: Código Cliente, Fecha de Cita, Hora de Cita, Servicio Cita | 3 | 3 | 2 | 4 | Moderado | 3 | 3 | 1 | 4 | Moderado | 3 | 2 | 2 |
| 17 | Empleado | Información personal del empleado | Información personal del Empleado: Numero de Cedula, Nombres, Apellidos, Estado Civil Dirección, Numero de teléfono convencional, numero de teléfono celular, email | 3 | 3 | 4 | 2 | Moderado | 3 | 3 | 3 | 3 | Moderado | 1 | 2 | 1 |
| 18 | | Información Financiera del Empleado | Información referente a pagos del empleado: Sueldo del empleado, cargo del empleado, deudas x pagar del empleado, cargas del empleado, roles de pago, etc. | 2 | 4 | 4 | 2 | Moderado | 4 | 3 | 4 | 4 | Mayor | 3 | 3 | 4 |
| 19 | | Información de capacitaciones del empleado | Información referente a los cursos y capacitaciones: Fecha de Certificación, Nombre Certificación, Vigencia Certificación, Empresa Certificación | 3 | 3 | 3 | 3 | Moderado | 4 | 3 | 4 | 4 | Mayor | 3 | 2 | 3 |

| Perdida de Cartera | Impacto Disponibilidad | Pérdidas Financieras | Interrupción de operaciones parciales y/o totales | Multas y Sanciones de los Organismos de Control | Perdida de Cartera | Impacto Privacidad | Impacto Confidencialidad | Impacto Integridad | Impacto Disponibilidad | Impacto Privacidad | Calculo Impacto | Criticidad |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | Bajo | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 2 | 0 | 2.67 | Moderado |
| 4 | Moderado | 0 | 0 | 0 | 0 | N/A | 4 | 5 | 3 | 0 | 4.00 | Crítico |
| 4 | Moderado | 0 | 0 | 0 | 0 | N/A | 4 | 3 | 3 | 0 | 3.33 | Mayor |
| 2 | Bajo | 0 | 0 | 0 | 0 | N/A | 3 | 2 | 2 | 0 | 2.33 | Moderado |
| 2 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 4 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 3 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 4 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 2 | Moderado | 0 | 0 | 0 | 0 | N/A | 4 | 4 | 3 | 0 | 3.67 | Mayor |
| 4 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 2 | 3 | 0 | 2.67 | Moderado |
| 3 | Moderado | 0 | 0 | 0 | 0 | N/A | 2 | 3 | 3 | 0 | 2.67 | Moderado |
| 3 | Moderado | 0 | 0 | 0 | 0 | N/A | 4 | 3 | 3 | 0 | 3.33 | Mayor |
| 5 | Crítico | 3 | 3 | 4 | 5 | Mayor | 5 | 4 | 5 | 4 | 4.50 | Crítico |
| 4 | Moderado | 4 | 3 | 5 | 4 | Crítico | 4 | 4 | 3 | 5 | 4.00 | Crítico |
| 3 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 3 | Moderado | 0 | 0 | 0 | 0 | N/A | 3 | 3 | 3 | 0 | 3.00 | Moderado |
| 2 | Bajo | 4 | 2 | 4 | 2 | Moderado | 3 | 3 | 2 | 3 | 2.75 | Moderado |
| 2 | Moderado | 3 | 3 | 4 | 3 | Mayor | 3 | 4 | 3 | 4 | 3.50 | Mayor |
| 3 | Moderado | 3 | 3 | 4 | 2 | Moderado | 3 | 4 | 3 | 3 | 3.25 | Mayor |

| Nro. | Nombre ENTIDAD | Nombre Tipo de Información | Descripción Tipo de Información | Impacto Confidencialidad | Impacto Integridad | Impacto Disponibilidad | Impacto Privacidad | Criticidad |
|---|---|---|---|---|---|---|---|---|
| 1 | Clientes | Información de Contacto del Cliente | Información para contacto con el cliente: Dirección Matriz, Numero de teléfono convencional, numero de teléfono celular, email | Moderado | Moderado | Bajo | N/A | Moderado |
| 2 | | Información Financiera del Cliente | Información referente a prestamos, deudas x pagar, deudas x cobrar así como facturas emitidas | Mayor | Crítico | Moderado | N/A | Crítico |
| 3 | | Información de Prospecto del Cliente | Información que permita identificar al prospecto. Ejemplo: Nombres y apellidos, numero de cedula, genero, numero de hijos, profesión. | Mayor | Moderado | Moderado | N/A | Mayor |
| 4 | Proveedores | Información de Contacto del Proveedor | Información que permita contactar a los proveedores, ya sea de manera física o por medios tecnológicos, Ejemplo: País, ciudad, dirección física de la empresa, número de teléfono convencional/ celular, email, pagina web. | Moderado | Bajo | Bajo | N/A | Moderado |
| 5 | | Información Legal del Proveedor | Información que permita identificar al proveedor, si es persona natural o jurídica. Ejemplo: Registro de la constitución de la empresa, RUC, representante legal, accionistas. | Moderado | Moderado | Moderado | N/A | Moderado |
| 6 | | Información Financiera del Proveedor | Información referente a prestamos, deudas x pagar, deudas x cobrar; así como cuentas bancarias o formas de pago | Moderado | Moderado | Moderado | N/A | Moderado |
| 7 | Organización | Información de Contratos con el cliente | Información sobre productos o servicios que se hayan contratado con la empresa, así como los SLA y garantías. | Moderado | Moderado | Moderado | N/A | Moderado |
| 8 | | Información de conformación de la empresa | Información sobre la conformación de la empresa y su operación. Ejemplo: Conformación de la empresa, socios de la empresa, registro pymes, ruc. | Moderado | Moderado | Moderado | N/A | Moderado |
| 9 | | Información Financiera de la Empresa | Información referente a prestamos, diarios contables, pagos, reembolsos. Utilidades. | Mayor | Mayor | Moderado | N/A | Mayor |
| 10 | | Información Productos y Servicios de la Empresa | Información referente a productos y servicios ofertados por la empresa | Moderado | Bajo | Moderado | N/A | Moderado |
| 11 | | Información sobre actividades diarias de la empresa | Información referente a las actividades diarias de la empresa como informes de servicio técnico, cursos, demos, capacitaciones. | Bajo | Moderado | Moderado | N/A | Moderado |
| 12 | | Información Estrategia de la Empresa | Información referente a estrategia de ventas, oportunidades, proyectos en fase pre-venta | Mayor | Moderado | Moderado | N/A | Mayor |
| 13 | Cartera de los Clientes | Información de contacto de la cartera del cliente. | Información para contacto con la cartera del cliente: Cedula de Identidad, Dirección, Numero de teléfono convencional, numero de teléfono celular, email | Crítico | Mayor | Crítico | Mayor | Crítico |
| 14 | | Información de adquisiciones de la cartera del cliente. | Información referente a los productos adquiridos por la cartera del cliente. Ej.: Contrato de Garantía, tipo vehículo, plazo de garantía, componentes vehículo. | Mayor | Mayor | Moderado | Crítico | Crítico |
| 15 | | Información de Gestión del Servicio de Atención a Clientes | Información que permite medir la operación del centro de contacto de los clientes. Ejemplo: Llamadas al mes, numero de citas registradas, número de atenciones realizadas | Moderado | Moderado | Moderado | N/A | Moderado |
| 16 | | Información de Operación del Servicio Contratado | Información que permite gestionar el centro de contacto de los clientes. Ejemplo: Código Cliente, Fecha de Cita, Hora de Cita, Servicio Cita | Moderado | Moderado | Moderado | N/A | Moderado |
| 17 | Empleado | Información personal del empleado | Información personal del Empleado: Numero de Cedula, Nombres, Apellidos, Estado Civil Dirección, Numero de teléfono convencional, numero de teléfono celular, email | Moderado | Moderado | Bajo | Moderado | Moderado |
| 18 | | Información Financiera del Empleado | Información referente a pagos del empleado: Sueldo del empleado, cargo del empleado, deudas x pagar del empleado, cargas del empleado, roles de pago, etc. | Moderado | Mayor | Moderado | Mayor | Mayor |
| 19 | | Información de capacitaciones del empleado | Información referente a los cursos y capacitaciones: Fecha de Certificación, Nombre Certificación, Vigencia Certificación, Empresa Certificación | Moderado | Mayor | Moderado | Moderado | Mayor |

| Nro. Activo | Nombre Activo | Formato de Activo | Dueño del Activo |
|---|---|---|---|
| 1 | Servidor ERP/CRM | Físico | CFO - Gerente Financiero |
| 2 | Carpeta Compartida OC | Digital | CFO - Gerente Financiero |
| 3 | Servidor Información Contact Center | Digital | Supervisor Call Center |
| 4 | Firewall | Físico | CSO - Gerente Técnico |
| 5 | Switch Core Empresarial | Físico | CSO - Gerente Técnico |
| 6 | Switch Core Call Center | Físico | Supervisor Call Center |
| 7 | Session Border Controler | Físico | CSO - Gerente Técnico |
| 8 | Central Telefónica Cloud | Físico | CSO - Gerente Técnico<br>Supervisor de Call Center |
| 9 | Router Internet 1 | Físico | CSO - Gerente Técnico |
| 10 | Router Internet 2 | Físico | CSO - Gerente Técnico |
| 11 | Router Canal SIP 1 | Físico | CSO - Gerente Técnico |
| 12 | Router Canal SIP 2 | Físico | CSO - Gerente Técnico |
| 13 | Laptop Gerente General | Físico | CEO - Generente General |
| 14 | Laptop Gerente Financiero | Físico | CFO - Gerente Financiero |
| 15 | Laptop Gerente Técnico | Físico | CSO - Gerente Técnico |
| 16 | Laptop Supervisor Call Center | Físico | Supervisor Call Center |
| 17 | Laptop Lider Desarrollo | Físico | Lider Desarrollo |
| 18 | Laptop Desarrollador 1 | Físico | Desarrollador 1 |
| 19 | Laptop Desarrollador 2 | Físico | Desarrollador 2 |
| 20 | Laptop Asesor 1 | Físico | Asesor 1 |
| 21 | Laptop Asesor 2 | Físico | Asesor 2 |
| 22 | Laptop Asesor 3 | Físico | Asesor 3 |
| 23 | Laptop Asesor 4 | Físico | Asesor 4 |
| 24 | Laptop Asesor 5 | Físico | Asesor 5 |
| 25 | Laptop Asesor 6 | Físico | Asesor 6 |
| 26 | Laptop Asesor 7 | Físico | Asesor 7 |
| 27 | Laptop Asesor 8 | Físico | Asesor 8 |
| 28 | Laptop Asesor 9 | Físico | Asesor 9 |
| 29 | Laptop Asesor Calidad | Físico | Asesor Calidad |
| 30 | Impresora Oficina | Físico | CSO - Gerente Técnico |
| 31 | Impresora Call Center | Físico | Supervisor Call Center |

| Nro. Activo | Nombre Activo | Formato de Activo | Dueño del Activo | Tipo de Información |
|---|---|---|---|---|
| 1 | Servidor ERP/CRM | Físico | CFO - Gerente Financiero | Información de Contacto del Cliente |
| | | | | Información Financiera del Cliente |
| | | | | Información de Prospecto del Cliente |
| | | | | Información de contacto del Proveedor |
| | | | | Información Legal del Proveedor |
| | | | | Información Financiera del Proveedor |
| 2 | Carpeta Compartida OC | Digital | CFO - Gerente Financiero | Información de contacto del Proveedor |
| | | | | Información Legal del Proveedor |
| | | | | Información Financiera del Proveedor |
| | | | | Información de Contratos con el Cliente |
| | | | | Información de conformación de la empresa |
| | | | | Información Financiera de la Empresa |
| | | | | Información Productos y Servicios de la Empresa |
| | | | | Información sobre actividades diarias de la empresa |
| | | | | Información personal del empleado |
| | | | | Información Financiera del Empleado |
| | | | | Información de capacitaciones del empleado |
| 3 | Servidor Información Contact Center | Digital | Supervisor Call Center | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| | | | | Información Financiera del Cliente |
| | | | | Información Financiera del Proveedor |
| | | | | Información sobre actividades diarias de la empresa |
| | | | | Información de capacitaciones del empleado |
| | | | | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |

| | | | | |
|---|---|---|---|---|
| 4 | Firewall | Físico | CSO - Gerente Técnico | Información de Operación del Servicio Contratado |
| | | | | Información Financiera del Empleado |
| | | | | Información de capacitaciones del empleado |
| | | | | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| 5 | Switch Core Empresarial | Físico | CSO - Gerente Técnico | Información de Contacto del Cliente |
| | | | | Información Financiera del Cliente |
| | | | | Información de Prospecto del Cliente |
| | | | | Información de Contratos con el cliente |
| | | | | Información de conformación de la empresa |
| | | | | Información Financiera de la Empresa |
| | | | | Información Productos y Servicios de la Empresa |
| | | | | Información sobre actividades diarias de la empresa |
| | | | | Información personal del empleado |
| | | | | Información Financiera del Empleado |
| | | | | Información de capacitaciones del empleado |
| 6 | Switch Core Call Center | Físico | Supervisor Call Center | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| 7 | Session Border Controler | Físico | CSO - Gerente Técnico | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| 8 | Central Telefónica Cloud | Físico | CSO - Gerente Técnico<br>Supervisor de Call Center | Información de contacto de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |

| | | | | |
|---|---|---|---|---|
| | | | | Información de Operación del Servicio Contratado |
| 9 | Router Internet 1 | Físico | CSO - Gerente Técnico | Información Financiera del Cliente |
| | | | | Información Financiera del Proveedor |
| | | | | Información sobre actividades diarias de la empresa |
| | | | | Información de capacitaciones del empleado |
| | | | | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| | | | | Información Financiera del Empleado |
| | | | | Información de capacitaciones del empleado |
| 10 | Router Internet 2 | Físico | CSO - Gerente Técnico | Información de contacto de la cartera del cliente. |
| | | | | Información de adquisiciones de la cartera del cliente. |
| | | | | Información de Gestión del Servicio de Atención a Clientes |
| | | | | Información de Operación del Servicio Contratado |
| 11 | Router Canal SIP 1 | Físico | CSO - Gerente Técnico | Información de Operación del Servicio Contratado |
| 12 | Router Canal SIP 2 | Físico | CSO - Gerente Técnico | Información de Operación del Servicio Contratado |

