FACULTAD DE POSTGRADOS

# DESARROLLO DEL PROGRAMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)


AUTORES

Luis Sebastián Guerra Andrade
Jenny Esther Zambrano Palacio


AÑO

2022


FACULTAD DE POSTGRADOS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

# DESARROLLO DEL PROGRAMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

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

Autores

Luis Sebastián Guerra Andrade

Jenny Esther Zambrano Palacio

2022

## DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

---

Luis Sebastián Guerra Andrade

1718085069

---

Jenny Esther Zambrano Palacio

2300274905

**AGRADECIMIENTOS**

A mi colega Sebastián por su paciencia y dedicación para culminar con éxito el presente trabajo. A la UDLA y todos los docentes por haber compartido sus conocimientos y experiencias.

Jenny

**AGRADECIMIENTOS**

Quiero agradecer a la UDLA y todos los docentes sus conocimientos me ayudaron para lograr esta nueva etapa académica.

A mi compañera de CAPSTONE Jenny por su esfuerzo y dedicación para lograr este proyecto.

Sebastián

**DEDICATORIA**

El presente trabajo se lo dedico a mi madre por su apoyo incondicional y palabras de aliento durante cada etapa de mi vida. A mi padre, hermanos y sobrinos que son mi fuente de inspiración.

Jenny

**DEDICATORIA**

Quiero dedicar este trabajo a mi Padre, a mi madre, a mis hermanos, a mis abuelos, tíos, tías y primos los cuales son el pilar para mi y los cuales me dan el animo necesario para cumplir mis objetivos.

Pero quiero dedicarle este logro a una persona muy especial quien con sus palabras y enseñanzas estuvo siempre impulsándonos a ser mejores cada día. Para ti PAPITO MARCELO.

Sebastián

## RESUMEN

El presente proyecto tiene como objetivo realizar el análisis y desarrollo de un sistema de gestión de la seguridad de la información (SGSI) que busca ayudar a solucionar un problema existente en un proveedor de servicios de internet (ISP).

Luego de realizar un análisis de los diferentes marcos de trabajo para seguridad de la información se decide utilizar COBIT 2019 e ISO27000 para el desarrollo del presente proyecto. La información que se utilizará en este proyecto fue recabada mediante el uso de matrices de evaluación, los resultados de estas evaluaciones se representarán de manera gráfica para una mejor visualización y comprensión. Este proyecto se divide en 5 fases las cuales son: Diagnostico, Clasificación de la información, Inventario de activos de información, Análisis de amenazas y vulnerabilidades y Documentos clave del SGSI.

En la primera fase de Diagnostico se realizó una evaluación de la situación actual de la organización, se obtuvo como resultado el nivel actual y se elaboró un plan de acción para llegar a un nivel de proyección. En la segunda fase se realizó un el análisis de las entidades que forman parte de la organización y se obtuvo como resultado una matriz de criticidad de las entidades y del tipo de información que estas poseen. En la tercera fase se realizó un análisis del inventario de activos y se obtuvo como resultado una matriz de criticidad de los activos del ISP. En la cuarta fase se realizó un análisis de amenazas y vulnerabilidades, se escogieron dos activos de información, se analizaron los controles y se obtuvo como resultado una matriz del riesgo inherente y residual de las amenazas de cada activo. En la fase 5 se realizaron las políticas de alto nivel para la organización y un roadmap con los planes de acción de mejora para la organización.

## ABSTRACT

In this document you can see the analysis and development of an information security management system (ISMS) that seeks to help solve an existing problem in an internet service provider (ISP).

After carrying out an analysis of the different frameworks for information security, it was decided to use COBIT 2019 and ISO27000 for the development of this project. The information that will be used in this project was collected using evaluation matrices, the results of these evaluations will be represented graphically for better visualization and understanding. This project is divided into 5 phases which are: Diagnosis, Classification of information, Inventory of information assets, Analysis of threats and vulnerabilities and ISMS key documents.

In the first phase of Diagnosis, an evaluation of the current situation of the organization was carried out, the current level was obtained as a result and an action plan was developed to reach a projection level. In the second phase, an analysis of the entities that are part of the organization was carried out and a criticality matrix of the entities and the type of information they possess was obtained as a result. In the third phase, an analysis of the asset inventory was carried out and a criticality matrix of the ISP's assets was obtained as a result. In the fourth phase, an analysis of threats and vulnerabilities was carried out, two information assets were chosen, the controls were analyzed and a matrix of the inherent and residual risk of the threats of each asset was obtained as a result. In phase 5, the high-level policies for the organization and a roadmap with the improvement action plans for the organization were made.

**ÍNDICE**

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

# INTRODUCCIÓN

## Antecedentes

El proveedor de servicios de internet “XYZ” (llamado de ahora en adelante ISP) es una empresa ubicada en la ciudad de Santo Domingo desde hace 4 años aproximadamente, brinda servicios por medio de fibra óptica y radio enlaces. Cuenta con alrededor de 8000 clientes con cobertura en Santo Domingo, Alluriquín, Tandapi, Luz de América, La Concordia, Quinindé, Viche y Jipijapa. Trabaja con algunos proveedores de internet por tal motivo ofrece planes de alta velocidad a bajo costo, teniendo una gran acogida por sus precios competitivos. Cuenta con un grupo de talento humano de 30 personas aproximadamente.

Actualmente el ISP no cuenta con un área de seguridad informática implementada, por lo cual no cuenta con un sistema de gestión de la seguridad de la información (SGSI). También sufre de ciertas falencias en el manejo de sus activos físicos, falencias en la comunicación dentro de la organización.

Con todo lo expuesto anteriormente se ha planteado en este proyecto el desarrollo del SGSI para el ISP, el cual ayudará a la organización a preservar la integridad, disponibilidad y confidencialidad de la información y de los activos de la organización.

# DESARROLLO DEL PROYECTO DE TITULACIÓN

## Objetivo General

Desarrollar un programa de gestión de seguridad que ayude a la organización a proteger todos los activos de información.

## Objetivos Específicos

- Garantizar la continuidad del negocio.
- Minimizar riesgos cumpliendo con los principios básicos de confidencialidad, disponibilidad, integridad y privacidad.
- Cumplir con normativas locales.
- Definir políticas de alto nivel para la organización que permitan conservar la disponibilidad, integridad y confidencialidad de la información y activos de información de la organización.

## Alcance

El desarrollo del programa contará con 5 fases las cuales se detallarán a lo largo de todo el documento. Estas fases son las siguientes:

- Fase 1. Diagnóstico
- Fase 2. Clasificación de la información
- Fase 3. Inventario de activos de información
- Fase 4. Análisis de amenazas y vulnerabilidades de activos de información críticos.
- Fase 5. Documentos clave del SGSI

## Fase 1: Diagnóstico

### Metodología

Se elaboró un caso de negocio, en el cual se conoció el contexto del ISP, cuáles son sus puntos de dolor, se detalló cuáles serán los beneficios que el ISP

obtendrá con este proyecto y con toda esta información se detalló el alcance inicial del proyecto.

Una vez finalizado y elaborado el caso de negocio se procedió a realizar una evaluación al estado actual del ISP. Para el análisis de la situación actual del ISP se utilizaron los marcos de referencia COBIT 2019 e ISO27001 con los cuales se pudo realizar una herramienta de evaluación que ayudo a realizar esta evaluación con mayor facilidad.

Se elaboró una matriz en la cual por cada cláusula de la ISO27001 se establecieron diferentes preguntas, las cuales permitieron recopilar toda la información necesaria para conocer el estado del ISP, como se observa en la figura 1.

| | Claúsulas |
|---|---|
| 4 | Contexto de la organización |
| 4.1 | Tiene definido los contextos internos y externos que afectan a su organización? |
| | Tiene documentos los contextos internos y externos que afectan a su organización? |
| | Tiene categorizado los contextos? |
| | Tiene documentada la categorización de los contextos |
| 4.2 | Tiene definidos las partes interesadas de la organización? |
| | Tiene documentadas las partes interesadas de la organización? |
| | Tiene clasificadas las partes interesadas? |
| | Tiene documentada la clasificación de las partes interesadas? |
| | Ha comprendido las necesidades y expectativas de las partes interesadas? |
| | Tiene documentado las necesidades y expectativas de las partes interesadas? |
| 4.3 | Ha determinado el alcance del sistema de seguridad de la información?* |
| | Tiene documentado el alcance del SGSI?* |
| 4.4 | Tiene implementado el sistema del SGSI? |

*Figura 1. Encuesta de recopilación*

Se elaboró una tabla de métricas de evaluación la cual ayudó a calificar las respuestas proporcionadas por el personal del ISP como se observa en la tabla 1.

*Tabla 1. Métricas de evaluación*

| Valor | Métricas de evaluación | Rango |
|---|---|---|
| N | Nada | 1 |
| P | Parcial | 2 |
| L | Documentado | 3 |
| F | Full | 4 |

Donde;

N: en la organización no existe la cláusula.

P: en la organización existe la cláusula, pero está parcialmente implementada.

L: en la organización existe la cláusula, está implementada y documentada.

F: en la organización está documentada la cláusula, implementada y se trabaja en la mejora continua.

Para determinar la situación actual del ISP se utilizó como referencia los niveles de capacidad para los procesos de Cobit 2019 como se observa en la figura 2, ya que en este modelo se detalla en qué nivel se encuentran los procesos por tal motivo ayudará a identificar el nivel actual que se encuentra la organización.

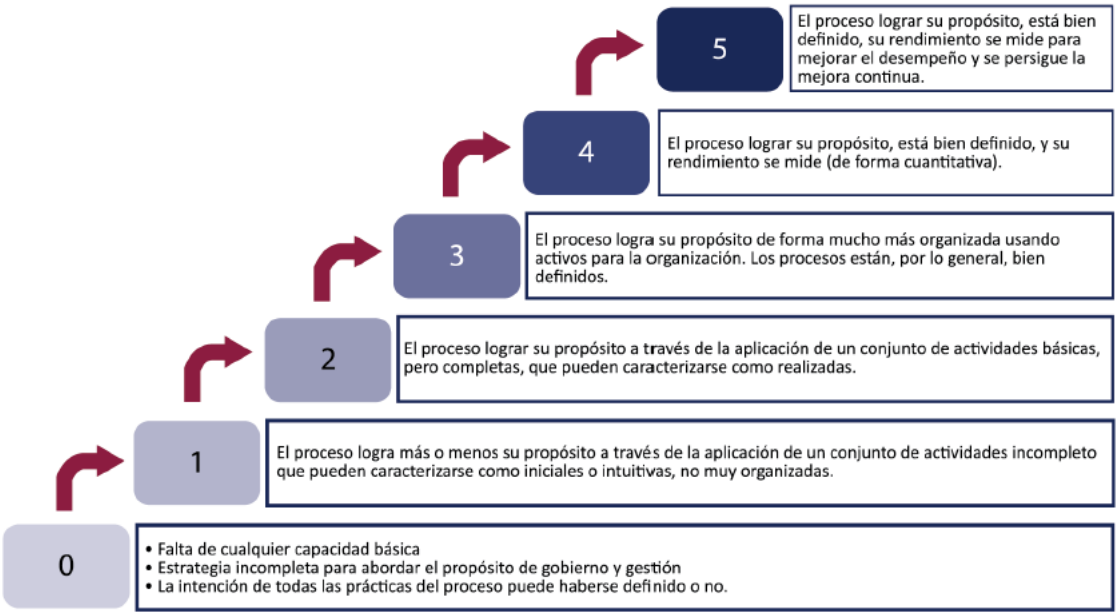


*Figura 2. Niveles de capacidad para los procesos (ISACA, 2018)*

En la tabla 2 se observa el resultado de la escala de medición personalizada para la conocer la situación actual del ISP.

*Tabla 2. Situación actual de la organización*

| Nivel | Situación Actual | Rango |
|---|---|---|
| 1 | En la organización existe cierta evidencia con logros sin definir y sin documentar | 0-1 |
| 2 | En la organización existe cierta evidencia con logros definidos, pero no documentados | >1 a 1.75 |
| 3 | En la organización existe evidencia clara con logros bien definidos y documentados | >1.75 a 2.5 |
| 4 | En la organización existe evidencia clara con logros bien definidos, documentados y evaluados | >2.5 a 3.25 |
| 5 | En la organización existe evidencia clara con logros bien definidos, documentados y evaluados. La organización trabaja en la mejora continua | > 3.25 a 4 |

Una vez establecidos los parámetros de evaluación y las escalas de medición, se realizó la evaluación y se definió la proyección a la que se quiere llegar para cada una de las cláusulas evaluadas, de esta manera se logró determinar la situación actual del ISP como se observa en la figura 3.

| | Claúsulas | Calificación Actual | | Nivel Actual |
|---|---|---|---|---|
| 4 | Contexto de la organización | | | |
| 4.1 | Tiene definido los contextos internos y externos que afectan a su organización? | Si | P | 2 |
| | Tiene documentos los contextos internos y externos que afectan a su organización? | No | | |
| | Tiene categorizado los contextos? | Si | P | |
| | Tiene documentada la categorización de los contextos | No | | |
| 4.2 | Tiene definidos las partes interesadas de la organización? | Si | P | |
| | Tiene documentadas las partes interesadas de la organización? | No | | |
| | Tiene clasificadas las partes interesadas? | Si | P | |
| | Tiene documentada la clasificación de las partes interesadas? | No | | |
| | Ha comprendido las necesidades y expectativas de las partes interesadas? | Si | P | |
| | Tiene documentado las necesidades y expectativas de las partes interesadas? | No | | |
| 4.3 | Ha determinado el alcance del sistema de seguridad de la información?* | No | N | |
| | Tiene documentado el alcance del SGSI?* | No | | |
| 4.4 | Tiene implementado el sistema del SGSI? | No | N | |