| Nro. Activo | Nombre Activo | Formato de Activo | Dueño del Activo | Tipo de Información | Clasificación Criticidad Información | Clasificación del Activo | Proceso(s) |
|---|---|---|---|---|---|---|---|
| 1 | Servidor ERP | Físico | CFO - Gerente Financiero | Información de Contacto del Cliente | Moderado | Crítico | Contabilidad |
| | | | | Información Financiera del Cliente | Crítico | | Proceso Ventas |
| | | | | Información de Prospecto del Cliente | Mayor | | Compras e Importaciones |
| | | | | Información de contacto del Proveedor | Moderado | | |
| | | | | Información Legal del Proveedor | Moderado | | |
| | | | | Información Financiera del Proveedor | Moderado | | |
| 2 | Carpeta Compartida OC | Digital | CFO - Gerente Financiero | Información de contacto del Proveedor | Moderado | Mayor | Compras e Importaciones |
| | | | | Información Legal del Proveedor | Moderado | | Contabilidad |
| | | | | Información Financiera del Proveedor | Moderado | | Seguimiento de Contratos |
| | | | | Información de Contratos con el Cliente | Moderado | | Proceso Ventas |
| | | | | Información de conformación de la empresa | Moderado | | Manejo RRHH |
| | | | | Información Financiera de la Empresa | Mayor | | |
| | | | | Información Productos y Servicios de la Empresa | Moderado | | |
| | | | | Información sobre actividades diarias de la empresa | Moderado | | |
| | | | | Información personal del empleado | Moderado | | |
| | | | | Información Financiera del Empleado | Mayor | | |
| | | | | Información de capacitaciones del empleado | Mayor | | |
| 3 | Servidor Información Contact Center | Digital | Supervisor Call Center | Información de contacto de la cartera del cliente. | Crítico | Crítico | Operación Contact Center |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| 4 | Firewall | Físico | CSO - Gerente Técnico | Información Financiera del Cliente | Crítico | Crítico | Compras e Importaciones |
| | | | | Información Financiera del Proveedor | Moderado | | Contabilidad |
| | | | | Información sobre actividades diarias de la empresa | Moderado | | Seguimiento de Contratos |
| | | | | Información de capacitaciones del empleado | Mayor | | Proceso Ventas |
| | | | | Información de contacto de la cartera del cliente. | Crítico | | Manejo RRHH |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | Operación Call Center |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | Soporte Técnico |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| | | | | Información Financiera del Empleado | Mayor | | |
| | | | | Información de capacitaciones del empleado | Mayor | | |
| | | | | Información de contacto de la cartera del cliente. | Crítico | | |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| 5 | Switch Core Empresarial | Físico | CSO - Gerente Técnico | Información de Contacto del Cliente | Moderado | Crítico | Compras e Importaciones |
| | | | | Información Financiera del Cliente | Crítico | | Contabilidad |
| | | | | Información de Prospecto del Cliente | Mayor | | Seguimiento de Contratos |
| | | | | Información de Contratos con el cliente | Moderado | | Proceso Ventas |
| | | | | Información de conformación de la empresa | Moderado | | Manejo RRHH |
| | | | | Información Financiera de la Empresa | Mayor | | Soporte Técnico |
| | | | | Información Productos y Servicios de la Empresa | Moderado | | |
| | | | | Información sobre actividades diarias de la empresa | Moderado | | |
| | | | | Información personal del empleado | Moderado | | |
| | | | | Información Financiera del Empleado | Mayor | | |
| | | | | Información de capacitaciones del empleado | Mayor | | |
| 6 | Switch Core Call Center | Físico | Supervisor Call Center | Información de contacto de la cartera del cliente. | Crítico | Crítico | Operación Call Center |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| 7 | Session Border Controler | Físico | CSO - Gerente Técnico | Información de Gestión del Servicio de Atención a Clientes | Moderado | Moderado | Operación Call Center |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| 8 | Central Telefónica Cloud | Digital | CSO - Gerente Técnico<br>Supervisor de Call Center | Información de contacto de la cartera del cliente. | Crítico | Crítico | Operación Call Center |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| | | | | Información Financiera del Cliente | Crítico | | Compras e Importaciones |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | Router Internet 1 | Físico | CSO - Gerente Técnico | Información Financiera del Proveedor | Moderado | Crítico | Contabilidad |
| | | | | Información sobre actividades diarias de la empresa | Moderado | | Seguimiento de Contratos |
| | | | | Información de capacitaciones del empleado | Mayor | | Proceso Ventas |
| | | | | Información de contacto de la cartera del cliente. | Crítico | | Manejo RRHH |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | Soporte Técnico |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| | | | | Información Financiera del Empleado | Mayor | | |
| | | | | Información de capacitaciones del empleado | Mayor | | |
| 10 | Router Internet 2 | Físico | CSO - Gerente Técnico | Información de contacto de la cartera del cliente. | Crítico | Crítico | Operación Call Center |
| | | | | Información de adquisiciones de la cartera del cliente. | Crítico | | |
| | | | | Información de Gestión del Servicio de Atención a Clientes | Moderado | | |
| | | | | Información de Operación del Servicio Contratado | Moderado | | |
| 11 | Router Canal SIP 1 | Físico | CSO - Gerente Técnico | Información de Operación del Servicio Contratado | Moderado | Moderado | Operación Call Center |
| 12 | Router Canal SIP 2 | Físico | CSO - Gerente Técnico | Información de Operación del Servicio Contratado | Moderado | Moderado | Operación Call Center |

| Nro. Activo | Nombre Activo | Nro Tipos de Información | Nro. Tipos Información Crítica | Prioridad |
|---|---|---|---|---|
| 1 | Servidor ERP | 6 | 1 | 4 |
| 2 | Carpeta Compartida OC | 11 | 0 | 5 |
| 3 | Servidor Información Contact Center | 4 | 2 | **3** |
| 4 | Firewall | 14 | 5 | **1** |
| 5 | Switch Core Empresarial | 11 | 1 | 4 |
| 6 | Switch Core Call Center | 4 | 2 | **3** |
| 7 | Session Border Controler | 2 | 0 | 5 |
| 8 | Central Telefónica Cloud | 3 | 1 | 4 |
| 9 | Router Internet 1 | 10 | 3 | **2** |
| 10 | Router Internet 2 | 4 | 2 | **3** |
| 11 | Router Canal SIP 1 | 1 | 0 | 5 |
| 12 | Router Canal SIP 2 | 1 | 0 | 5 |

# ANEXO 5

# EVALUACIÓN DE RIESGOS DEL ACTIVO CRÍTICO

## Entregable 7 - Evaluación de Riesgos de activos críticos y Roadmap de planes de acción

En esta fase se hará la evaluación de riesgos del activo crítico denominado “Firewall” que resultó ser el equipo que maneja más tipos de información crítica.

La pestaña "Modulador de Riesgos" contiene el modulador de Impacto de los Riesgos, la probabilidad y la escala de Severidad.

La pestaña "Análisis de Vulnerabilidades" contiene la evaluación de las vulnerabilidades de los componentes Hardware y Software del Activo crítico de Información basado en Magerit y ajustado con el modulador del Riesgo.

La pestaña "Análisis de Controles - Gob. IT" contiene la evaluación a controles basados en planes de gobierno de IT, políticas y definiciones.

La pestaña "Análisis de Controles - Hardware" contiene la evaluación referente a análisis sobre los componentes de hardware y las políticas o controles asociados a problemas con hardware.

La pestaña "Análisis de Controles - Software" contiene la evaluación referente a los componentes de software, sistema operativo y configuraciones y las políticas o controles asociados a estos temas.

Finalmente, la pestaña "Resumen Planes de Acción" muestra una tabla resumen que indica el número de Tipos de Información y el numero de Tipos de Información crítica

| Impacto | | | | | |
|---|---|---|---|---|---|
| | **Escala numérica** | **Pérdidas Financieras** | **Interrupción de operaciones parciales y/o totales** | **Multas y Sanciones de los Organismos de Control** | **Perdida de Cartera** |
| **Catastrófico** | **5** | Perdidas mayores al 30% del ingreso neto | | Mayor a 3 sanciones al año | Perdida de 4 o más clientes |
| **Mayor** | **4** | Perdidas mayores al 15% y menores al 30% del ingreso neto | Perdida del servicio mayor a 8 horas y menor a 12 horas. | Mayor a 2 sanciones al año | Perdida de 2 o 3 clientes |
| **Moderado** | **3** | Perdidas mayores al 8% y menores al 15% del ingreso neto | Perdida del servicio mayor a 4 horas y menor a 8 horas | Mayor a 1 sanciones al año | Perdida de 1 cliente |
| **Menor** | **2** | Perdidas mayores al 3% y menores al 8% del ingreso neto | Perdida del servicio mayor a 2 horas y menor a 4 horas | | |
| **Insignificante** | **1** | Perdidas menores al 3% del ingreso neto | Perdida de servicio menor a 2 horas | | |

**Probabilidad**

| | | | | | |
|---|---|---|---|---|---|
| Casi Certeza | MODERADO | MAYOR | MAYOR | CRITICO | CRITICO |
| Probable | MODERADO | MODERADO | MAYOR | CRITICO | CRITICO |
| Posible | BAJO | MODERADO | MODERADO | MAYOR | CRITICO |
| Poco probable | BAJO | BAJO | MODERADO | MAYOR | MAYOR |
| Raro | INSIGNIFICANTE | BAJO | BAJO | MODERADO | MAYOR |
| | Insignificante | Menor | Moderado | Mayor | Catastrófico |

**Impacto**

| Probabilidad | | |
|---|---|---|
| | % | Descripción |
| 5 | 100% | Casi Certeza |
| 4 | 85% | Probable |
| 3 | 50% | Posible |
| 2 | 25% | Poco probable |
| 1 | 5% | Raro |

| Nro. Activo | Nombre Activo | Formato de Activo | Dueño del Activo | Clasificación del Activo | Proceso(s) | Componente | Taxonomías | Salvaguardas Esperadas | Amenazas | Posibles Vulnerabilidades | Impacto | Probabilidad |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | Firewall | Físico | CSO - Gerente Técnico | Crítico | Compras e Importaciones<br>Contabilidad<br>Proceso Ventas<br>Manejo RRHH<br>Operación Call Center<br>Soporte Técnico | Hardware | [ip] punto de interconexión<br>[mid] equipos medios<br>[bp] dispositivo de frontera<br>[network] soporte de la red [firewall] cortafuegos<br>[Internet] Internet<br>[electronic] electrónicos<br>[disk] discos | HW.A Aseguramiento de la disponibilidad<br>HW.op Operación<br>HW.CM Cambios (actualizaciones y mantenimiento)<br>AUX.power Suministro eléctrico<br>AUX.AC Climatización<br>AUX.wires Protección del cableado<br><br>L.AC Control de los accesos físicos<br>L.A Aseguramiento de la disponibilidad BC.BIA Análisis de impacto (BIA)<br>BC.DRP Plan de Recuperación de Desastres (DRP)<br><br>NEW.HW Equipos: Adquisición o desarrollo<br>NEW.COM Comunicaciones: Adquisición o contratación<br>NEW.MP Soportes de Información: Adquisición<br>NEW.C Productos certificados o acreditados | I.5 Daño por avería física | No hay componentes de hardware de backup dentro de la empresa | Insignificante | Probable |
| | | | | | | | | | | Los equipos tienen 4 años de ser adquiridos | Moderado | Probable |
| | | | | | | | | | | No hay mantenimiento físico en el hardware | Menor | Posible |
| | | | | | | | | | | No hay un análisis de impacto del negocio sobre el equipo | Moderado | Posible |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Moderado | Probable |
| | | | | | | | | | I.7 Condiciones inadecuadas de temperatura y/o humedad | No hay componentes de hardware de backup dentro de la empresa | Menor | Poco probable |
| | | | | | | | | | | Los equipos tienen 4 años de ser adquiridos | Moderado | Posible |
| | | | | | | | | | | No hay mantenimiento físico en el hardware | Insignificante | Posible |
| | | | | | | | | | | No hay un análisis de impacto del negocio sobre el equipo | Mayor | Poco probable |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Moderado | Probable |
| | | | | | | | | | I.10 Degradación de los soportes de almacenamiento de la información | No hay componentes de hardware de backup dentro de la empresa | Moderado | Probable |
| | | | | | | | | | | Los equipos tienen 4 años de ser adquiridos | Mayor | Probable |
| | | | | | | | | | | No hay mantenimiento físico en el hardware | Moderado | Posible |
| | | | | | | | | | | No hay un análisis de impacto del negocio sobre el equipo | Moderado | Posible |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Moderado | Probable |
| | | | | | | | | | | No hay un plan de renovación de tecnología | Moderado | Probable |
| | | | | | | | | | A.25 Robo | No hay componentes de hardware de backup dentro de la empresa | Moderado | Posible |
| | | | | | | | | | | No hay un análisis de impacto del negocio sobre el equipo | Mayor | Posible |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Moderado | Posible |
| | | | | | | | | | | La adquisición e implementación de un equipo pudiera demorar | Mayor | Posible |
| 4 | Firewall | Físico | CSO - Gerente Técnico | Crítico | Compras e Importaciones<br>Contabilidad<br>Proceso Ventas<br>Manejo RRHH<br>Operación Call Center<br>Soporte Técnico | Sistema Operativo | [ip] punto de interconexión<br>[info] protección de la información<br>[auth] datos de validación de credenciales<br>[acl] datos de control de acceso<br>[log] registro de actividad<br>[edi] intercambio electrónico de datos<br>[std] estándar [os] sistema operativo | H.IA Identificación y autenticación<br>H.AC Control de acceso lógico<br>H.ST Segregación de tareas<br>H.IR Gestión de incidencias<br>H.tools.AV Herramienta contra código dañino<br>H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión<br>H.tools.CC Herramienta de chequeo de configuración<br>H.tools.VA Herramienta de análisis de vulnerabilidades<br>H.tools.TM Herramienta de monitorización de tráfico<br>H.tools.DLP DLP: Herramienta de monitorización de contenidos<br>H.tools.LA Herramienta para análisis de logs<br>H.AU Registro y auditoría<br>SW.A Copias de seguridad (backup) SW.start Puesta en producción<br>SW.CM Cambios (actualizaciones y mantenimiento)<br>PS.AT Formación y concienciación<br>BC.BIA Análisis de impacto (BIA)<br>BC.DRP Plan de Recuperación de Desastres (DRP) | E.2 Errores del administrador | No hay copias de seguridad de la configuración | Menor | Probable |
| | | | | | | | | | | No hay gestión de control de cambio | Moderado | Posible |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Posible |
| | | | | | | | | | E.4 Errores de configuración | No hay copias de seguridad de la configuración | Insignificante | Probable |
| | | | | | | | | | | No hay gestión de control de cambio | Insignificante | Probable |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Probable |
| | | | | | | | | | | No hay gestión de logs del firewall | Menor | Posible |
| | | | | | | | | | E.20 Vulnerabilidades de los programas (software) | No se ha realizado un análisis de vulnerabilidad al sistema operativo del firewall | Mayor | Posible |
| | | | | | | | | | | No se ha definido un plan de actualización de la versión del sistema operativo | Moderado | Probable |
| | | | | | | | | | | No se ha deshabilitado funcionalidades que ya no se usan | Moderado | Probable |
| | | | | | | | | | E.21 Errores de mantenimiento / actualización de programas (software) | No se ha definido un plan de actualización de la versión del sistema operativo | Moderado | Posible |
| | | | | | | | | | | No hay copias de seguridad de la configuración | Moderado | Posible |
| | | | | | | | | | | No hay gestión de control de cambio | Menor | Posible |
| | | | | | | | | | | No hay gestión de logs del firewall | Moderado | Probable |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Probable |
| | | | | | | | | | E.24 Caída del sistema por agotamiento de recursos | Los equipos tienen 4 años de ser adquiridos | Moderado | Poco probable |
| | | | | | | | | | | No se ha definido un plan de actualización de la versión del sistema operativo | Moderado | Posible |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Posible |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Mayor | Posible |
| | | | | | | | | | | No se ha deshabilitado funcionalidades que ya no se usan | Moderado | Probable |
| | | | | | | | | | A.4 Manipulación de la configuración | No hay gestión de logs del firewall | Menor | Posible |
| | | | | | | | | | | La contraseña de los usuarios del equipo no se ha actualizado periódicamente | Moderado | Probable |
| | | | | | | | | | | No hay gestión de control de cambio | Moderado | Posible |
| | | | | | | | | | A.7 Uso no previsto | No se ha deshabilitado funcionalidades que ya no se usan | Moderado | Probable |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Posible |
| | | | | | | | | | | No hay gestión de logs del firewall | Moderado | Probable |
| | | | | | | | | | A.11 Acceso no autorizado | No se cuenta con personal especializado en la configuración del firewall | Moderado | Posible |
| | | | | | | | | | | No hay gestión de control de cambio | Moderado | Poco probable |
| | | | | | | | | | | La contraseña de los usuarios del equipo no se ha actualizado periódicamente | Mayor | Probable |
| | | | | | | | | | | No se ha deshabilitado funcionalidades que ya no se usan | Menor | Probable |
| | | | | | | | | | A.24 Denegación de servicio | No hay un análisis de impacto del negocio sobre el equipo | Mayor | Probable |
| | | | | | | | | | | No hay un plan de recuperación de desastres | Mayor | Probable |
| | | | | | | | | | | No se cuenta con personal especializado en la configuración del firewall | Moderado | Posible |
| | | | | | | | | | | No hay gestión de logs del firewall | Menor | Posible |
| | | | | | | | | | | No se ha deshabilitado funcionalidades que ya no se usan | Moderado | Probable |