*Figura 3. Situación actual de la organización*

Se propusieron planes de acción los cuales ayudaron a justificar el nivel de proyección seleccionado de esta manera mejorar la situación actual de la organización, como se observa en la figura 4.

| Proyección | Plan de acción |
|---|---|
| 3 | Documentar los contextos internos y externos que afectan a su organización |
| | Categorizar y documentar los contextos |
| | Documentar las partes interesadas de la organización |
| | Documentar la clasificación de las partes interesadas |
| | Documentar las necesidades y expectativas de las partes interesadas |
| | Determinar y documentar el alcance del SGSI |
| | Implementar el SGSI |

*Figura 4. Proyección y planes de acción*

**Resultados**

Como se puede evidenciar en la figura 5 el ISP se encuentra en un nivel inicial en gestión de seguridad de la información, existe mayor falencia en las cláusulas de planificación, soporte, operación, evaluación de desempeño y mejora continua. Pero hay procesos que están implementados, aunque no se encuentran documentados por tal motivo existen grandes oportunidades de mejora. Nuestra proyección es mejorar los principales procesos y a mediano plazo obtener un nivel superior en cada proceso.

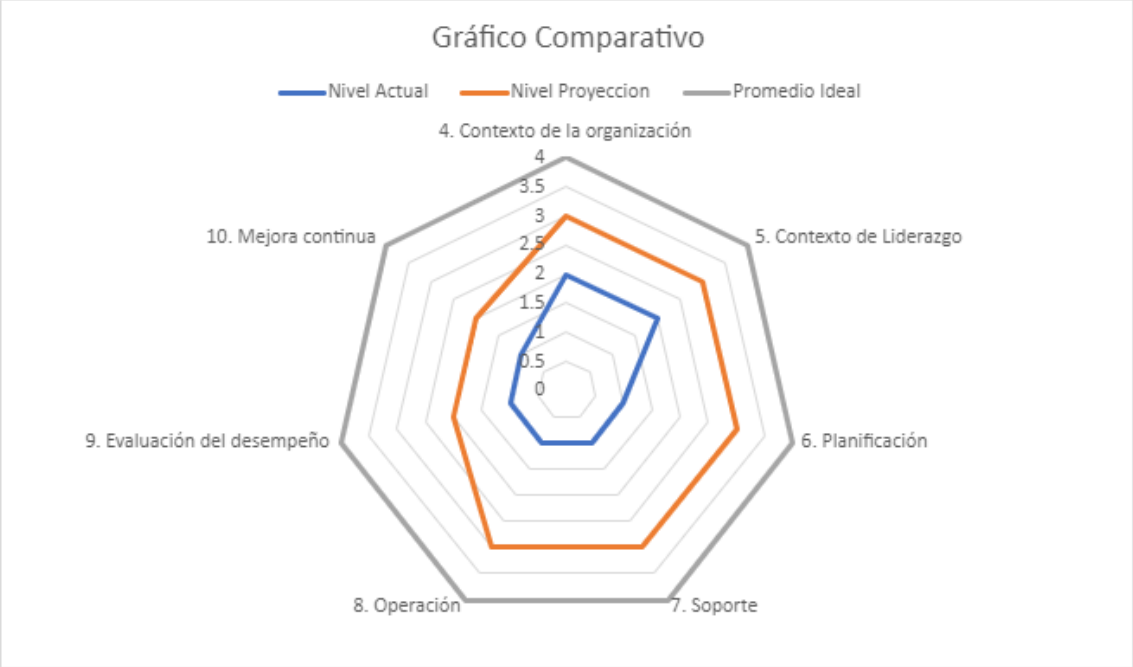


*Figura 5. Resultado de evaluación de la situación actual de la organización*

**Referencia Anexos**

En el anexo Caso de Negocio.pptx se puede encontrar el caso negocio en donde se puede observar toda la información para la propuesta de este proyecto.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Matriz de Evaluación” se puede encontrar la matriz de evaluación utilizada en donde se puede observar la situación inicial de la organización tomando como referencia las cláusulas de la norma ISO27001.

**Fase 2: Clasificación de la información**

La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas. (Asociación Española de Normalización, 2017)

La clasificación de la información trata de comprender el tipo de información que maneja la organización, posteriormente se realiza un análisis respecto a la

confidencialidad, integridad y disponibilidad de la información, para así poder conocer la criticidad de la información.

El apetito del riesgo es la cantidad de riesgo que la organización está dispuesta a asumir o aceptar. (Alonso, 2020)

La confidencialidad es la protección de la información contra accesos no autorizados. (Asociación Española de Normalización, 2017)

La disponibilidad garantiza el acceso y el uso oportuno de la información y los sistemas. (Asociación Española de Normalización, 2017)

La integridad es la protección de la información contra modificación no autorizada. (Asociación Española de Normalización, 2017)

## Metodología

En la fase 2 se elaboró una matriz en la cual se detallan las entidades de la organización, siendo la entidad el sujeto de información del cual se almacena, genera o transmite información. Para cada entidad se asoció los tipos de información y se evaluó respecto a la confidencialidad, integridad y disponibilidad de la información. Además, se evaluó el nivel de cumplimiento y de esta manera se pudo obtener la criticidad total de la entidad.

## Apetito del riesgo

En la tabla 3 se puede observar el impacto del riesgo según su aversión, neutralidad o agresividad que puede afectar a la organización, para poder identificar los activos críticos.

*Tabla 3. Apetito del riesgo*

| Impacto | Aversión | Neutral | Agresivo |
|---|---|---|---|
| Multas y sanciones de los Organismos de Control | Reputación organizacional | | |
| Demandas judiciales | | | |
| Pérdida o degradación de la imagen institucional | | | |
| Interrupción de operaciones | Disponibilidad del servicio | | |
| Pérdidas de vida de las personas | | | |
| Afectación de la salud de las personas | | Disponibilidad del Servicio | |
| Afectación al clima laboral | | | x |
| Pérdidas financieras | | Cartera de clientes | |
| Pérdidas / destrucción de bienes materiales | | Infraestructura | |
| Lucro cesante | | Expansión de red | |
| Observaciones de auditoría interna o externa | | | x |
| Pérdida de contratos | | | Registro de clientes |

En la tabla 4 se puede visualizar el nivel del impacto para los diferentes riesgos, para la organización una interrupción del servicio de 2 semanas sería catastrófico ya que los clientes usan el internet diariamente para sus actividades cotidianas y laborales.