| Severidad Individual | Severidad General |
|---|---|
| MODERADO | MAYOR |
| MAYOR | |
| MODERADO | |
| MODERADO | |
| MAYOR | |
| BAJO | MODERADO |
| MODERADO | |
| BAJO | |
| MAYOR | |
| MAYOR | |
| MAYOR | CRITICO |
| CRITICO | |
| MODERADO | |
| MODERADO | |
| MAYOR | |
| MAYOR | |
| MODERADO | MAYOR |
| MAYOR | |
| MODERADO | |
| MAYOR | |
| MODERADO | MODERADO |
| MODERADO | |
| MODERADO | |
| MODERADO | MODERADO |
| MODERADO | |
| MAYOR | |
| MODERADO | |
| MAYOR | MAYOR |
| MAYOR | |
| MAYOR | |
| MODERADO | MODERADO |
| MODERADO | |
| MODERADO | |
| MAYOR | |
| MAYOR | |
| MODERADO | MODERADO |
| MODERADO | |
| MODERADO | |
| MAYOR | |
| MAYOR | |
| MODERADO | MODERADO |
| MAYOR | |
| MODERADO | |
| MAYOR | MAYOR |
| MODERADO | |
| MAYOR | |
| MODERADO | CRITICO |
| MODERADO | |
| CRITICO | |
| MODERADO | |
| CRITICO | CRITICO |
| CRITICO | |
| MODERADO | |
| MODERADO | |
| MAYOR | |

| Componente Sub-área | Riesgo(s) | Objetivos del Control | Controles | Tipo de Control | Clasificación del Control | Frecuencia del Control | Pasos de Evaluación | Estándar/Marco Referencia | Evidencia de Referencia | Resultado Evaluación | Planes de Acción | Código del Plan de Acción |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Gobierno IT | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información<br>E.20 Vulnerabilidades de los programas (software)<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>E.24 Caída del sistema por agotamiento de recursos<br>A.24 Denegación de servicio<br>A.25 Robo<br>I.10 Degradación de los soportes de almacenamiento de la información<br>A.25 Robo | Mitigar las interrupciones parciales o totales por fallas de los componentes IT.<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe un plan de recuperación de desastres. | Correctivo | Manual | Semestral | Solicitar el manual de procesos de la empresa.<br>Verificar si existen Políticas o Planes para ejecutarse en caso de una recuperación de desastres. | Cobit | Plan de Recuperación de Desastres | No existe un plan de recuperación de desastres | Elaborar un Plan de recuperación de desastres como parte de las políticas de continuidad del negocio. | AVAC-GB-01 |
| | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información<br>E.20 Vulnerabilidades de los programas (software)<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>E.24 Caída del sistema por agotamiento de recursos<br>A.24 Denegación de servicio<br>A.25 Robo<br>I.10 Degradación de los soportes de almacenamiento de la información<br>A.25 Robo | Mitigar las interrupciones parciales o totales por fallas de los componentes IT.<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe un Plan de Impacto del Negocio | Preventivo | Manual | Semestral | Solicitar el manual de procesos de la empresa.<br>Verificar si existe un Plan de Impacto del Negocio | Cobit | Plan de Impacto del Negocio | No existe un plan de Impacto del Negocio | Elaborar un Plan de Impacto del Negocio de los componentes de IT como parte de las políticas de continuidad del negocio. | AVAC-GB-02 |

| Componente Sub-área | Riesgo(s) | Objetivos del Control | Controles | Tipo de Control | Clasificación del Control | Frecuencia del Control | Pasos de Evaluación | Estándar/Marco Referencia | Evidencia de Referencia | Resultado Evaluación | Planes de Acción | Código del Plan de Acción |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Hardware | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe un contrato de garantía extendida con el fabricante | Manual | Preventivo | Anual | Solicitar al Gerente Financiero el contrato y la OC por la renovación de la garantía. Validar que el contrato este vigente a la actualidad. | Cobit | Contrato de soporte o extensión de garantía | Existe un contrato de extensión de garantía vigente | Generar una política de renovación de soporte y garantía para los equipos críticos de IT. | AVAC-HW-01 |
| | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información<br>I.7 Condiciones inadecuadas de temperatura y/o humedad | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe el monitoreo del estado de los componentes de hardware | Automático | Preventivo | Semanal | Solicitar al Gerente técnico se facilite acceso a la plataforma de monitoreo.<br>Solicitar acceso al monitoreo del firewall en donde se muestre el estado del hardware.<br>Verificar si es posible acceder al monitoreo del estado de los componentes de hardware. | ISO 27002 | Captura de pantalla sobre el monitoreo y la información que muestra | Existe monitoreo del estado de hardware, sin embargo no hay detalle del estado de los componentes internos. | Definir un plan de mejora del monitoreo del estado del firewall a través de herramientas que brinden mejor detalle del funcionamiento del hardware. | AVAC-HW-02 |
| | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe un plan de renovación/mejoramiento de la plataforma de IT. | Manual | Preventivo | Semestral | Solicitar al Gerente Financiero o al Gerente Técnico un plan de renovación o mejoramiento sobre los componentes de IT | ISO 27001 | Plan de renovación/mejoramiento de los componentes de IT | No existe un plan de renovación/mejoramiento de la plataforma de IT. | Definir un plan de renovación de los componentes de IT.<br>Definir un plan de contingencia para componentes críticos de IT. | AVAC-HW-03 |
| | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información<br>I.7 Condiciones inadecuadas de temperatura y/o humedad | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe un cronograma de mantenimiento físico del firewall. | Manual | Preventivo | Semestral | Solicitar la Gerente Técnico el plan de mantenimiento del firewall | ISO 27001/ISO 27002 | Plan de mantenimiento de la infraestructura de IT: | No existe un plan de mantenimiento de la infraestructura de IT. | Definir una política de mantenimiento preventivo de los componentes de IT | AVAC-HW-04 |
| | I.5 Daño por avería física<br>I.10 Degradación de los soportes de almacenamiento de la información<br>I.7 Condiciones inadecuadas de temperatura y/o humedad | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas | Verificar si existe monitoreo de las condiciones operativas respecto al Data Center, su ventilación y temperatura. | Manual | Preventivo | Semanal | Solicitar al Gerente Técnico una bitácora del monitoreo de las condiciones de operación del Data Center | ISO 27002 | Bitácora de monitoreo del estado de operación del data Center | No existe una bitácora de monitoreo del estado de operación del Data Center | Definir un plan de monitoreo de las condiciones operativas del Dat Center | AVAC-HW-05 |
| | A.25 Robo | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si existe aseguramiento a nivel de los equipos IT de la empresa que cubran casos como destrucción o robo de bienes. | Manual | Preventivo | Anual | Solicitar al Gerente Financiero la documentación si existen pólizas de seguros sobre los equipos de TI. | ISO 27001/ISO 27002 | Póliza de aseguramiento de los componentes IT de la empresa. | Existe una póliza de aseguramiento de IT de los activos de | Definir un plan de actualización de la póliza de seguros en casos de que se adquieran nuevos elementos de IT. | AVAC-HW-06 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A.25 Robo | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si dentro de la empresa si existen medios de grabación para identificación al acceso del data center y de la empresa | Manual | Preventivo | Mensual | Solicitar al Gerente Técnico evidencia respecto a que los accesos al data center se graben o se almacenen. | ISO 27001/ISO 27002 | Acceso a la herramienta de grabación de videos | No existe una herramienta para la grabación de acceso a la empresa o el datacenter, únicamente hay esas medidas en el edificio. | Definir un plan de registro de visitas de clientes, proveedores y un registro de video de acceso a las oficinas. | AVAC-HW-07 |
| | A.25 Robo | Mitigar las interrupciones parciales o totales por fallas de hardware<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Verificar si dentro de la oficina se cumplen con los controles físicos dispuestos como medidas de seguridad tales como restricción de acceso, identificación en el acceso, etc. | Manual | Preventivo | Mensual | Solicitar al Gerente Técnico una bitácora de accesos al data center que incluyan autorizaciones e identificaciones de quienes acceden al Data Center. | ISO 27001/ISO 27002 | Bitácora de Acceso al Data Center | No existe una bitácora de acceso del personal al Data Center | Definir una política de registro de acceso a la data center y documentar estos accesos. | AVAC-HW-08 |

| Componente Sub-área | Riesgo(s) | Objetivos del Control | Controles | Tipo de Control | Clasificación del Control | Frecuencia del Control | Pasos de Evaluación | Estándar/Marco Referencia | Evidencia de Referencia | Resultado Evaluación | Planes de Acción | Código del Plan de Acción |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistema Op | E.2 Errores del administrador<br>E.4 Errores de configuración<br>E.21 Errores de mantenimiento / actualización de programas (software) | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si el sistema operativo del firewall permite sacar copias de seguridad sobre la configuración y si existen copias de seguridad de la configuración | Preventivo | Manual | Mensual | Solicitar acceso a la interface web del firewall. Validar que el firewall permita generar un backup de la configuración. Verificar con el Gerente Técnico si hay un procedimiento para backup de configuraciones. | Cobit | Archivo de backup de información. Bitácora de ejecución de copias de respaldo. | Las copias de seguridad de la configuración del firewall se pueden obtener de la interface gráfica. No se cuenta con un procedimiento de backup de configuraciones. | Definir una política de respaldos de configuraciones del firewall. | AVAC-SO-01 |
| | E.2 Errores del administrador<br>E.4 Errores de configuración<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>A.4 Manipulación de la configuración<br>A.11 Acceso no autorizado | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si existe un procedimiento dentro de la empresa para gestionar cambios en la infraestructura o configuraciones de los componentes IT. | Preventivo | Manual | Semanal | Solicitar al Gerente Técnico una bitácora o registro de los controles de cambio ejecutados en la empresa en los últimos 6 meses. | ISO 27001/ISO27002 | Registro o Bitácora de los cambios registrados de los últimos 6 meses sobre la infraestructura de IT de la empresa. | No se cuenta con un registro formal o bitácora de los cambios en la infraestructura IT registrados en los últimos 6 meses. Existen registros de cambios de los sistemas de la empresa. | Definir una política de control de cambios para la infraestructura de IT, incluir una calendarización y documentación sobre los cambios a ejecutarse. | AVAC-SO-02 |
| | E.2 Errores del administrador<br>E.4 Errores de configuración<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>E.24 Caída del sistema por agotamiento de recursos<br>A.7 Uso no previsto<br>A.11 Acceso no autorizado<br>A.24 Denegación de servicio | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si el personal que administra el firewall cuenta con experiencia previa en manejo de equipos de seguridad de la información. | Preventivo | Manual | Semestral | Solicitar al Gerente Técnico/ Gerente Financiero las hojas de vida de las personas que administran el firewall. | ISO 27001/ISO27002 | Hojas de Vida del personal que administra el firewall. | El personal que administra el firewall cuenta con experiencia previa en administración de firewall. | Reforzar los conocimientos del personal por medio de cursos y capacitaciones sobre el firewall de la empresa. | AVAC-SO-03 |
| | E.2 Errores del administrador<br>E.4 Errores de configuración<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>E.24 Caída del sistema por agotamiento de recursos<br>A.7 Uso no previsto<br>A.11 Acceso no autorizado<br>A.24 Denegación de servicio | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si el personal que administra el firewall cuenta con una certificación vigente del fabricante del firewall. | Preventivo | Manual | Semestral | Solicitar al Gerente Técnico/ Gerente Financiero el listado de certificaciones que tiene el personal que administra el firewall. | ISO 27001/ISO27002 | Listado de Certificaciones que posee el personal que administra el firewall. | El personal que administra el firewall cuenta con certificaciones de otros fabricantes diferentes al del firewall existente en la empresa. | Implementar un plan de certificación del personal que administra el firewall, que incluya cursos del fabricante del firewall y la certificación del personal. | AVAC-SO-04 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| e r a t i v o | E.4 Errores de configuración<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>A.4 Manipulación de la configuración<br>A.7 Uso no previsto<br>A.24 Denegación de servicio | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si existe análisis de logs y gestión de logs. | Preventivo | Manual | Semanal | Solicitar al Gerente Técnico acceso al firewall y validar la opción de logs y determinar en donde se almacenan estos logs. | ISO 27001/ISO27002 | Pantalla de acceso a la configuración de los logs en el firewall | El firewall cuenta con una opción para manejar y analizar los logs, los logs se almacenan únicamente en el equipo, y se mantienen hasta por 15 días. | Implementar una política de gestión y análisis de logs para almacenar una copia de los logs en otra herramienta y por mas de 15 días. | AVAC-SO-05 |
| | E.20 Vulnerabilidades de los programas (software) | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si se han hecho análisis de vulnerabilidades sobre el firewall existente en la empresa y si estas vulnerabilidades se encuentran parchadas. | Preventivo | Manual | Mensual | Solicitar al Gerente Técnico un reporte sobre análisis de vulnerabilidades del firewall y su plan de remediación. | ISO 27001/ISO27002 | Informe de vulnerabilidades detectadas en el firewall y las acciones necesarias para remediar esas vulnerabilidades. | No existe un informe sobre el análisis de vulnerabilidades del firewall. | Implementar una política de análisis y gestión de vulnerabilidades para componentes críticos de IT. | AVAC-SO-06 |
| | E.20 Vulnerabilidades de los programas (software)<br>E.21 Errores de mantenimiento / actualización de programas (software)<br>E.24 Caída del sistema por agotamiento de recursos | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Identificar si existen planes de mantenimiento preventivo lógico y actualización de versión del sistema operativo del firewall. | Preventivo | Manual | Semestral | Solicitar al Gerente Técnico información sobre los mantenimientos preventivos lógicos y actualización del sistema operativo de los equipos de IT. | ISO 27001/ISO27002 | Cronograma o Planificación de mantenimientos preventivos lógicos y actualizaciones del sistema operativo de los componentes de IT. | No existe una planificación sobre el mantenimiento preventivo lógico y actualización del sistema operativo de los equipos de IT. | Definir una política de mantenimiento preventivo de los componentes de IT | AVAC-HW-04 |
| | E.24 Caída del sistema por agotamiento de recursos<br>A.7 Uso no previsto<br>A.11 Acceso no autorizado<br>A.24 Denegación de servicio | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Evaluar si existen registros de ajustes de configuraciones basados en recomendaciones del fabricante del firewall. | Preventivo | Manual | Semestral | Solicitar la Gerente Técnico información sobre registros de ajustes de configuraciones basados en las recomendaciones del fabricante. | ISO 27001/ISO27002 | Informe técnico sobre ajustes basados en recomendaciones del fabricante. | Se cuenta con un reporte que se ejecutó en la ultima actualización del sistema operativo. El informe no se encuentra actualizado. | Incluir en la política de mantenimientos preventivos de los componentes de IT una actividad referente a aplicar ajustes y configuraciones recomendadas por fábrica. | AVAC-HW-04 |
| | E.24 Caída del sistema por agotamiento de recursos<br>A.7 Uso no previsto<br>A.11 Acceso no autorizado<br>A.24 Denegación de servicio | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Evaluar si existen funcionalidades del firewall que se encuentren activas y que ya no se estén utilizando. | Preventivo | Manual | Semestral | Solicitar la Gerente Técnico información sobre la configuración actual del firewall y una descripción de los usos de las funciones configuradas | ISO 27001/ISO27002 | Captura de pantallas de las configuraciones realizadas en el firewall. Entrevista con el personal que administra el firewall. | Se ha determinado que existen configuradas funciones en el firewall que ya no se encuentran siendo ocupadas. | Incluir en la política de mantenimientos preventivos de los componentes de IT una actividad referente a desactivar las funcionalidades que ya no se utilizan en la empresa. | AVAC-HW-04 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A.4 Manipulación de la configuración<br>A.11 Acceso no autorizado | Mitigar las interrupciones parciales o totales por fallas de Software<br>Mitigar posibles perdidas financieras<br>Mitigar las posibles multas y sanciones de organismos de control<br>Mitigar las posibles perdidas de clientes | Evaluar si existen contraseñas seguras del firewall, quien las administra y si estas se han actualizado. | Preventivo | Manual | Trimestral | Solicitar al Gerente Técnico la revisión de la configuración de contraseñas para el firewall y consultar cada cuanto se cambian estas contraseñas. | ISO 27001/ISO27002 | Revisión de formatos de contraseñas, bitácora de contraseñas y registro de cambios de contraseñas. | Se cuenta con una bitácora de contraseñas para todos los equipos de IT, sin embargo, las contraseñas no se han actualizado en más de un año. | Reforzar la política de gestión de contraseñas de los componentes de IT en la empresa para que se incluyan periodos para los cambios de las contraseñas de administración. | AVAC-SO-07 |

| *Código Plan* | *Plan de Acción* | *Objetivos del Plan de Acción* | *Desarrollo del Plan* | *Fecha Inicio* | *Fecha Fin* | *Responsable(s)* |
|---|---|---|---|---|---|---|
| AVAC-GB-01 | Elaborar un Plan de recuperación de desastres como parte de las políticas de continuidad del negocio. | Obtener un plan de recuperación de desastres que se encuentre apegado a las necesidades y a la realidad de la empresa. | Definir un marco de referencia para la elaboración del plan, analizar las actividades fundamentales para generar la recuperación de las operaciones de la empresa, definir las notificaciones de servicio a los clientes que hayan sido afectados. | 1/12/2021 | 30/5/2022 | Gerente Técnico Oficial de Seguridad de la información |
| AVAC-GB-02 | Elaborar un Plan de Impacto del Negocio de los componentes de IT como parte de las políticas de continuidad del negocio. | Obtener un plan de Impacto al negocio que haga referencia a los componentes IT críticos para la empresa | Definir un análisis de activos críticos. Definir el impacto en las operaciones que estos activos críticos tienen. Determinar las perdidas financieras que conllevaría la falla de ese equipo. | 1/12/2021 | 30/5/2022 | Gerente Técnico Oficial de Seguridad de la información |
| AVAC-HW-01 | Generar una política de renovación de soporte y garantía para los equipos críticos de IT. | Disponer de lineamientos para la renovación de las garantías y soporte técnico de los componentes de hardware críticos de la empresa. | Definir un listado de proveedores conocidos para la organización. Solicitar certificados y referencias a los proveedores. | 30/3/2022 | 30/4/2022 | Gerente Técnico Gerente Financiero |

| | | | | | | |
|---|---|---|---|---|---|---|
| AVAC-HW-02 | Definir un plan de mejora del monitoreo del estado del firewall a través de herramientas que brinden mejor detalle del funcionamiento del hardware. | Disponer de lineamientos y procesos para mejorar las capacidades actuales del monitoreo en base a herramientas que ayuden a manejar el monitoreo del hardware crítico. | Definir la necesidad de implementar una solución de monitoreo. Definir las métricas de monitoreo necesarias. Definir calendarización de reportes. | 1/5/2022 | 31/7/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT |
| AVAC-HW-03 | Definir un plan de renovación de los componentes de IT. Definir un plan de contingencia para componentes críticos de IT. | Definir las necesidad de redundancia y alta disponibilidad para componentes de IT críticos, así como definir el tiempo que las adquisiciones se mantengan operativas en la empresa. | Definir la vida útil de los componentes IT. Definir la reutilización de los componentes IT si aplica. Definir un roadmap de adquisiciones como parte de las renovaciones de IT. | 3/1/2022 | 28/2/2022 | Gerente General, Gerente Técnico, Gerente Financiero. |
| AVAC-HW-04 | Definir una política de mantenimiento preventivo de los componentes de IT | Definir las actividades referente a los mantenimientos preventivos de los componentes críticos tanto físicamente como lógicamente. | Definir el calendario de mantenimiento de los componentes de IT. Definir las actividades de los mantenimientos. Definir alcances adicionales como actualización de sistema operativo, desactivación de funcionalidades que no se usan. Incluir la aplicación de las recomendaciones de fabrica respecto a la configuración de los equipos | 1/3/2022 | 1/4/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT |

| | | | | | | |
|---|---|---|---|---|---|---|
| AVAC-HW-05 | Definir un plan de monitoreo de las condiciones operativas del Data Center | Señalar las actividades referentes al monitoreo ambiental del data center | Definir la frecuencia de medición de las condiciones operativas del data center. Definir las acciones a tomarse en caso que haya desviaciones de las condiciones regulares. | 1/5/2022 | 1/7/2022 | Gerente Técnico Personal de IT. |
| AVAC-HW-06 | Definir un plan de actualización de la póliza de seguros en casos de que se adquieran nuevos elementos de IT. | Definir los lineamientos para la adquisición de pólizas de seguros y la definición de qué equipos deben contar con estas pólizas. | Definir las pólizas a ser adquiridas. Definir los equipos que se incluyan en las pólizas. Definir las condiciones respecto a la aplicación de las pólizas. | 1/5/2022 | 1/7/2022 | Gerente Técnico Gerente Financiero |
| AVAC-HW-07 | Definir un plan de registro de visitas de clientes, proveedores y un registro de video de acceso a las oficinas. | Definir procedimientos para documentar las visitas de proveedores a la oficina, incluir la grabación de partes vitales como el acceso al data center. | Definir las áreas sociales de la oficina. Definir las áreas sensibles de la organización en donde se deba instalar cámaras. | 1/6/2022 | 1/7/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT |
| AVAC-HW-08 | Definir una política de registro de acceso a la data center y documentar estos accesos. | Definir procedimientos, lineamientos para registrar el acceso al data center e identificar a los visitantes del data center. | Definir un formato para registro de las visitas. Definir procesos para registrar el personal que van a visitar el data center y las actividades. | 1/6/2022 | 1/7/2022 | Gerente Técnico Oficial de Seguridad de la información |
| AVAC-SO-01 | Definir una política de respaldos de configuraciones del firewall. | Definir procedimientos para obtener un backup de la configuración del firewall, ya sea de forma manual o automática. | Definir la periodicidad de los respaldos. Definir los pasos para obtener la copia de seguridad. Definir en donde se almacenarán los respaldos. | 1/6/2022 | 1/7/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT |

| | | | | | | |
|---|---|---|---|---|---|---|
| AVAC-SO-02 | Definir una política de control de cambios para la infraestructura de IT, incluir una calendarización y documentación sobre los cambios a ejecutarse. | Definir los lineamientos para mantener un registro de cambios sobre la infraestructura de IT así como los días de ejecutarse estos cambios. | Definir horarios para los trabajos en la infraestructura. Definir el procedimiento de registro del control de cambios. | 1/7/2022 | 1/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT |
| AVAC-SO-03 | Reforzar los conocimientos del personal por medio de cursos y capacitaciones sobre el firewall de la empresa. | Definir capacitaciones las cuales refuercen los conocimientos de los encargados de seguridad e IT. | Definir un listado de cursos para cada persona que maneja equipos de IT durante el año 2022. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Gerente Financiero<br>Oficial de Seguridad de la Información<br>Personal de IT |
| AVAC-SO-04 | Implementar un plan de certificación del personal que administra el firewall, que incluya cursos del fabricante del firewall y la certificación del personal. | Definir un plan de cursos de certificación del personal que administra el firewall. | Definir un listado de cursos referentes a administración de firewalls de la marca de los equipos de la empresa. Definir las certificaciones que se van a rendir, definir los costos de estas certificaciones. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Gerente Financiero<br>Oficial de Seguridad de la Información<br>Personal de IT |
| AVAC-SO-05 | Implementar una política de gestión y análisis de logs para almacenar una copia de los logs en otra herramienta y por mas de 15 días. | Definir los lineamientos, planes de acción y periodicidad del almacenamiento de los logs para sus análisis. | Definir el sitio de almacenamiento de los logs. Definir el tiempo de retención de los logs. Definir la periodicidad de cuando se respalden los logs. Definir el responsable de estas actividades. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT |

| | | | | | | |
|---|---|---|---|---|---|---|
| AVAC-SO-06 | Implementar una política de análisis y gestión de vulnerabilidades para componente críticos de IT. | Definir las actividades necesarias para evaluar vulnerabilidades en los componentes críticos así como la periodicidad de estos análisis. | Definir los métodos o herramientas para el análisis de vulnerabilidades. Definir un cronograma de análisis. Definir los planes de acción en base a las vulnerabilidades que se encuentren. | 15/7/2022 | 30/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT |
| AVAC-SO-07 | Reforzar la política de gestión de contraseñas de los componentes de IT en la empresa para que se incluyan periodos para los cambios de las contraseñas de administración. | Definir lineamientos para mejorar la gestión de las contraseñas, así como definir periodicidad e indicación de contraseñas al personal que lo requiera basado en sus actividades. | Definir esquemas de contraseñas. Definir calendarización para el cambio de contraseñas. Definir responsables del cambio de contraseñas. | 1/7/2022 | 1/10/2022 | Gerente Técnico<br>Personal de IT. |

# ANEXO 6

# POLÍTICAS DE ALTO NIVEL

## Entregable 5 – Políticas de Seguridad de Alto Nivel

Las políticas de seguridad de la información tienen como objetivo definir lineamientos sobre la protección de activos de la información de la empresa, de la mano de procesos, prácticas, normas y documentación que permitan alcanzar los objetivos de seguridad de la información.

Las políticas expuestas en el presente documento tienen como referencia lo establecido en el marco de referencia ISO 27001 haciendo referencia a las de la ISO 27001 y adaptándose al estado actual de la empresa.

Por otra parte, para identificar la estructura de las políticas, se ha tomado la estructura del "Formato de Referencia de Política de Seguridad de la Información –EGSI"[1], el mismo que señala una estructura que se compone de las siguientes consideraciones por política:

- **Descripción de la política:** Se señala una breve descripción de las políticas, y como estas políticas aportan a la empresa.
- **Objetivo:** Se señala cual es la meta de la política en la organización.
- **Roles y Responsabilidades:** En esta sección se mencionará quien o quienes serán los responsables de implementar, monitorear, evaluar e incluir mejoras a estas políticas.
- **Alcance:** Esta sección hará referencia a que componentes, procesos, personal de la empresa se hará aplicable la política.

En esta sección también se hace referencia a la **Comunicación de la política**, en este caso esta actividad se la hará por medio talleres de concienciación sobre las normas y la difusión del documento una vez que el programa de seguridad de la información inicie sus operaciones.

Para el caso del sistema de gestión de seguridad de la información que se encuentra en desarrollo, es necesario definir las siguientes Políticas de Seguridad de Alto Nivel:

1. **<u>Política de definición de objetivos de seguridad.</u>**

   *Descripción:* Esta política estará encargada de la definición de nuevos objetivos de seguridad de la información en caso de que la empresa amplié su portafolio de productos y servicios.

   *Objetivo:* Brindar consideraciones y lineamientos basados en los objetivos y necesidades empresariales para definir nuevos objetivos de seguridad.

[1] Ministerio de Telecomunicaciones – Gobierno electrónico. Formato referencial para la elaboración de la política de seguridad de la información (EGSI) .Tomado de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/03/Formato-Referencial_Pol%C3%ADtica-de-Seguridad-de-la-Informaci%C3%B3n-EGSI.pdf

*Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor)

.

*Alcance:* El SGSI y el programa de seguridad de la información.

2. **Política de seguimiento, medición y cumplimiento de objetivos de seguridad.**

   *Descripción:* Esta política tendrá como objetivo el cumplimiento de los objetivos de seguridad de la información, tomando en cuenta los diferentes contextos de la organización, así como su mejora continua.

   *Objetivo:* Definir un esquema de métricas de seguimiento, medición y cumplimiento de los objetivos de control que se apoyan en marcos de referencia existentes para brindar evaluaciones periódicas y generar una mejora continua en el SGSI.

   *Roles y Responsabilidades:* CEO – Gerente General(Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor).

   *Alcance:* El SGSI y el programa de seguridad de la información.

3. **Política para la gestión de los riesgos de seguridad de la información.**

   *Descripción:* Esta política estará orientada a la identificación, manejo y tratamiento de los riesgos de seguridad de la información y como estos riesgos pueden afectar a la empresa calculando su impacto.

   *Objetivo:* Definir un procedimiento para la identificación de los riesgos de seguridad de la información, su impacto en las operaciones de la empresa y la gestión de estos riesgos durante el tiempo.

   *Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CFO – Gerente Financiero (Evaluador), CTO – Gerente Técnico (Ejecutor) y OSI – Oficial de Seguridad de la Información(Ejecutor).

   *Alcance:* El SGSI y el programa de seguridad de la información.

4. **Política de asignación de roles y responsabilidades dentro del programa de seguridad de la información.**

   *Descripción:* Esta política estará encargada de definir los roles y responsabilidades de la seguridad de la información y como estas responsabilidades se repartirán dentro del departamento de IT.

*Objetivo:* Definir un listado de responsabilidades referentes a la seguridad de la información y su interrelación dentro del departamento IT para definir procesos e interacciones, además de definir las actividades del responsable de seguridad de la información.

*Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CTO – Gerente Técnico (Ejecutor), OSI – Oficial de Seguridad de la Información y departamento de IT (Ejecutor).

*Alcance:* Personal del departamento de IT y OSI – Oficial de Seguridad de la información.

5. **Política de gestión de recursos de seguridad de la información.**

*Descripción:* Esta política estará encargada de la definición de los recursos de seguridad de la información, así como de los equipos, servicios y tecnologías que ayuden a alcanzar los objetivos de seguridad de la información dentro de la empresa.

*Objetivo:* Definir la implementación, gestión, monitoreo y mejora continua de los recursos de seguridad de acción, en conjunto con sus responsables por medio de las soluciones, mecanismos y tecnología adquiridas para poder implementar mecanismos de seguridad de la información.

*Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CFO - Gerente Financiero (Evaluador), CTO – Gerente Técnico (Ejecutor) y OSI – Oficial de Seguridad de la Información (Ejecutor).

*Alcance:* El inventario tecnológico de la empresa, las adquisiciones para seguridad de la información que fueran necesarias y el personal de la empresa.

6. **Política de gestión de la documentación del sistema de seguridad de la información.**

*Descripción:* En esta política se señalará como se lleva a cabo la documentación respecto a la operación del SGSI durante el tiempo y como se actualizará la documentación sobre el SGSI.

*Objetivo:* Definir la documentación se generará, en que periodos se generará para generar evaluaciones y un registro de seguimiento de las actividades del programa de seguridad de la información en el tiempo.

*Roles y Responsabilidades:* CEO – Gerente General(Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor).

*Alcance:* El SGSI y el programa de seguridad de la información.

7. **Política de operaciones seguras y gestión de incidentes**

   *Descripción:* Esta política definirá los lineamientos para asegurar la operación teniendo en cuenta la confidencialidad, integridad, disponibilidad y privacidad en la operación de la empresa, adicionalmente de incluir planes de manejo de incidentes de seguridad de la información y su recuperación.

   *Objetivo:* Brindar lineamientos para que las operaciones que ejecuta la empresa en su día a día contemplen la seguridad de la información, así como señalar los procedimientos para el manejo de incidentes de seguridad y continuidad del negocio.