*Tabla 4. Impacto organizacional*

| Niveles | Pérdidas financieras | Interrupción de operaciones | Salud de las personas | Multas y sanciones de los Organismos de Control | Pérdidas / destrucción de bienes materiales | Pérdida de contratos |
|---|---|---|---|---|---|---|
| Catastrófico | ≥ 500000 | ≥ 2 semanas | Muerte | 6 avisos | 20 o más equipos | |
| Mayor | De 250k a 499,999k | De 4 a 13 días | Enfermedad catastrófica | 4 a 5 avisos | De 11 a 20 equipos | |
| Moderado | De 50k a 249,999k | De 1 a 3 días | Hospitalización | 3 avisos | De 5 a 10 equipos | |
| Menor | De 5k a 49,999k | | | 2 avisos | De 2 a 4 equipos | > 5 |
| Insignificante | ≤ 4,999k | | | 1 avisos | 1 equipo | ≤ 5 |

## Identificación de las entidades de información

En el ISP se identificaron las siguientes entidades

- Cliente Persona Natural
- Cliente Persona Jurídica
- Prospecto de Clientes
- Empleados
- Proveedores
- Vehículos
- Accionistas/Socios
- Organización
- Ex-clientes
- Vendedores freelance
- Bancos

Para cada entidad se asociaron los tipos de información que se maneja en cada entidad, adicional se definió el tipo de información como se observa en figura 6.

| Nombre de la Entidad | Nombre del tipo de información | Definición del tipo de información |
|---|---|---|
| Cliente Persona Natural | Información General de cliente persona natural | Información general del cliente como por ejemplo Nombre, Apellido, Cédula, referencias personales |
| | Información Bancaria | Información bancaría del cliente que se usa para el cobro por ejemplo Número de cuenta, tipo de cuenta, entidad bancaria |
| | Información de contacto | Información que se usa para ubicar y contactar al cliente como por ejemplo Ubicación GPS, teléfonos |
| Cliente Persona Jurídica | Información General de cliente persona Juridica | Información general del cliente como por ejemplo Nombre de la empresa, RUC, representante legal |
| | Información Bancaria | Información bancaría del cliente que se usa para el cobro por ejemplo Número de cuenta, tipo de cuenta, entidad bancaria |
| | Información de contacto | Información que se usa para ubicar y contactar al cliente como por ejemplo Ubicación GPS, teléfonos |

*Figura 6. Entidades del ISP*

Al ser la organización un ISP se consideró el criterio de mayor de evaluación es la integridad y confidencialidad de la información por tal motivo se le asignó mayor peso dentro de los criterios de evaluación como se visualiza en la tabla 5.

*Tabla 5. Criterios de evaluación*

| Criterio | Porcentaje |
|---|---|
| Disponibilidad | 25 |
| Integridad | 30 |
| Confidencialidad | 30 |
| Cumplimiento | 15 |

En la tabla 6 se observa la matriz calificación personalizada considerando la disponibilidad, integridad, confidencialidad y cumplimiento, con la ayuda de esta tabulación obtener el nivel de criticidad de la información.

*Tabla 6. Nivel de criticidad*

| Nivel | Disponibilidad | Integridad | Confidencialidad | Cumplimiento |
|---|---|---|---|---|
| Catastrófico | 25 | 30 | 30 | 15 |
| Mayor | 20 | 24 | 24 | 12 |
| Moderado | 15 | 18 | 18 | 9 |
| Menor | 10 | 12 | 12 | 6 |
| Insignificante | 5 | 6 | 6 | 3 |

Una vez establecidos los parámetros de evaluación, se realizó la evaluación de los tipos de información como se observa en la figura 7.

| Definición del tipo de información | Disponibilidad | Integridad | Confidencialidad |
|---|---|---|---|
| Información general del cliente como por ejemplo Nombre, Apellido, Cédula, referencias personales | Moderado | Menor | Menor |
| Información bancaría del cliente que se usa para el cobro por ejemplo Número de cuenta, tipo de cuenta, entidad bancaria | Mayor | Catastrofico | Catastrofico |
| Información que se usa para ubicar y contactar al cliente como por ejemplo Ubicación GPS, teléfonos | Menor | Menor | Menor |
| Información general del cliente como por ejemplo Nombre de la empresa, RUC, representante legal | Mayor | Mayor | Menor |
| Información bancaría del cliente que se usa para el cobro por ejemplo Número de cuenta, tipo de cuenta, entidad bancaria | Mayor | Catastrofico | Catastrofico |

*Figura 7. Evaluación de los tipos de información*

Posteriormente se realizó un análisis según la etiqueta de confidencialidad, considerando la asignación de la tabla 7. Esta etiqueta ayudara a saber cómo manipular la información al ser compartida dentro de la organización.

*Tabla 7. Etiqueta de confidencialidad*

| Nivel | Etiqueta |
|---|---|
| Catastrófico | Secreta |
| Mayor | Restringida |
| Moderado | Confidencial |
| Menor | Uso interno |
| Insignificante | Publica |

## Resultados

En la figura 8 se puede observar el resultado del nivel de criticidad del tipo de información de la entidad obtenido dependiendo de la integridad, disponibilidad, confidencialidad y cumplimiento de la información. Donde podemos observar que toda la información bancaria es la más crítica.

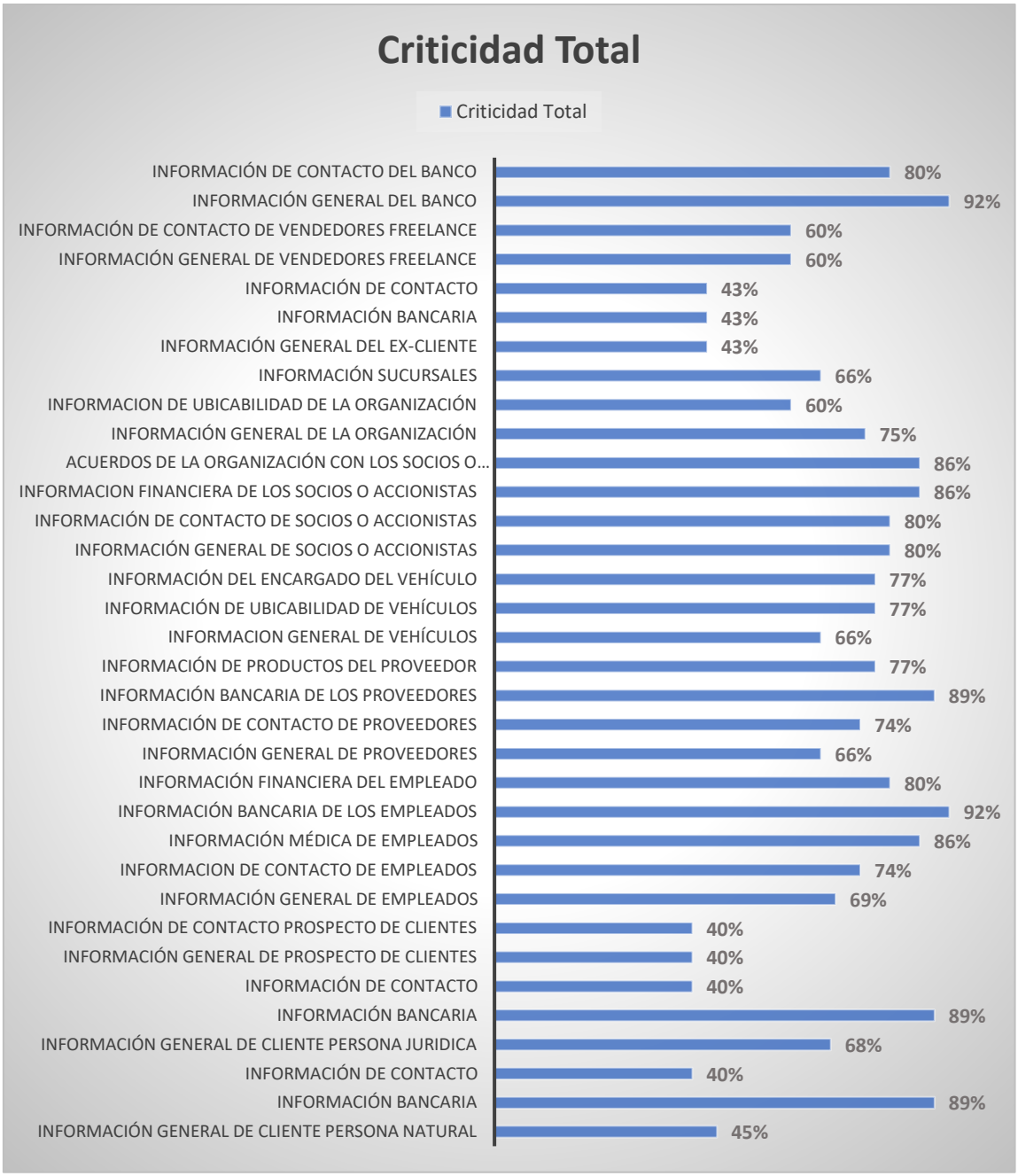


*Figura 8. Criticidad de los tipos de Entidades*

## Referencia Anexos

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Apetito del riego” se puede encontrar la matriz de apetito del riego y la matriz de impacto organizacional, establecida para la organización.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Tipo de información” se puede encontrar la matriz de tipos de información y su calificación de criticidad,

así como las tablas de criterio de calificación y la tabla de etiquetas de confidencialidad.

## Fase 3: Inventario de activos de información

Según la norma ISO 27001 un activo de información es cualquier elemento de la organización que genera, transmite, almacena o comparte información crítica y sensible, los cuales valora y protege. (Asociación Española de Normalización, 2017)

El inventario de activos de información trata de detallar todos los activos que posee la organización, posteriormente se realiza un análisis respecto al nivel de criticidad de la información que manejan.

### Metodología

En la fase 3 se detallaron todos los activos de información de la organización, de esta manera clasificar los activos que manejan información crítica, como se observa en la tabla 8.

*Tabla 8 Activos de información*

| Cantidad | Activo de información |
|---|---|
| **1** | Servidor del sistema |
| **1** | Servidor de WhatsApp |
| **1** | Servidor contable |
| **1** | Servidor de respaldos |
| **20** | Router |
| **10** | OLT |
| **10** | PC |
| **1** | Central telefónica |

En la figura 9 se observa la clasificación del activo según el tipo de información que maneja. Para el análisis se tomó como referencia la integridad de la información en los cuales los procesos fueron mayor y catastrófico, de esta manera poder tener el nivel de criticidad del activo de información.

| Codigo | Codificación | Nombre del activo de informacion | Proceso | Tipo de informacion | Clasificacion del tipo de informacion | Criticidad del activo de información |
|---|---|---|---|---|---|---|
| 1 | tec-bdd-1 | BDD del sistema ISP Administrador | Mayor/Catastrofico | Información Bancaria de cliente persona natural | Catastrofico | Catastrofico |
| | | | | Información General de cliente persona Juridica | Mayor | |
| | | | | Información Bancaria de cliente persona Juridica | Catastrofico | |
| | | | | Información General de empleados | Mayor | |
| | | | | Informacion de contacto de empleados | Mayor | |
| | | | | Información médica de empleados | Catastrofico | |
| | | | | Informacion general de vehículos | Mayor | |
| | | | | Información de ubicabilidad de vehículos | Mayor | |
| | | | | Información del encargado del vehículo | Mayor | |

*Figura 9. Inventario de activos de información*

## Resultados

Como se puede evidenciar en la figura 10 los activos del ISP con mayor nivel de criticidad son los servidores, BDDs y aplicaciones, en cada activo se obtuvo una criticidad catastrófica para el tipo de información que manejan.

| Codigo | Codificación | Nombre del activo de informacion | Proceso | Tipo de informacion | Clasificacion del tipo de informacion | Criticidad del activo de información |
|---|---|---|---|---|---|---|
| 1 | tec-bdd-1 | BDD del sistema ISP Administrador | Mayor/Catastrofico | Información Bancaria de cliente persona natural | Catastrofico | Catastrofico |
| | | | | Información General de cliente persona Juridica | Mayor | |
| | | | | Información Bancaria de cliente persona Juridica | Catastrofico | |
| | | | | Información General de | Mayor | |
| | | | | Informacion de contacto de empleados | Mayor | |
| | | | | Información médica de | Catastrofico | |
| | | | | Informacion general de | Mayor | |
| | | | | Información de ubicabilidad de vehículos | Mayor | |
| | | | | Información del encargado del vehículo | Mayor | |
| 2 | tec-bdd-2 | D del sistema conta | Mayor/Catastrofico | Información bancaria de los empleados | Catastrofico | Catastrofico |
| | | | | Información Financiera | Mayor | |
| | | | | Información General de proveedores | Mayor | |
| | | | | Información de contacto de proveedores | Mayor | |
| | | | | Información bancaria de los proveedores | Catastrofico | |
| | | | | Información de productos del proveedor | Mayor | |
| | | | | Información general de socios o accionistas | Mayor | |
| | | | | Información de contacto de socios o accionistas | Mayor | |

*Figura 10. Clasificación de activos de información*

### Referencia Anexos

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Inventario de activos” se puede encontrar la matriz del inventario de activos de la organización junto con su respectivo análisis de criticidad.

## Fase 4: Análisis de amenazas y vulnerabilidades de activos de información críticos

Una amenaza es la causa potencial de un incidente no deseado que puede ocasionar daño a la organización. (Asociación Española de Normalización, 2017)

Una vulnerabilidad es una debilidad de un activo que puede ser explotada por una o más amenazas. (Asociación Española de Normalización, 2017)

El análisis de amenazas y vulnerabilidades tiene el objetivo de identificar el nivel de riesgo que está expuesta la organización y encontrar los mejores controles para mitigar estas amenazas o vulnerabilidades encontradas en los activos críticos de la organización.

### Metodología

En la fase 4 se realizó un análisis de dos activos críticos los cuales se escogieron por su nivel de criticidad dependiendo el tipo de información que manejan.

En la tabla 9 se definió una matriz de impacto y probabilidad para el análisis de los activos críticos del ISP.