   *Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CFO - Gerente Financiero (Ejecutor), CTO – Gerente Técnico (Ejecutor) y OSI – Oficial de Seguridad de la Información (Ejecutor).

   *Alcance:* Toda la organización.

8. **Política de Evaluación del desempeño del SGSI**

   *Descripción:* Esta política estará encargada de definir métricas de evaluación para los diferentes objetivos de seguridad de la información de la empresa.

   *Objetivo:* Definir métricas de evaluación de las diferentes políticas utilizando marcos de referencia que fortalezcan la evaluación de las métricas y que ayuden a medir el nivel de madurez de las políticas y controles establecidos en la empresa.

   *Roles y Responsabilidades:* CEO – Gerente General(Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor).

   *Alcance:* El SGSI y el programa de seguridad de la información.

9. **Política de Auditorias de seguridad de la información**

   *Descripción:* Esta política definirá el esquema de funcionamiento de las auditorias de seguridad de la información, así como la gestión de las no conformidades y observaciones encontradas en dichas auditorias.

   *Objetivo:* Establecer las condiciones de las auditorias que se vayan a llevar a cabo sobre el SGSI, el programa de seguridad de la información

y la organización; así como también establecer los lineamientos para tratar las observaciones y no conformidades y las acciones que la empresa tome para afrontar estas observaciones.

*Roles y Responsabilidades:* CEO – Gerente General (Evaluador), CFO - Gerente Financiero (Evaluador), CTO – Gerente Técnico (Ejecutor) y OSI – Oficial de Seguridad de la Información (Ejecutor). Se debe contratar un Auditor externo para esta actividad.

*Alcance:* El SGSI y el programa de seguridad de la información.

## 10. Política de mejora continua del SGSI

*Descripción:* Esta política estará encargada de señalar lineamientos que la empresa debe seguir para la mejora continua del SGSI y su programa de seguridad de la información.

*Objetivo:* Establecer procedimientos para generar procesos de mejora continua en el SGSI basadas en las evaluaciones del cumplimiento del SGSI y el alcance de los objetivos de seguridad de la información.

*Roles y Responsabilidades:* CEO – Gerente General(Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor).

*Alcance:* El SGSI y el programa de seguridad de la información.

## 11. Política de seguimiento por parte de la alta dirección

*Descripción:* Esta política señalará las actividades para permitir a la alta dirección tenga información sobre el status del SGSI y el programa de seguridad de la información durante su funcionamiento, evaluación y mejora continua.

*Objetivo:* Definir procedimientos y políticas que permitan dar seguimiento a la alta dirección de la empresa para evaluar el avance del programa de seguridad de la información, así como su operación, su evaluación y mejora continua durante periodos definidos de tiempo previamente acordados.

*Roles y Responsabilidades:* CEO – Gerente General(Evaluador), CTO – Gerente Técnico (Evaluador) y OSI – Oficial de Seguridad de la Información (Ejecutor).

*Alcance:* El SGSI y el programa de seguridad de la información.

# ANEXO 7

# MODELO OPERACIONAL Y MÉTRICAS DE LOS PROCESOS CLAVE

## Entregable 6 – Definición del modelo Operacional del SGSI y métricas de los procesos

Para el caso la empresa y sus necesidades actuales, se ha definido el siguiente modelo operacional basado en los marcos de referencia de NIST Cybersecurity Framework y Cobit 5, por lo que se ha definido el siguiente modelo:

### Modelo operacional

Para este modelo operacional y siguiendo la estructura del NIST Cybersecurity Framework maneja un modelo de funcionamiento y operación en 5 etapas. El Marco de Referencia de NIST cita que "El Marco está diseñado para complementar las operaciones empresariales y de seguridad cibernética existentes. Puede servir como base para un nuevo programa de seguridad cibernética o un mecanismo para mejorar un programa existente.." [1].

A su vez estas fases cuentan con subdivisiones del proceso o identificadas como prácticas asociadas, que permiten completar el objetivo que persigue la práctica. En este marco de referencia en específico se incluyen referencias informativas hacia otros marcos de referencia, tales como ISO 27001, COBIT, NIST801, ISA, etc., para el caso de este análisis se ha tomado las referencias hacia COBIT 5 y COBIT 5 con enfoque a la seguridad.

De este cruce entre el marco de referencia NIST y COBIT, del segundo marco de referencia se han tomado las métricas asociadas a las Referencias Informativas que el marco de referencia NIST incluye, es por eso que en las métricas asociadas se incluyen las referencias a los objetivos de gobierno y gestión de donde se obtuvieron.

[1] National Institute of Standards and Technology, NIST. NIST Cibersecurity Framework. Tomado de: https://www.nist.gov/document/frameworkesmellrev20181102mncleanpdf Pág. 20

**Etapa 1 – Identificar**

El modelo operacional arranca con la etapa de Identificar, en esta fase se busca desarrollar entendimiento sobre la organización, sus activos, información, personas, procesos, este detalle y algunas características de dicha fase se lo puede observar en la tabla 1.

| Proceso | Objetivo | Enfoque a la empresa | Prácticas asociadas | Métricas asociadas al proceso |
|---|---|---|---|---|
| **Identificar** | Desarrollar un entendimiento organizacional para gestionar los riesgos asociados a sistemas, personas, activos, datos y capacidades de la empresa. | Entender los diferentes componentes de la organización permitiría priorizar la aplicación de prácticas y políticas a los diferentes componentes empresariales y alcanzar los objetivos de seguridad planteados | Gestión de Activos<br>Entorno Empresarial<br>Gobernanza<br>Evaluación de Riesgos<br>Estrategias de Gestión de Riesgos<br>Gestión del riesgo de la cadena de suministro | Porcentaje de activos con clasificación de seguridad definida en el inventario de activos (BAI09.02)<br>Número de sistemas críticos de seguridad de la información cubiertos por el plan de recuperación de desastres. (DSS04.01)<br>Porcentaje de procesos y prácticas de seguridad de la información con trazabilidad a los principios de gobernanza (EDM01.02) |

*Tabla 1. Descripción del Proceso Identificar, las métricas seleccionadas y su contribución al modelo operacional*

De la tabla 1, las métricas que se presentan para este proceso y que se han considerado como más importantes hacen referencia a que tan bien se han identificados sus activos críticos, como esos sistemas críticos están cubiertos por otros procesos y como estos procesos se interrelacionan con el gobierno de IT. Existen muchas métricas en esta sección, sin embargo, se han priorizado estas 3 métricas debido a la claridad y facilidad de diagnóstico que pueden ofrecer.

**Etapa 2 – Proteger**

Luego de la fase de Identificar que ayuda a entender el entorno empresarial, es necesario empezar a definir cómo vamos a proteger los activos, servicios, información identificados en el primer paso, para esto la segunda fase puede proveer de algunos lineamientos importantes, dicha información se la puede ver en la tabla 2.

| Proceso | Objetivo | Enfoque a la empresa | Prácticas asociadas | Métricas asociadas al proceso |
|---|---|---|---|---|
| Proteger | Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. | Al cumplirse el objetivo, dichos servicios podrán mantener adecuados de funcionamiento y se minimizara los riesgos de interrupciones/fallas debido a eventos de seguridad | Gestión de identidad, autenticación y control de acceso.<br>Concienciación y capacitación.<br>Seguridad de los datos.<br>Procesos y procedimientos de protección de la información.<br>Mantenimiento.<br>Tecnología de protección. | Porcentaje de planes de acción de riesgo de I&T ejecutados según se diseñaron. (APO12.06)<br>Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad (DSS05.02)<br>Número de incidentes de disponibilidad (BAI04.05) |

*Tabla 2. Descripción del Proceso Proteger, las métricas seleccionadas y su contribución al modelo operacional*

En el caso de la tabla 2, se ha priorizado como métricas aquellas que permitan definir que tan bien el SGSI hace su trabajo, como en el caso de la primera que permite validar que tan bien fueron diseñados los planes de acción, la segunda métrica habla sobre el porcentaje de tiempo de indisponibilidad que puede asociarse a un SLA (Service Level Agreement) y finalmente la última métrica puede dar una idea de que tan bien o no se está protegiendo a los activos, servicios, usuarios, etc. y que tiene una relación estrecha con la segunda métrica.

**Etapa 3 – Detectar**

Cuando ya se encuentran las protecciones definidas e implementadas con sus respectivos planes y procesos; es necesario incluir actividades que permitan detectar eventos o incidentes de seguridad. Mientras más rápido se pueda detectar y tomar acción en un incidente de seguridad se puede manejar el impacto de dicho incidente de mejor manera. La tabla 3 contiene la información referente a la fase 3.

| Proceso | Objetivo | Enfoque a la empresa | Prácticas asociadas | Métricas asociadas al proceso |
|---|---|---|---|---|
| Detectar | Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad. | El poder detectar eventos de seguridad de forma temprana ayudará a mitigar el impacto de que un evento de seguridad pueda tener dentro de la empresa | Anomalías y Eventos. Monitoreo Continuo de la Seguridad. Procesos de Detección. | Número de vulnerabilidades descubiertas durante las pruebas. (DSS05.07) |
| | | | | Porcentaje de incidentes resueltos conforme a los SLA acordados. (DSS03.01) |
| | | | | Porcentaje de inventario de procesos críticos y controles clave completado. (DSS06.01) |

*Tabla 3. Descripción del Proceso Detectar, las métricas seleccionadas y su contribución al modelo operacional*

Las métricas seleccionadas para esta fase hacen referencia a que tan bien se han detectado y corregido algunos incidentes así y que tan bien se ha avanzado con la implementación de controles críticos. La métrica 1 señala que tan bien se han detectado nuevas vulnerabilidades, la métrica 2 hace referencia a que porcentaje de incidentes ha sido resuelto a tiempo lo que puede indicar la madurez de los procesos de detección y resolución de incidentes. Finalmente, la métrica 3 indica el avance en la implementación de controles en procesos críticos, lo cual puede señalar cual es el avance en el aseguramiento de componentes sensibles para el funcionamiento de la empresa.

**Etapa 4 – Responder**

La etapa 4 hace referencia a que pasos o procedimientos se ejecutan cuando se está enfrentando un incidente de seguridad, en esta fase las diferentes acciones que se puedan ejecutar permitirán manejar de mejor manera al impacto que puede tener el incidente. En esta etapa, también es posible medir que tan bien la empresa puede responder a incidentes de seguridad de la información. La tabla 4 contiene la información referente a esta fase.

| Proceso | Objetivo | Enfoque a la empresa | Prácticas asociadas | Métricas asociadas al proceso |
|---|---|---|---|---|
| Responder | Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad. | Un desarrollo adecuado de procesos y actividades en respuesta a eventos de seguridad podría mitigar riesgos y manejar el impacto que pudiera generar un incidente de seguridad | Planificación de la Respuesta<br>Comunicaciones<br>Análisis<br>Mitigación<br>Mejoras | Porcentaje del Riesgo de IT Mitigado. (APO12.06)<br>Tiempo medio para detectar incidentes de seguridad de la información. (DSS02.02)<br>Número de problemas de seguridad de la información identificados como falsos positivos. (DSS03.02) |

*Tabla 4. Descripción del Proceso Responder, las métricas seleccionadas y su contribución al modelo operacional*

Las métricas de estas fases hacen mención a la efectividad de cómo la empresa responde a los incidentes y para entender el contexto de las respuestas la métrica 1 señala cuando del riesgo a nivel de IT se encuentra mitigado, esto es un indicativo de cuantas medidas se han tomado sobre todo el entorno IT respecto a disminuir el riesgo, la segunda métrica hace mención a cuánto tiempo en promedio toma detectar los incidentes, esto sirve mucho para esta sección y pudiera ser considerada para la anterior. Finalmente, la tercera métrica, va enfocada a probar la definición y exactitud de los controles y evaluar su definición, mientras menor sea el número de la métrica 3 quiere decir que los controles están identificados con una mayor exactitud.

**Etapa 5 – Recuperar**

La etapa 5 hace referencia a que pasos o procedimientos se ejecutan para poder retornar a operar debido a un incidente de seguridad. Esta fase es clave ya que aquí se pone a prueba la resiliencia de la organización. Esta fase no solo abarca los procesos referentes a IT, sino también a cómo manejar las comunicaciones con entidades reguladoras, stakeholders y otras partes interesadas. La tabla 5 contiene la información referente a esta fase.

| Proceso | Objetivo | Enfoque a la empresa | Prácticas asociadas | Métricas asociadas al proceso |
|---|---|---|---|---|
| Recuperar | Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad. | El tener políticas y procedimientos que ayuden a reanudar las operaciones lo más pronto posible permiten disminuir la indisponibilidad debido a incidentes de seguridad. | Planificación de la recuperación.<br>Mejoras.<br>Comunicaciones. | Tiempo medio para resolver incidentes de seguridad de la información. (DSS02.05)<br><br>Tiempo promedio entre la identificación de los problemas de cumplimiento externo y su resolución. (MEA03.02) |

*Tabla 5. Descripción del Proceso Recuperar, las métricas seleccionadas y su contribución al modelo operacional*

Para esta fase, se han seleccionado 2 métricas que pueden ayudar a evaluar el comportamiento. La primera métrica al igual que en la fase anterior hace referencia al tiempo medio, en este caso se mide el tiempo para resolver los incidentes de seguridad. Este tiempo puede volverse un indicativo de la madurez de los procesos de recuperación ya que a menor tiempo tome levantar las operaciones indicaría que sus procesos se encuentran mejor definidos y ejecutados. La segunda métrica hace referencia a las comunicaciones que la empresa debe hacer a entidades de cumplimiento, este tiempo se toma en cuenta para notificar a entidades de control sobre los incidentes y su resolución, esto es fundamental en los casos que se manejan entidades como superintendencias u otras organizaciones de control.

# ANEXO 8

# PLANES DE MEJORA

## Entregable 8 - Programa de mejora continua del SGSI

En el presente entregable, se han definido los planes de Mejora que se han obtenido de los entregables "Metodología y Evaluación SGSI" y "Analisis de Activo Crítico" de donde se desprendieron planes de mejoras.

Estos planes de mejora han sido consolidados en una sola calendarización definiendose fases según el siguiente esquema:

Fase 1: 01/12/2021 - 30/03/2022
Fase 2: 01/04/2022 - 31/07/2022
Fase 3: 01/06/2022 - 30/12/2022

Los planes cuentan con un presupuesto estimado en el área, y los mismos cuentan con un estado. La mayoria de los planes ya expuestos sen encuentran como "Aprobados", sin embargo existen planes que se encuentran "En Revisión".

| Código Plan | Plan de Acción | Categoria del Proyecto | Fuente | Objetivos del Plan de Acción | Desarrollo del Plan | Fecha Inicio | Fecha Fin | Responsable(s) | Presupuesto | Estado | Fase |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AVAC-GB-01 | Elaborar un Plan de recuperación de desastres como parte de las políticas de continuidad del negocio. | Implementación | Analisis de Riesgos | Obtener un plan de recuperación de desastres que se encuentre apegado a las necesidades y a la realidad de la empresa. | Definir un marco de referencia para la elaboración del plan, analizar las actividades fundamentales para generar la recuperación de las operaciones de la empresa, definir las notificaciones de servicio a los clientes que hayan sido afectados. | 1/12/2021 | 30/3/2022 | Gerente Técnico<br>Oficial de Seguridad de la información | 6000 | Aprobado | Fase 1 |
| AVAC-GB-02 | Elaborar un Plan de Impacto del Negocio de los componentes de IT como parte de las políticas de continuidad del negocio. | Implementación | Analisis de Riesgos | Obtener un plan de Impacto al negocio que haga referencia a los componentes IT críticos para la empresa | Definir un análisis de activos críticos. Definir el impacto en las operaciones que estos activos críticos tienen. Determinar las perdidas financieras que conllevaría la falla de ese equipo. | 1/12/2021 | 30/3/2022 | Gerente Técnico<br>Oficial de Seguridad de la información | 6000 | Aprobado | Fase 1 |
| AVAC-HW-01 | Generar una política de renovación de soporte y garantía para los equipos críticos de IT. | Refuerzo | Analisis de Riesgos | Disponer de lineamientos para la renovación de las garantías y soporte técnico de los componentes de hardware críticos de la empresa. | Definir un listado de proveedores conocidos para la organización. Solicitar certificados y referencias a los proveedores. | 1/4/2022 | 30/4/2022 | Gerente Técnico<br>Gerente Financiero | 4500 | Aprobado | Fase 2 |
| AVAC-HW-02 | Definir un plan de mejora del monitoreo del estado del firewall a través de herramientas que brinden mejor detalle del funcionamiento del hardware. | Prevención | Analisis de Riesgos | Disponer de lineamientos y procesos para mejorar las capacidades actuales del monitoreo en base a herramientas que ayuden a manejar el monitoreo del hardware crítico. | Definir la necesidad de implementar una solución de monitoreo. Definir las métricas de monitoreo necesarias. Definir calendarización de reportes. | 1/5/2022 | 31/7/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1500 | Aprobado | Fase 2 |
| AVAC-HW-03 | Definir un plan de renovación de los componentes de IT. Definir un plan de contingencia para componentes críticos de IT. | Refuerzo | Analisis de Riesgos | Definir las necesidad de redundancia y alta disponibilidad para componentes de IT críticos, así como definir el tiempo que las adquisiciones se mantengan operativas en la empresa. | Definir la vida útil de los componentes IT. Definir la reutilización de los componentes IT si aplica. Definir un roadmap de adquisiciones como parte de las renovaciones de IT. | 3/1/2022 | 28/2/2022 | Gerente General,<br>Gerente Técnico,<br>Gerente Financiero. | 2000 | Aprobado | Fase 1 |
| AVAC-HW-04 | Definir una política de mantenimiento preventivo de los componentes de IT | Prevención | Analisis de Riesgos | Definir las actividades referente a los mantenimientos preventivos de los componentes críticos tanto físicamente como lógicamente. | Definir el calendario de mantenimiento de los componentes de IT. Definir las actividades de los mantenimientos. Definir alcances adicionales como actualización de sistema operativo, desactivación de funcionalidades que no se usan. Incluir la aplicación de las recomendaciones de fabrica respecto a la configuración de los equipos | 1/3/2022 | 1/4/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 0 | Aprobado | Fase 2 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AVAC-HW-05 | Definir un plan de monitoreo de las condiciones operativas del Data Center | Prevención | Analisis de Riesgos | Señalar las actividades referentes al monitoreo ambiental del data center | Definir la frecuencia de mediición de las condiciones operativas del data center. Definir las acciones a tomarse en caso que haya desviaciones de las condiciones regulares. | 1/6/2022 | 1/8/2022 | Gerente Técnico<br>Personal de IT. | 500 | Aprobado | Fase 3 |
| AVAC-HW-06 | Definir un plan de actualización de la póliza de seguros en casos de que se adquieran nuevos elementos de IT. | Refuerzo | Analisis de Riesgos | Definir los lineamientos para la adquisición de polizas de seguros y la definiciónd e que equipos deben contar con estas pólizas. | Definir las polizas a ser adquiridas. Definir los equipos que se incluyan en las polizas. Definir las condiciones respecto a la aplicación de las pólizas. | 1/5/2022 | 1/7/2022 | Gerente Técnico<br>Gerente Financiero | 2500 | Aprobado | Fase 2 |
| AVAC-HW-07 | Definir un plan de registro de visitas de clientes, proveedores y un registro de video de acceso a las oficinas. | Prevención | Analisis de Riesgos | Definir procedimientos para documentar las visitas de proveedores a la oficina, incluir la grabación de partes vitales como el acceso al data center. | Definir las areas sociales de la oficina. Definir las areas sensibles de la organización en donde se deba instalar camaras. | 1/10/2022 | 1/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1500 | En revisión | Fase 3 |
| AVAC-HW-08 | Definir una política de registro de acceso a la data center y documentar estos accesos. | Prevención | Analisis de Riesgos | Definir procedimientos, lineamientos para registrar el acceso al data center e identificar a los visitantes del data center. | Definir un formato para registro de las visitas. Definir procesos para registrar el personal que van a visitar el data center y las actividades. | 1/6/2022 | 1/7/2022 | Gerente Técnico<br>Oficial de Seguridad de la información | --- | Aprobado | Fase 3 |
| AVAC-SO-01 | Definir una política de respaldos de configuraciones del firewall. | Prevención | Analisis de Riesgos | Definir procedimientos para obtener un backup de la configuración del firewall, ya sea de forma manual o automática. | Definir la periodicidad de los respaldos. Definir los pasos para obtener la copia de seguridad. Definir en donde se almacenarán los respaldos. | 1/6/2022 | 1/7/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 500 | Aprobado | Fase 3 |
| AVAC-SO-02 | Definir una política de control de cambios para la infraestructura de IT, incluir una calendarización y documentación sobre los cambios a ejecutarse. | Refuerzo | Analisis de Riesgos | Definir los lineamientos para mantener un registro de cambios sobre la infraestructura de IT así como los días de ejecutarse estos cambios. | Definir horarios para los trabajos en la infraestructura. Definir el procedimiento de registro del control de cambios. Definir los formatos para aprobaciones de cambios. Definir el proceso de aprobación de cambios. | 1/7/2022 | 1/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| AVAC-SO-03 | Reforzar los conocimientos del personal por medio de cursos y capacitaciones sobre el firewall de la empresa. | Capacitación | Analisis de Riesgos | Definir capacitaciones las cuales refuercen los conocimientos de los encargados de seguridad e IT. | Definir un listado de cursos para cada persona que maneja equipos de IT durante el año 2022. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Gerente Financiero<br>Oficial de Seguridad de la Información<br>Personal de IT | 1000 | Aprobado | Fase 2 |
| AVAC-SO-04 | Implementar un plan de certificación del personal que administra el firewall, que incluya cursos del fabricante del firewall y la certificación del personal. | Capacitación | Analisis de Riesgos | Definir un plan de cursos de certificación del personal que adminsitra el firewall. | Definir un listado de cursos referentes a administración de firewalls de la marca de los equipos de la empresa. Definir las certificaciones que se van a rendir, definir los costos de estas certificaciones. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Gerente Financiero<br>Oficial de Seguridad de la Información<br>Personal de IT | 1500 | Aprobado | Fase 2 |
| AVAC-SO-05 | Implementar una política de gestión y análisis de logs para almacenar una copia de los logs en otra herramienta y por mas de 15 días. | Implementación | Analisis de Riesgos | Definir los lineamientos, planes de acción y periodicidad del almacenamiento de los logs para sus análisis. | Definir el sitio de almacenamiento de los logs. Definir el tiempo de retención de los logs. Definir la periodicidad de cuando se respladen los logs. Definir el responsable de estas actividades. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 500 | Aprobado | Fase 2 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AVAC-SO-06 | Implementar una política de análisis y gestión de vulnerabilidades para componente críticos de IT. | Prevención | Analisis de Riesgos | Definir las actividades necesarias para evaluar vulnerabilidades en los componentes críticos así como la peridicidad de estos análisis. | Definir los métodos o herramientas para el análisis de vulnerabilidades. Definir un cronograma de análisis. Definir los planes de acción en base a las vulnerabilidades que se encuentren. | 15/7/2022 | 30/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 700 | En Revisión | Fase 3 |
| AVAC-SO-07 | Reforzar la política de gestión de contraseñas de los componentes de IT en la empresa para que se incluyan periodos para los cambios de las contraseñas de administración. | Prevención | Analisis de Riesgos | Definir lineamientos para mejorar la gestión de las contraseñas, así como definir periodicidad e indicación de contraseñas al personal que lo requiera basado en sus actividades. | Definir esquemas de contraseñas. Definir calendarización para el cambio de contraseñas. Definir responsables del cambio de contraseñas. | 1/7/2022 | 1/10/2022 | Gerente Técnico<br>Personal de IT. | --- | Aprobado | Fase 3 |
| SGSI-4-1-a | Actualizar la definición de las partes interesadas del SGSI tomando en contexto la realidad actual de la empresa | Cumplimiento Norma | Análisis SGSI | Actualizar la definición de las partes interesadas para brindar un mejor conocimiento de la organización y su contexto. | Actualizar la definición de las partes interesadas, los requisitos de las partes interesadas y el contexto interno y externo de la empresa. Reforzar y actualizar la definición de interfaces y dependencias con otras organizaciones. Actualizar la documentación referente al alcance del SGSI. | 1/12/2021 | 30/12/2021 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-4-2-a | Actualizar el SGSI para cubrir las necesidades actuales de la empresa | Cumplimiento Norma | Análisis SGSI | Actualizar y reforzar el SGSI para que sea establecido acorde a las necesidades actuales de la empresa. | Definir las necesidades actuales de la empresa, definir como el SGSI aopya a las actividades de la empresa. Definir un procedimiento para mantener y proveer una retroalimentación para la mejora continua en cuanto a cubrir las necesidades de la empresa por medio del SGSI. | 1/12/2021 | 30/12/2021 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-5-1-a | Ajustar la política de seguridad y sus objetivos para que estos sean compatibles con la dirección estratégica de la organización. | Refuerzo | Análisis SGSI | Revisar y reforzar las políticas de seguridad, sus objetivos y que estas políticas esten alineadas a los objetivos de la organización. | Actualizar los objetivos empresariales. Actualizar el lsitado de políticas de seguridad. Definir una matriz entre los objetivos de la empresa y las políticas de seguridad de la información. | 1/4/2022 | 1/5/2022 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 2 |
| SGSI-5-1-b | Crear un plan de comunicación sobre el seguimiento de las actividades referentes al SGSI y sus ajustes. | Cumplimiento Norma | Análisis SGSI | Crear un plan de comunicaciones que informe de las actividades respecto al SGSI y sus avances. | Crear un cronograma de comunicaciones. Definir las actividades a ser comunicadas. Definir los responsables de comunicar estos avances. Definir un plan de aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-5-1-c | Reforzar el plan de seguimiento de la eficacia de los controles previsto en el SGSI en donde se incluyan factores de medición. | Mejora Continua | Análisis SGSI | Actualizat el plan de segumiento de la eficacia de los controles definidos el SGSI. | Definir las métricas que se asociarán a los controles. Definir los umbrales de las métricas. Definir la periodicidad de cuando se tomen las mediciones. Definir un formato de documentación de las mediciones. Medir y documentar los resultados obtenidos en el plan de seguimiento de la eficacia de los controles previsto en el SGSI. Incluir un listado de los documentos relacionados con las mejoras continuas que se definan. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-5-2-a | Generar un documento de compromiso de cumplimiento de mejora continua del SGSI. | Mejora Continua | Análisis SGSI | Actualizar y generar un nuevo documento de compromiso de cumplimiento de requisitos aplicables respecto a la seguridad de la información. Se debe incluir comprobación del cumplimiento del compromiso. | Generar un nuevo documento de compromiso de cumplimiento de requisitos aplicables respecto a la seguridad de la información. Generar un formato de constancia sobre el cumplimiento del compomiso de mejora continua del SGSI. | 1/12/2021 | 30/12/2021 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-5-2-b | Generar un plan de documentación del SGSI que incluya versionamiento y actualizaciones periodicas | Cumplimiento Norma | Análisis SGSI | Definir un plan de documentación para el manejo de la documentación del SGSI. | Definir un sistema de versionamiento de esta documentación. Definir los responsables de los cambios de la documentación. Definir el proceso de aprobación de la documentación. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-5-2-c | Generar un plan de comunicación sobre las políticas que tiene el SGSI en la empresa y definir un calendario de comunicación | Cumplimiento Norma | Análisis SGSI | Crear un plan de comunicaciones que informe de las políticas definidas en el SGSI, así como su aplicación dentro de la empresa. | Crear un cronograma de comunicaciones. Definir las actividades a ser comunicadas. Definir los responsables de comunicar estos avances. Definir un plan de aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-5-2-d | Definir un plan de almacenamiento y distribución de la documentación del SGSI. | Cumplimiento Norma | Análisis SGSI | Definir un plan de almacenamiento de la documentación del SGSI dentro de la organización. | Definir la ubicación en donde se va a almacenar la documentación del SGSI. Definir los permisos de lectura/escritura que les serán asignados a los diferentes miembros de la organización. Definir los planes de respaldos de la documentación. Incluir en el plan de almacenamiento las instrucciones para la identificación de la documentación externa | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-5-3-a | Realizar una revisión interna luego de 6 meses de haberse implementado el nuevo SGSI en la organización.para definir el estado del SGSI | Mejora Continua | Análisis SGSI | Definir un plan de revisión interna luego de haberse modificado el SGSI para definir un nuevo estado del SGSI. | Definir un cronograma de revisiones internas para actualizar el estado del SGSI. Definir los responsables de la revisión del SGSI. Definir el formato de presentación del estado del SGSI. | 1/6/2022 | 1/7/2022 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-6-1-a | Reforzar la definición de riesgos de la empresa y la evaluación de riesgos. | Refuerzo | Análisis SGSI | Actualizar el listado de riesgos considerados para la operación de la empresa en base a la situación actual de la empresa. | Levantar los riesgos asociados a la operación del call center. Definir el apetito al riesgo con respecto a las nuevas actividades a ejecutarse. Definir los riesgos asociados al trabajo en las nuevas condiciones. | 1/12/2021 | 30/12/2021 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-6-1-b | Definir un plan de seguimiento y mejora de tratamiento de riesgos. | Mejora Continua | Análisis SGSI | Al identificarse el listado de riesgos, se debe definir como se hará seguimiento a la gestión de riesgos y se definirá como generar mejora continua en esta gestión de riesgos. | Se debe definir planes de tratamiento de riesgos. Se debe definir planes de medición de la gestión de riesgos. Se deben definir un cronograma de revisión de las métricas. Se deben definir planes de mejora en base a las métricas detectadas. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-6-1-c | Definir una política de manejo de documentación sobre los riesgos que se consideraron para el SGSI. | Cumplimiento Norma | Análisis SGSI | Definir como se realizará el manejo de la documentación referente a la gestión del riesgo, su tratamiento y la medición de sus metricas, asi como la documentación de las oportunidades de mejora continua. | Se debe definir los formatos para documentar los riesgos, los planes de tratamiento de riesgos. Se debe definir los formatos sobre los informes de medición de los riesgos. Se debe definir el formato de la documentación de las oportnuidades de mejora o cambios sobre los riesgos. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-6-1-d | Reforzar la definición de los controles necesarios dentro de la empresa y apegar los controles al anexo A. | Refuerzo | Análisis SGSI | Actualizar la definición de las políticas del Anexo A para ajustarlos con las nuevas definiciones de la empresa en cuanto a sus actividades. | Realizar un levantamiento de los controles definidos dentro de la empresa. Evaluar si los controles cumplemn con los objetivos de la empresa. Definir nuevos controles en caso de no tener controles implementados. Tomar en consideración la actualización de la declaración de aplicabilidad. | 1/4/2022 | 1/6/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 2 |