*Tabla 9. Descripción de impacto y probabilidad*

| Impacto | | Probabilidad | |
|---|---|---|---|
| Insignificante | Perdidas ligeras de contratos de clientes y financieras | Raro | 2% |
| Menor | Perdidas moderadas de contratos de clientes y financieras | Poco Probable | 5% |
| Moderado | Pérdidas financieras moderadas, afectaciones ligeras a la operación y hospitalización del personal | Posible | 25% |
| Mayor | Pérdidas financieras significantes, afectaciones significantes a la operación y enfermedades catastróficas del personal | Probable | 75% |
| Catastrófico | Perdidas significantes financieras, se haría complicado mantener la operación y muerte del personal | Casi Certeza | 100% |

En la tabla 10 se determinó una matriz de impacto vs probabilidad que posteriormente se va a utilizar para poder obtener la severidad del riesgo.

*Tabla 10. Impacto vs Probabilidad*

| | | Impacto | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| **Probabilidad** | **Raro** | **Bajo** | **Bajo** | **Medio** | **Medio** | **Alto** |
| | **Poco Probable** | **Bajo** | **Bajo** | **Medio** | **Medio** | **Alto** |
| | **Posible** | **Bajo** | **Medio** | **Medio** | **Alto** | **Critico** |
| | **Probable** | **Medio** | **Medio** | **Alto** | **Critico** | **Critico** |
| | **Casi Certero** | **Medio** | **Alto** | **Alto** | **Critico** | **Critico** |

Siendo:

**Critico**: Evento de riesgo que representa una posibilidad de pérdida muy alta, que puede afectar gravemente la continuidad del negocio e incluso ocasionar un cierre de la organización, por lo tanto, requiere tomar acciones inmediatas por parte de la Gerencia de la organización

**Alto**: Evento de riesgo que representa una posibilidad de pérdida alta, que puede afectar el funcionamiento normal de algunos procesos, por lo tanto, requiere poner atención por parte de la Gerencia de la organización

**Medio**: Evento de riesgo que representa una posibilidad de pérdida moderada, que puede afectar el funcionamiento normal de ciertos procesos, por lo tanto, requiere poner atención por parte de la Gerencia de la organización

**Bajo**: Evento de riesgo que representa una posibilidad que no afecta significativamente a la organización o a sus procesos, por lo tanto, requiere controles y procedimientos de rutina por parte de la Gerencia de la organización

Para la identificar las vulnerabilidades a las cuales los activos críticos están expuestos se tomó como referencia MAGERIT versión 3. (Ministerio de Hacienda y Administraciones Públicas, 2012)

Una vez que se identificaron las vulnerabilidades del servidor se procedió a analizar las amenazas y relacionarlas con las vulnerabilidades, el impacto de seguridad y el impacto organizacional.

Posteriormente se analizó la probabilidad e impacto inherente y de esta manera poder obtener la severidad inherente con las consideraciones de la matriz de impacto vs probabilidad como se observa en la figura 11.

| | **Servidor** | | | | **Inherencia** | | |
|---|---|---|---|---|---|---|---|
| **#** | **Amenazas** | **Vulnerabiliadad** | **Impacto Seguridad** | **Impacto Organizacional** | **Probabilidad Inherente** | **Impacto Inherente** | **Severidad Inherete** |
| 1 | Desastres Naturales | Falta de aseguramiento de la<br>Falta de protección de los equipos | Disponibilidad | Interrupción de operaciones | **Poco Probable** | **Catastrofico** | **Alto** |
| 2 | Corte de suministro electrico | No se tiene un backup eléctrico<br>Falta de aseguramiento de la | Disponibilidad | Interrupción de operaciones | **Posible** | **Mayor** | **Alto** |
| 3 | Averia de origen fisico | No se han realizado actualizaciones y mantenimiento a los equipos | Disponibilidad | Interrupción de operaciones | **Probable** | **Mayor** | **Critico** |
| 4 | Condiciones inadecuadas de temperatura o humedad | Falta de aseguramiento de la<br>Falta de protección de los equipos | Disponibilidad | Interrupción de operaciones | **Posible** | **Moderado** | **Medio** |

*Figura 11. Riesgo inherente servidor*

En la figura 12 se puede observar la identificación de amenazas para cada vulnerabilidad que está expuesto el activo crítico servidor.

| Vulnerabilidades | Desastres Naturales | Corte de suministro electrico | Averia de origen fisico | Condiciones inadecuadas de temperatura o humedad | Interrupcion de servicios y suministros esenciales | Fallo de servicios de comunicaciones | Errores de los usuarios |
|---|---|---|---|---|---|---|---|
| Falta de aseguramiento de la disponibilidad | x | x | | x | x | | |
| Falta de protección de los equipos | x | | | x | | | |
| No se tiene un backup eléctrico | | x | | | x | | |
| No se han realizado actualizaciones necesarias y mantenimiento a los equipos | | | | | x | | x |
| No hay proteccion de los servicios de comunicaciones | | | | | | X | |
| Falta de capacitaciones | | | | | | | X |

*Figura 12. Vulnerabilidades del servidor*

Posteriormente se identificaron los controles para las vulnerabilidades encontradas, esta identificación se la realizó con la ayuda del marco de referencia CIS Controls (Center for Internet Security, 2022), luego se realizó una descripción de cada control como se observa en la figura 13.

| Controles | Descripcion del Control |
|---|---|
| Aseguramiento de la disponibilidad | Asegura que los servidores esten disponibles |
| Protección de los equipos | Los servidores deben situarse de forma que reduzcan los riesgos de amenzas y oportunidades que produzcan accesos no autorizados |
| Backup eléctrico | Es necesario contar con un backup eléctrico, disponer de alarmas de detección de fallas eléctricas y activación de backup |
| Realizar actualizaciones necesarias y mantenimiento a los | Los servidores deben recibir mantenimiento correcto teniendo en cuentra si se va a realizar por personal propio de la organización o en un lugar externo. Se debe establecer programas |
| Proteccion de los servicios de comunicaciones | Asegurar la protección de los servicios de comunicaciones |
| Herramienta de chequeo de configuraciones | Debe implementarse un sistema de chequeo de configuraciones |

*Figura 13. Controles del servidor*

En la tabla 11 se observa el peso considerado para los parámetros de oportunidad, automatización y estandarización de los controles del ISP, se colocó puntajes más altos a los parámetros que ayudan a fortalecer el control.

*Tabla 11. Calificación de los controles*

| Parámetro Oportunidad | Calificación |
|---|---|
| Preventivo | 3 |
| Detectivo | 2 |
| Correctivo | 1 |
| **Parámetro Automatización** | **Calificación** |
| Automatizado | 3 |
| Semi Automatizado | 2 |
| Manual | 1 |
| **Parámetro Estandarización** | **Calificación** |
| Implementado Ad-hoc | 1 |
| Implementado/Estandarizado | 2 |

Posteriormente se realizó una tabulación la cual ayudó a determinar el nivel de fortaleza del control de la organización, como se observa en la tabla 12.

*Tabla 12. Calificación de fortaleza de controles*

| Nivel | Calificación |
|---|---|
| **Fuerte** | **7 a 8** |
| **Moderado** | **5 a 6** |
| **Débil** | **3 a 4** |

En la figura 14 se puede visualizar la fortaleza de cada control obtenida mediante la consideración de los parámetros calificación, en algunos casos se observa que el ISP cuenta con controles fuertes, pero hay muchos controles que deben mejorar para que la organización sea resiliente ante exposición de alguna vulnerabilidad.

| Controles | Descripcion del Control | Oportunidad | Automatización | Estandarización | Fortaza Control |
|---|---|---|---|---|---|
| Aseguramiento de la disponibilidad | Asegura que los servidores esten disponibles | Preventivo | Semi Automatizado | Implementado Ad-hoc | Moderado |
| Protección de los equipos | Los servidores deben situarse de forma que reduzcan los riesgos de amenzas y oportunidades que produzcan accesos no autorizados | Detectivo | Manual | Implementado Ad-hoc | Débil |
| Backup eléctrico | Es necesario contar con un backup eléctrico, disponer de alarmas de detección de fallas eléctricas y activación de backup | Preventivo | Manual | Implementado/Estandarizado | Moderado |
| Realizar actualizaciones necesarias y mantenimiento a l | Los servidores deben recibir mantenimiento correcto teniendo en cuentra si se va a realizar por personal propio de la organización o en un lugar externo. Se debe | Preventivo | Semi Automatizado | Implementado/Estandarizado | Fuerte |

*Figura 14. Fortaleza de controles*

Luego de obtener la fortaleza de los controles se realizó un análisis de las vulnerabilidades respecto al impacto y probabilidad que pueden tener en la organización. Para esta consideración se tomó como referencia el parámetro oportunidad del control en el caso de ser un control preventivo la fortaleza de este control ayudará a determinar la probabilidad de la vulnerabilidad y en el caso de ser un control detectivo o correctivo la fortaleza del control ayudará a determinar el impacto que tendría esta vulnerabilidad en el ISP, como se observa en la figura 15.

| Controles | Descripcion del Control | Oportunidad | Automatización | Estandarización | Fortaza Control | Falta de aseguramiento de la disponibilidad | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Impacto | Probabilidad |
| | | | | | | | Débil | Moderado |
| | | | | | | Relación Control / Vulnerabilidad | # de controles que afectan | |
| | | | | | | | 1 | 6 |
| Aseguramiento de la disponibilidad | Asegura que los servidores esten disponibles | Preventivo | Semi Automatizado | Implementado Ad-hoc | Moderado | x | | |
| Protección de los equipos | Los servidores deben situarse de forma que reduzcan los riesgos de amenzas y oportunidades que produzcan accesos no autorizados | Detectivo | Manual | Implementado Ad-hoc | Débil | | | |
| Backup eléctrico | Es necesario contar con un backup eléctrico, disponer de alarmas de detección de fallas eléctricas y activación de backup | Preventivo | Manual | Implementado/ Estandarizado | Moderado | x | | |

*Figura 15. Controles del ISP*

Después de analizar las fortalezas de los controles se procedió a elaborar un plan de acción el cual ayudará a la organización al mejoramiento de los controles con la finalidad de reducir los riesgos, como se observa en la figura 16.

| Activo Servidor | | | |
|---|---|---|---|
| **Control** | **Oportunidad de mejora** | **Roadmap** | **Responsable** |
| Aseguramiento de la disponibilidad | Es recomendable tener pantallas que proyecten el estado actual de cada servidor | 6 meses | Personal de compras |
| Protección de los equipos | Implementar seguridades físicas para que sólo personal autorizado pueda acceder a los servidores. | 3 meses | Jefe tecnico |
| Backup eléctrico | Adquirir un sistema electrógeno que cuente con alarmas de detección de fallas eléctricas y activación automática del backup eléctrico | 9 meses | Personal de compras |
| Realizar actualizaciones necesarias y mantenimiento a los equipos | Colocar en el sistema agendamiento de cada mantenimiento de los servidores detallando fecha y hora | 6 meses | Desarrollador |
| Proteccion de los servicios de comunicaciones | Implementar seguridades físicas con MFA para que sólo personal autorizado pueda acceder a los servicios de comunicaciones | 2 meses | Jefe tecnico |
| Herramienta de chequeo de configuraciones | Implementar un sistema que permita revisar las configuraciones que fueron realizadas detallando el responsable, fecha y hora. | 6 meses | Jefe tecnico |
| Control de cambios de configuracion | | | |

*Figura 16, Plan de acción del activo critico servidor*

Una vez obtenido el impacto y probabilidad se relacionaron las vulnerabilidades y amenazas con la ayuda de la figura 12 de esta manera se pudo obtener la mitigación del impacto y probabilidad de cada amenaza.

Posteriormente se realizó un análisis aplicando controles al riesgo inherente de esta manera se pudo obtener el riesgo residual de cada amenaza del activo crítico servidor, como se observa en la figura 17.

| | Servidor | | | | Inherencia | | | Controles | | Residual | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Amenazas | Vulnerabiliadad | Impacto Seguridad | Impacto Organizacional | Probabilidad Inherente | Impacto Inherente | Severidad Inherete | Mitigación Probabilidad | Mitigación Impacto | Probabilidad Residual | Impacto Residual | Severidad Residual |
| 1 | Desastres Naturales | Falta de aseguramiento de la<br>Falta de protección de los equipos | Disponibilidad | Interrupción de operaciones | Poco Probable | Catastrofico | Alto | Moderado | Débil | Raro | Catastrofico | Alto |
| 2 | Corte de suministro electrico | No se tiene un backup eléctrico<br>Falta de aseguramiento de la | Disponibilidad | Interrupción de operaciones | Posible | Mayor | Alto | Moderado | Débil | Poco Probable | Mayor | Medio |
| 3 | Averia de origen fisico | No se han realizado actualizaciones y mantenimiento a los equipos | Disponibilidad | Interrupción de operaciones | Probable | Mayor | Critico | Fuerte | Débil | Poco Probable | Mayor | Medio |

*Figura 17. Riesgo residual del activo crítico servidor*

Luego se realizó el mismo análisis para el activo critico Bases de Datos, el resultado del análisis se puede visualizar en la figura 18.

| | Base de Datos | | | Inherencia | | | Controles | | Residual | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Amenazas | Impacto Seguridad | Impacto Organizacional | Probabilidad Inherente | Impacto Inherente | Severidad Inherete | Mitigación Probabilidad | Mitigación Impacto | Probabilidad Residual | Impacto Residual | Severidad Residual |
| 1 | Errores de los usuarios | Disponibilidad | Interrupción de operaciones | Probable | Moderado | Alto | Moderado | Débil | Posible | Moderado | Medio |
| 2 | Errores de administrador | Disponibilidad | Interrupción de operaciones | Posible | Moderado | Medio | Moderado | Débil | Poco Probable | Moderado | Medio |
| 3 | Errores de configuración | Disponibilidad | Interrupción de operaciones | Casi Certero | Mayor | Critico | Moderado | Débil | Probable | Mayor | Critico |
| 4 | Difusión de software maligno | Disponibilidad | Pérdidas financieras | Posible | Mayor | Alto | Moderado | Débil | Poco Probable | Mayor | Medio |

*Figura 18. Riesgo residual del activo crítico BDD*

## Resultados

Como resultado del análisis del activo critico servidor se obtuvo un mapa de calificación del riesgo en el cual se colocaron las amenazas con su respectivo riesgo inherente y la mejora que se obtendría con el riesgo residual, como se observa en la figura 19.