| SGSI-6-1-e | Reforzar la declaración de aplicabilidad conforme a las nuevas responsabilidades de la empresa. | Refuerzo | Análisis SGSI | Actualizar la política de aplicabilidad sobre los controles del Anexo A que se utilizarán para la evaluación de la empresa en base a sus objetivos y actividades. | Actualizar la política de aplicabilidad considerando las nuevas actividades de la empresa. | 1/4/2022 | 1/6/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 2 |
| SGSI-6-2-a | Definir nuevos objetivos de seguridad que se encuentren acordes a las políticas de seguridad de la información. | Refuerzo | Análisis SGSI | Actualizar la definición de los objetivos de seguridad en base a las nuevas actividades de la empresa e incluir nuevos objetivos de seguridad. | Evaluar los objetivos de seguridad que se deben obtener con las nuevas actividades de la empresa. Definir las métricas para evaluar el avance del cumplimiento de los nuevos objetivos de seguridad. | 1/12/2021 | 30/12/2021 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |
| SGSI-6-2-b | Actualizar la planificación existente incluyendo las acciones necesarias para alcanzar los objetivos de seguridad de la información. | Refuerzo | Análisis SGSI | Actualizar la planificación sobre las actividades, evaluaciones y seguimiento existente. | Con los nuevos objetivos de seguridad definidos, se debe ajustar las actividades, políticas, procesos necesarios para cumplir con estas nuevos objetivos y se debe definir una estimación de tiempo para dichas actividades. | 1/12/2021 | 30/12/2021 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-7-1-a | Reforzar y Actualizar los recursos necesarios para cumplir con el nuevo SGSI. | Prevención | Análisis SGSI | Definir que recursos adicionales se necesitan para cumplor con los nuevos objetivos de seguridad. | Definir los recursos en equipamiento IT necesario para el cumplimiento de objetivos. Definir los esquemas de funcionamiento de los componentes IT: | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | 8000 | Aprobado | Fase 1 |
| SGSI-7-2-a | Definir un plan de asignación de responsabilidades referente a la participación en las actividades del SGSI | Prevención | Análisis SGSI | Definir un plan de asignación de actividades y sus responsables, tomando en cuenta las actividades definidas para el SGSI. | Definir el personal técnico que estará a cargo de la gestión de los equipos IT. Definir los responsables del seguimiento, ajuste de configuraciones en los activos de IT. Definir responsables para la medición del alcance de los objetivos de seguridad de la información. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-7-3-a | Definir un plan de concienciación sobre las políticas y los objetivos de seguridad de la información, así como sus beneficios y las implicaciones de no cumplir con los objetivos. | Prevención | Análisis SGSI | Definir un plan de concienciamiento dentro de la organización sobre la importancia de la seguridad de la información, el SGSI y sus políticas y las mediciones que se realizarán para el SGSI. | Definir el contenido de la concienciaciión. Definir el número de sesiones necesarias para la concienciamiento. Definir los responsables y el auditorio de las charlas. Definir acciones adicionales para fomentar la concienciación como envio de emails sobre consejos de seguridad. | 1/4/2022 | 1/6/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 2 |
| SGSI-7-4-a | Elaborar un esquema de comunicación que incluya que se debe comunicar, cuando comunicar, a quien comunicar, quien debe comunicar y que procesos se deben utilizar para comunicar. | Cumplimiento Norma | Análisis SGSI | Se debe definir un esquema para el manejo de las comunicaciones que involucre la generación de un proceso de comunicación. | Se debe definir los responsables de hacer las comunicaciones. Se debe definir el formato de las comunicaciones. Se debe definir el proceso de comunicación. Se debe definir los responsables de la elaboración y aprobación de las comunicaciones. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-7-5-a | Definir un listado de documentación necesaria para medir la eficacia del SGSI. | Cumplimiento Norma | Análisis SGSI | Definir un listado de los documentos/informes necesarios que incluyan métricas y que ayuden a realizar la medición de las actividades del SGSI. | Definir los informes necesarios para medir el cumplimiento y desempeño del SGSI. Definir el calendario de entrega de los informes para consolidación. Definir un cronograma para entregar la consolidación. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-7-5-b | Definir un reglamento sobre el formato de la documentación y los requisitos minimos que esta documentación debe tener. | Cumplimiento Norma | Análisis SGSI | Definir las acaracteristicas respecto a la documentación y su contenido, y que esta documentación cumpla requisitos mínimos para el uso en le SGSI. | Definir un listado de campos que llos formatos deben tener. Definir un reglamento sobre el contenido de la documentación, así como su actualización. Reforzar el proceso de aprobación manteniendo la revisión de idoneidad y adecuación. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-7-5-c | Definir un plan de protección de la documentación que incluya acciones en caso de perdida de confidencialidad, el uso inadecuado y la perdida de integridad. | Implementación | Análisis SGSI | Definir un plan para proteger la documentación del SGSI y definir acciones en caso de que se pierda la confidencialidad, la integridad y el uso inadecuado. | Definir esquemas para proteger la documentación . Definir escenarios para determinar acciones para el uso indebido, perdida de confidencialidad y perdida de integridad. Documentar estos planes. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-9-2-a | Definir un plan de auditoria para el SGSI, sus politicas y sus resultados | Implementación | Análisis SGSI | Definir los lineamientos sobre las auditorias internas y externas, asi como el tratamiento a las observaciones y no conformidades en el SGSI y las políticas de seguridad de la información. | Definir un cronograma para las auditorias internas, auditorias externas. Definir un plan de acción respecto a los resultados de la auditoria, así como el tratamiento de las no conformidades, las acciones correctivas del SGSI y de las políticas de seguridad de la información. | 1/4/2022 | 1/6/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | 7000 | Aprobado | Fase 2 |
| SGSI-A1-A5-1-1 | Actualizar el documento de la política de seguridad de la información. | Refuerzo | Análisis SGSI - Anexo A | Actualizar las politicas de seguridad de la información considerando la definición actualizada de los objetivos de seguridad de la información. | Obtener los nuevos objetivos de seguridad de la información. Actualizar las políticas de seguridad de la información para que estas ayuden al cumplimiento de los objetivos de seguridad de la información. Definir nuevas métricas para las políticas de seguridad de la información. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-A1-A6-1-1 | Generar un plan de asignación interna respecto a la definición, seguimiento y mantenimiento de las políticas de seguridad de la información. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir la asignación de un responsable que coordine y supervise las actividades referente a las políticas de seguridad de la información y al seguimiento de las mismas. Definir el rol de Oficial de seguridad de la información y sus funciones. | Definir un coordinador de seguridad de la información. Definir las funciones del cargo de coordinador de seguridad de la información. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-A1-A6-1-2 | Definir una política de procesamiento de información que incluya autorizaciones. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir un proceso para autorizar cambios en las políticas de seguridad de la información, asi como cualquier cambio en IT que afecte a la seguridad de la información. | Definir un formato de autorizaciones para cambios que afecten a la sefuridad de la información. Definir un responsable para autorizar los cambios que afecten a las políticas de seguridad de la información o sus métricas. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-A1-A6-1-3 | Reforzar la documentación sobre los acuerdos de confidencialidad con clientes y proveedores. | Refuerzo | Análisis SGSI - Anexo A | Actualizar la documentación sobre los acuerdos de confidencialidad que se manejan con los clientes y proveedores. | Definir una bitácora o historial de los acuerdos de confindencialidad que se manejan con los clientes y proveedores. Actualizar los acuerdos de confidencialidad para que se ajusten a las nuevas necesidades de la empresa y a la ley vigente. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A6-1-4 | Definir una política de contacto con las autoridades para los temas de seguridad de la empresa. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir un cronograma de reuniones internas entre los encargados de seguridad de la información y las gerencias de la empresa. | Definir un cronograma para las revisiones de las gerencias respecto a la revisión de los avances de seguridad de la información. Definir un proceso de documentación de resumen de los temas tratados dentro de las reuniones. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-A1-A6-1-5 | Definir una política de contacto con grupos de interés especiales en los temas de seguridad de la información. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir los lineamientos para establecer contactos con grupos de interes especiales y generar un entendimiento común sobre seguridad de la infromación. | Definir un calendario para reuniones con los grupos de inyteres especiales. Definir un formato para documentar los temas tratados con los grupos de interes especiales. | 1/4/2022 | 1/6/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 2 |
| SGSI-A1-A6-2-1 | Definir un análisis de riesgos referente al trato con partes externas, clientes, proveedores y terceras partes. | Prevención | Análisis SGSI - Anexo A | Definir los riesgos para la empresa respecto al trato con partes externas, proveedores y terceras partes y que afecten a la seguridad de la información. | Definir los riesgos asociados a la interacción de la empresa con terceros. Definir las acciones referentes a la gestión de riesgos con terceros. Definir planes de acción para el tratamiento del riesgo. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-A1-A7-1-1 | Generar una política de contratación en donde se documenten los roles y responsabilidades de los cargos de la empresa, así como los perfiles de acceso a la información en base a ese cargo. | Implementación | Análisis SGSI - Anexo A | Definir una política de contratación en donde se definan los roles y responsabilidades de los empleados, asi como el nivel de acceso a la información de la empresa. | Definir una politica de acceso a la información basado en los cargos de la empresa. Incluir los requerimientos sobre conocimiento de seguridad de la información. Definir las responsabilidades frente a sus superiores sobre el manejo de la información. Definir un código disciplinario. | 1/7/2022 | 1/9/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | En Revisión | Fase 3 |
| SGSI-A1-A8-1-1 | Actualizar el inventario tecnológico. | Refuerzo | Análisis SGSI - Anexo A | Actualizar el inventario tecnológico e incluir la fecha de adquisición de ese activo tecnológico. Definir el registro de los prestamos y devoluciones de los activos tecnológicos. | Definir una matriz de los activos tecnológicos que incluyan la fecha de adquisición. Definir los responsables de los activos de información que se hayna asignado. Definir formatos para asignación de activos. Definir formatos para devolución de activos. Definir bitácoras para registrar las devoluciones y prestamos. | 1/7/2022 | 1/9/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A8-1-2 | Definir una política de uso aceptable de los activos tecnológicos de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir las consideraciones que se deben tener al utilizar equipos de IT provistos por la empresa. | Definir las condiciones de uso y los propositos de uso del equipamiento existente en la empresa. Automatizar en lo posible los controles que ayuden a que se cumplan con los lineamientos definidos de uso aceptable. | 1/7/2022 | 1/9/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información | --- | En Revisión | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A8-2-1 | Documentar la directriz de clasificación de información existente y ampliarla a las demás áreas de la empresa. | Prevención | Análisis SGSI - Anexo A | Documentar la directriz de clasificación de información existente y ampliarla a las demás áreas de la empresa. Asi mismo definir esquemas de etiques para clasificar la información. | Actualizar la directriz de clasificación de información. Incluir las actividades de etiquetado de la información en base a categorías. Documentar los permisos de acceso de los usuarios en base a las directriz definida. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A8-2-2 | Extender la política de gestión medios extraíbles y soportes de almacenamiento a toda la organización en base a las necesidades de la empresa. | Refuerzo | Análisis SGSI - Anexo A | Extender la gestión de medios extraíbles y soportes de almacenamiento a toda la organización en base a las necesidades de la empresa. | Actualizar la política de gestión de medios extraibles y soportes de información para abarcar a toda la empresa. Definir procedimientos para limpiar y reutilizar medios extraibles. Definir procesos de limpieza de soportes de almacenamiento de información. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A9-1-1 | Se debe definir una política de control de acceso a recursos utilizando usuarios temporales y autenticacion temporal. | Prevención | Análisis SGSI - Anexo A | Definir una política de generación de usuarios temporales para acceder a los recursos de la empresa. | Definir procesos de compartición de documentos digitales, la duración del permiso, definir el tipo de información que se puede transmitir de esta forma. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A9-2-1 | Generar una política de gestion de usuarios y contraseñas. | Prevención | Análisis SGSI - Anexo A | Generar una política de gestion de usuarios y contraseñas en donde se señalen los lineamientos de seguridad de los usuarios y contraseñas. | Definir como se definiran los nombres de usuario dentro de la organización. Definir los esquemas de las contraseñas. Definir la periodicidad del cambio de contraseñas. | 1/4/2022 | 1/6/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 2 |
| SGSI-A1-A9-3-1 | Definir una política de uso de esquemas de autenticación mas robustas como uso de biométrica o doble factor de autenticación. | Refuerzo | Análisis SGSI - Anexo A | Definir esquemas de autenticación mas robustos para el acceso a recursos que conlleven un mayor nivel de sensibilidad. | Definir que esquemas de autenticación adicionales se implementarán para el acceso a información clasificada como sensible o crítica. Definir que sistemas tendrán esta configuración. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A9-4-1 | Definir una política de restricción de acceso a sistemas y aplicaciones basada en permisos y usuarios. | Refuerzo | Análisis SGSI - Anexo A | Definir las consideraciones para que determinados usuarios puedan utilizar herramientas de la empresa, asi como delimitar el acceso a la información. | Definir el listado de usuarios existentes. Definir los permisos de los usuarios hacia las aplicaciones. Definir los permisos de los usuarios para el acceso a los recursos de la empresa. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A9-4-2 | Definir una política de uso de software y permisos de sistema operativo dependiendo de los usuarios. | Implementación | Análisis SGSI - Anexo A | Definir los permisos que cada usuario del sistema operativo puede ejecutar sobre el mismo. | Definir el formato y permisos de los usuarios del sistema operativo. Definir los perfiles de acceso que se asignara a cada persona de la empresa. Definir los roles que tendrán permiso de instalación de software en sus máquinas. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A9-4-3 | Definir una política de protección de acceso al repositorio de código fuente de los programas entregados. | Implementación | Análisis SGSI - Anexo A | Definir los permisos necesarios para los usuarios que acceden a los repositorios de código fuente en la empresa. | Definir medidas de control de acceso lógico al repositorio de codigo fuente basado en usuarios, contraseñas y permisos. Definir medidas de protección y respaldo del repositorio de códgo fuente. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A10-1-1 | Crear una nueva política de gestión de claves en donde se incluyan las prácticas de seguridad ya existentes y nuevas consideraciones de seguridad. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos sobre las contraseñas que se configurarán dentro de los equipos de IT de la organización y su gestión. | Definir un esquema de definición de contraseñas. Definir el listado de los equipos que utilizaran esta definición de contraseñas. Definir la periodicidad de las contraseñas. Definir un cronograma de actualización de contraseñas. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A11-1-1 | Definir una política de acceso, seguridad física de la oficina y sus diferentes áreas para colaboradores y proveedores. | Implementación | Análisis SGSI - Anexo A | Definir las consideraciones sobre seguridad física a las áreas sensibles de la emptresa en cuanto a seguridad de la información. | Reconocer las áreas sensibles en la empresa en cuanto a acceso a fuentes de información. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 800 | Aprobado | Fase 3 |
| SGSI-A1-A11-2-1 | Incluir en la política de acceso, seguridad física de la oficina las protecciones que deben tener considerados los equipos informáticos y de IT. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos adicionales respecto a la consideración del aseguramiento de las áreas en donde funcionan o se almacenan equipos IT. | Definir los controles necesarios para asegurar las áreas en donde se almacene o procese información sensible de la empresa y que sean equipos de IT. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 800 | Aprobado | Fase 3 |
| SGSI-A1-A11-2-2 | Definir un plan de mantenimiento y mejora respecto a la instalación de suministro y sus contingencias como el UPS. | Mejora Continua | Análisis SGSI - Anexo A | Definir las condiciones que se deben tener en cuenta para mantener funcional y operativo el suministro de energía electrica y sus medidas de contingencia. | Definir las condiciones de funcionamiento de los equipos IT de la empresa en cuanto a temas de energía. Definir un cronograma de mantenimiento de las contingencias de interrupción del suministro de energía electrica. Definir los niveles de funcionamiento adecuados del UPS. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 500 | Aprobado | Fase 3 |
| SGSI-A1-A11-2-3 | Definir un plan de actualización, mantenimiento del cableado estructurado y organización en los rack del data center. | Mejora Continua | Análisis SGSI - Anexo A | Definir las condiciones que se deben tener en cuenta para mantener funcional y operativo la conectividad de la empresa y sus medidas de contingencia. | Definir las condiciones de funcionamiento del cableado estructurado. Definir la edad máxima del cableado de seguridad. Definir un plan de actualización y mantenimiento del cableado estructurado. Definir un esquema de peinado de los cables de energía y de red que se utilizan en el data center. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1200 | Aprobado | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A11-2-4 | Definir un plan de mantenimiento, actualización y reasignación de equipos y medios; | Mejora Continua | Análisis SGSI - Anexo A | Definir los lineamientos para generar reasignación de equipos y componentes asignados al personal de la empresa. Definir una política para el mantenimiento de pólizas de los equipos. | Definir periodos de vida util de los equipos adquiridos. Definir esquemas de revisión y generación de informes del estado de los equipos. Definir su asignación dentro y fuera de la empresa e incluir garantias o seguros. | 1/5/2022 | 1/7/2022 | Gerente Técnico<br>Gerente Financiero | --- | Considerado con otro plan | Fase 2 |
| SGSI-A1-A11-2-5 | Actualizar y reforzar la política de reutilización de medios e incluir procedimientos para la retirada segura de dispositivos de almacenamiento. | Refuerzo | Análisis SGSI - Anexo A | Definir los lineamientos para la reutilización de medios de almacenamiento dentro y fuera de la empresa, asi como su reutilización. | Definir procesos para extraer medios de lamacenamiento de forma segura de componentes que cumplieron su vida util y se pueda reutilizar | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1500 | En Revisión | Fase 3 |
| SGSI-A1-A11-2-6 | Definir una política para el manejo de equipos informáticos de usuarios desatendidos . | Prevención | Análisis SGSI - Anexo A | Definir una política para el manejo de equipos informáticos de usuarios desatendidos y adicionar una política de puesto de trabajo despejado y bloqueo de pantalla de forma automática. | Definir las condiciones que deben cumplirse para manejar equipos con usuarios desatendidos. Definir políticas de bloqueo de pantallas. Definir acciones cuando un colaborador va a dejar su puesto de trabajo momentaneamente. | 1/5/2022 | 1/7/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 2 |
| SGSI-A1-A12-1-1 | Definir una política de documentación de la operación tales como apagado/encendido de equipos. Gestion de cambios y Gestión de capacidades | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir una política que defina los lineamientos de la operación de la empresa tales como apagado/encendido de equipos, la gestión de cambios en los equipos y la gestión de capacidades de los equipos. | Definir la planificación para el pagado, encendido de los equipos. Definir un plan para gestionar controles de cambio sobre los equipos que funcionan en el data center. Definir un esquema de monitoreo de las capacidades de los componentes de IT que funcionan en el data center. Definir un formato de evaluación de capacidades de los componentes del data center. Definir un proceso de aumento de capacidades. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 3 |
| SGSI-A1-A12-2-1 | Actualizar la definición de la separación de los ambientes de desarrollo, prueba y producción con herramientas de automatización. | Refuerzo | Análisis SGSI - Anexo A | Definir un esquema de trabajo contando con al menos 3 entornos para el desarrollo interno y el desarrollo de los productos. | Definir los requisitos necesarios para incorporar los ambientes de desarrollo y pruebas para el desarrollo en general y el ambiente de producción par el desarrollo interno. Definir las librerias, herramientas, SDK, plugins necesarios para habilitar dichos ambientes, definir que usuarios pueden acceder a dichos ambientes. | 1/7/2022 | 1/9/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 500 | Aprobado | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A12-3-1 | Establecer una política de copias de seguridad para los activos de mayor importancia. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos para generar copias de seguridad de la información y configuración de los equipos de mayor importancia. | Identificar los equipos de los cuales se obtendrán copias de seguridad. Definir un cronograma de obtención de copias de respaldo. Definir donde se almacenarán estas copias de respaldo. | 1/6/2022 | 1/7/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 500 | Aprobado | Fase 3 | |
| SGSI-A1-A12-4-1 | Definir una política de tratamiento, almacenamiento y revisión de logs de los equipos IT de la empresa. Incluir la sincronocidad de tiempo en sus procedimientos. | Refuerzo | Análisis SGSI - Anexo A | Definir los lineamientos, planes de acción y periodicidad del almacenamiento de los logs para sus análisis. | Definir el sitio de almacenamiento de los logs. Definir el tiempo de retención de los logs. Definir la periodicidad de cuando se respladen los logs. Definir el responsable de estas actividades. | 1/1/2022 | 31/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Considerado con otro plan | Fase 2 | |
| SGSI-A1-A12-5-1 | Reforzar y actualizar la política de adquisición de software para uso empresarial con el fin mantener el software empresarial lo mas estable posible y actualizado. | Prevención | Análisis SGSI - Anexo A | Definir lineamientos respecto al software empresarial, su actualización y estabilización. | Definir el listado del software que se ocupa por la empresa. Definir la periodicidad de las actualizaciones. Definir los procesos para realizar la actualización del software y las pruebas de estabilización. | 1/1/2022 | 31/3/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 2500 | Aprobado | Fase 1 | AVAC-SO-05 |
| SGSI-A1-A12-6-1 | Definir un plan de hardening semestral de los equipos informáticos que permitan parchar las vulnerabilidades. | Prevención | Análisis SGSI - Anexo A | Definir las actividades necesarias para evaluar vulnerabilidades en los componentes críticos así como la peridicidad de estos análisis. | Definir los métodos o herramientas para el análisis de vulnerabilidades. Definir un cronograma de análisis. Definir los planes de acción en base a las vulnerabilidades que se encuentren. | 15/7/2022 | 30/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Considerado con otro plan | Fase 3 | |
| SGSI-A1-A13-1-1 | Definir una política de diseño, implementación y operación de una red redundante y con medidas de seguridad acorde a las necesidades de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir un plan de diseño de la red empresarial, parametrizar su implementación y operación. | Definir el estado actual de la red. Definir los componentes necesarios para alcanzar el diseño de la red. Definir los lineamientos de operación de la red y configuraciones de seguridad. | 1/10/2022 | 1/12/2022 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | 3000 | En Revisión | Fase 3 | AVAC-SO-06 |
| SGSI-A1-A13-2-1 | Definir una política de intercambio de información y mensajería electrónica. | Implementación | Análisis SGSI - Anexo A | Definir un esquema de intercambio de información y mensajería electrónica teniendo en cuenta la confidencialidad, integridad, disponibilidad y privacidad. | Definir los lineamientos del intercambio de seguridad, su alcance y las aclaraciones respecto a la seguridad de la información al compartir información por mensajería electrónica. Definir ajustes que señalen estos cambios en la mensajería electrónica. | 1/1/2022 | 31/3/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Aprobado | Fase 1 | |
| SGSI-A1-A14-1-1 | Definir una política de implementación de seguridad en servidores que alberguen sistemas de información. | Mejora Continua | Análisis SGSI - Anexo A | Delimitar las necesidades de seguridad de la información en los servidores de la empresa basado en los lineamientos de confidencialidad, integridad y disponibilidad. | Definir los servidores a ser intervenidos. Definir las herramientas necesarias para implementar seguridad de la información en los servidores. Definir métricas que ayuden a indetificar la eficiencia de las herramientas. | 1/1/2022 | 31/3/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1200 | Aprobado | Fase 1 | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A14-2-1 | Definir una política de desarrollo seguro para la empresa basada en principios de ingenieria de sistemas seguros. | Prevención | Análisis SGSI - Anexo A | Definir las consideraciones necesarias para generar desarrollos seguros dentro de la empresa basados en ingenieria de desarrollo seguro. | Definir los marcos de referencia a utilizarse. Definir las medidas de seguridad al momento de desarrollar. Definir las herramientas de seguridad para los entornos de desarrollo. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | 1000 | En Revisión | Fase 3 |
| SGSI-A1-A14-2-2 | Definir una política de control de cambios en los sistemas de la empresa que incluyan cambios en funcionalidad, en sus librerias, en su entorno de desarrollo o en paquetes de software. | Prevención | Análisis SGSI - Anexo A | Definir una política de control de cambios para los sistemas de la empresa que incluyan cambios de funcionalidad, en el uso de librerias o dependencias o software adicionales. | Definir horarios para los trabajos en la infraestructura. Definir el procedimiento de registro del control de cambios. Definir los formatos para aprobaciones de cambios. Definir el proceso de aprobación de cambios. | 1/7/2022 | 1/8/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Considerado con otro plan | Fase 3 |
| SGSI-A1-A14-2-3 | Definir una política de aseguramiento del entorno de desarrollo. | Prevención | Análisis SGSI - Anexo A | Definir procesos, uso de herramientas y formatos para volver a los entornos de desarrollos ambientes seguros de desarrollo de software. | Definir procesos para asegurar el acceso al entorno de desarrollo. Definir herramientas informáticas para reforzar el entorno de desarrollo. Identificar componentes del entorno de desarrollo que mejoren la seguridad del desarrollo. Definir los usuarios y permisos del entorno de desarrollo. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A14-2-4 | Definir un procedimiento para ejecutar pruebas funcionales de seguridad en los sistemas desarrollados. | Implementación | Análisis SGSI - Anexo A | Definir procesos, herramientas y responsables para ejecutar pruebas funcionales de seguridad en el software que se desarrolla en la empresa. | Definir un marco de referencia o buenas prácticas a seguir para ejecutar pruebas funcionales de seguridad. Definir las pruebas funcionales de seguridad que se ejecutarian como parte de las pruebas funcionales. Definir los resultados esperados de las pruebas funcionales. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A14-2-5 | Definir una política de pruebas de aceptación basada en cumplimiento de requisitos y normas de seguridad. | Implementación | Análisis SGSI - Anexo A | Definir los lineamientos para establecer pruebas de aceptación que consideren requisitos y normas de seguridad. | Definir un marco de referencia o buenas prácticas para aplicarse sobre las pruebas de aceptación. Seleccionar las pruebas aplicables a los desarrollos. Definir los requisitos e seguridad que se evaluaran en las pruebas de aceptación. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A14-3-1 | Definir una política de tratamiento de datos de pruebas, su procesamiento y privacidad en caso de ser datos personales. | Cumplimiento Norma | Análisis SGSI - Anexo A | Definir los lineamientos y consideraciones para el manejo de los datos de prueba y la privacidad de los mismos en caso de ser datos personales. | Definir documentación de autorización de uso de datos de prueba. Definir el proceso de pruebas tomando en cuenta los datos observados.Definir el manejo de los datos luego de la fase de pruebas. | 1/12/2021 | 30/12/2021 | Gerente General,<br>Gerente Financiero<br>Gerente Técnico Oficial de Seguridad de la Información | --- | Aprobado | Fase 1 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A15-2-1 | Definir una política de control de los servicios contratados con los proveedores en base a disponibilidad de servicio y cumplimiento del SLA. | Mejora Continua | Análisis SGSI - Anexo A | Definir los objetivos sobre los servicios contratados referente a su disponibilidad durante un mes, asi como los procesos y herramientas que se utilizarán para estas mediciones. | Listar los SLA de los proveedores que tienen productos o servicios contratados con la empresa. Definir métodos de evaluación del cumplimiento de los SLA. Definir los esquemas de escalamiento que ofrece cada proveedor. | 1/5/2022 | 1/7/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | 500 | Aprobado | Fase 2 |
| SGSI-A1-A16-1-1 | Definir una política de gestión de incidentes de seguridad de la información que incluya procedimientos de analisis, recopilación y mejora continua. | Implementación | Análisis SGSI - Anexo A | Definir procesos para manejar los incidentes de seguridad que pudiera manejar la empresa, estos procesos deben incluir procedimientos de análisis, recopilación, documentación y mejora continua. | Definir procesos para tratar incidentes de seguridad y activar esquemas de contingencia definidos. Definir un plan de comunicación a los clientes/proveedores afectados.Definir acciones de remediación para los incidentes detectados. | 1/1/2022 | 28/2/2022 | Gerente General, Gerente Financiero Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | Aprobado | Fase 1 |
| SGSI-A1-A17-1-1 | Definir un plan de continuidad de la seguridad de la información, sus controles, su revisión, ajuste y mejora continua. | Refuerzo | Análisis SGSI - Anexo A | Definir la continuidad de la seguridad de la información como parte de los esquemas de continuidad, identificar adicionalmente esquemas de revisión ajuste y mejora continua. | Definir los mecanismos de continuidad respecto a la seguridad que se implementarán en la empresa. Definir procesos de revisión de los procesos de continuidad. Definir las métricas sobre las medidas de continuidad. Definir planes de mejora en base de la evaluación de métricas. | 3/1/2022 | 28/2/2022 | Gerente General, Gerente Técnico, Gerente Financiero. | --- | Considerado con otro plan | Fase 1 |
| SGSI-A1-A17-2-1 | Definir un proyecto para reforzar y mejorar los esquemas existentes en los componentes que se consideren como críticos. | Prevención | Análisis SGSI - Anexo A | Definir las necesidad de redundancia y alta disponibilidad para componentes de IT críticos, así como definir el tiempo que las adquisiciones se mantengan operativas en la empresa. | Definir la vida útil de los componentes IT. Definir la reutilización de los componentes IT si aplica. Definir un roadmap de adquisiciones como parte de las renovaciones de IT. | 3/1/2022 | 28/2/2022 | Gerente General, Gerente Técnico, Gerente Financiero. | --- | Considerado con otro plan | Fase 1 |
| SGSI-A1-A18-1-1 | Realizar una auditoria externa para identificar puntos de mejora respecto al cumplimiento legal y requisitos contractuales. | Prevención | Análisis SGSI - Anexo A | Definir los objetivos que se persiguen con la auditoria externa respecto a la conformación de la empresa, el cumplimiento legal y los requisitos contractuales. | Definir el alcance de la auditoria. Definir que lineamientos de cumplimiento legal se buscan evaluar. Definir que areas de cumplimiento se van a evaluar. Seleccionar un proveedor de servicios de auditoria | 1/10/2022 | 30/12/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | 2500 | En Revisión | Fase 3 |
| SGSI-A1-A18-1-2 | Definir una política para registro de derechos de propiedad intelectual en el caso de los desarrollos que se manejan dentro de la empresa. | Implementación | Análisis SGSI - Anexo A | Definir los procesos para identificar y registrar los desarrollos que se hacen dentro de la empresa como propiedad intelectual. | Incluir en los procesos de venta de productos y servicios la sección de "Porpiedad Intelectual". Definir una bitácora de desarrollos efectuados por la empresa. Definir un proceso de registro de los desarrollos como parte de la propiedad intelectual de la empresa. | 1/10/2022 | 30/12/2022 | Gerente Técnico Oficial de Seguridad de la Información Personal de IT | --- | En Revisión | Fase 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SGSI-A1-A18-1-3 | Definir una política de protección de los registros de la organización y reforzar las medidas de seguridad de estos registros. | Implementación | Análisis SGSI - Anexo A | Definir procesos para proteger los registros importantes de la empresa e identificar las medidas de seguridad que sean aplicables a la empresa. | Clasificar la información que maneja la empresa. Definir en que partes de la empresa se almacena esta información. Definir procesos para asegurar el acceso a la información y a los registros. | 1/10/2022 | 30/12/2022 | Gerente Técnico<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | En Revisión | Fase 3 |
| SGSI-A1-A18-1-4 | Definir una política de protección y privacidad de la información de carácter personal. | Implementación | Análisis SGSI - Anexo A | Definir los pasos necesarios para proteger los documentos o procesos empresariales que manejen información de carácter personal, asi como las medidas de protección de esta información. | Clasificar la información que maneja la empresa y los tipos de información en base a la privacidad. Definir procesos que permitan asegurar la privacidad en el manejo de la información.Definir procesos de manejo de información personal que contenga autorizaciones por parte de los encargados de procesar esa información o de los dueños de esa información. | 3/1/2022 | 28/2/2022 | Gerente General,<br>Gerente Técnico,<br>Gerente Financiero.<br>Oficial de Seguridad de la Información<br>Personal de IT | --- | Considerado con otro plan | Fase 1 |