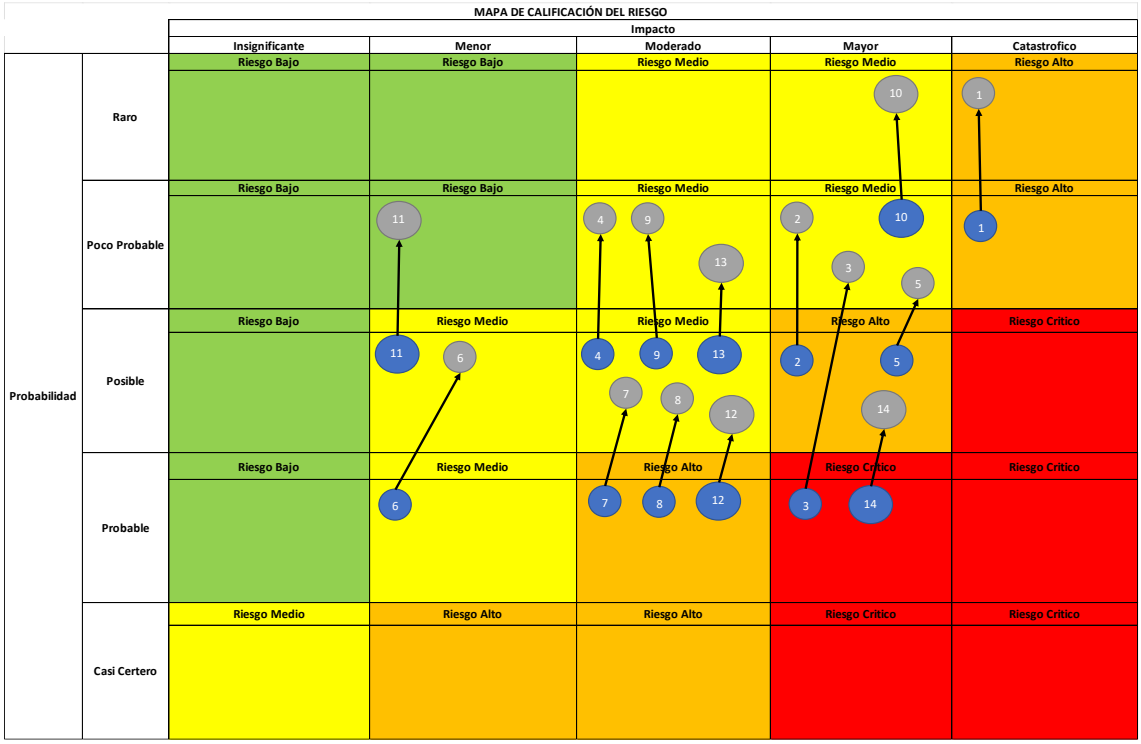


*Figura 19. Mapa de calificación del riesgo del activo crítico servidor*

En la figura 20 se observa el mapa de calificación del riesgo del activo crítico BDD.

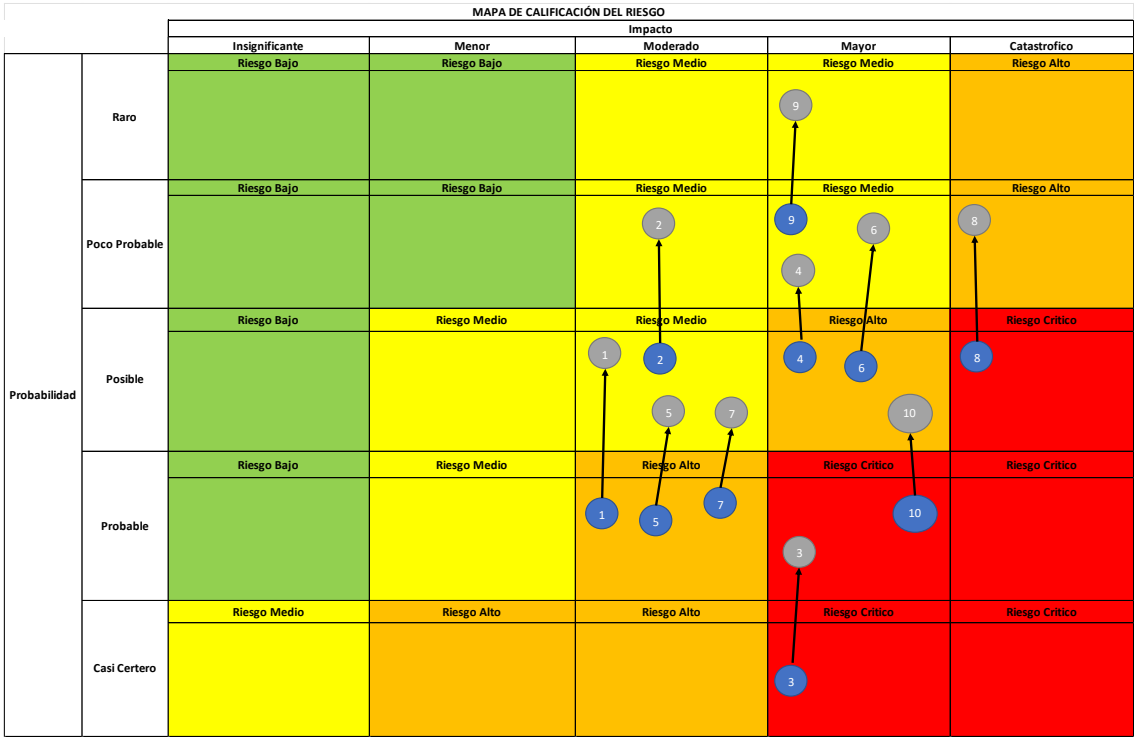


*Figura 20. Mapa de calificación del riesgo del activo crítico BDD*

## Referencia Anexos

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Amenazas del servidor” se puede encontrar el análisis de amenazas y riesgo del activo servidor.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Controles del Servidor” se puede encontrar el análisis de los controles de la organización para el servidor.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Amenazas BDD” se puede encontrar el análisis de amenazas y riesgo del activo base de datos.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Controles BDD” se puede encontrar el análisis de los controles de la organización para la base de datos.

En el anexo Proyecto CAPSTONE.xlsx en la pestaña “Planes de Acción” se puede encontrar el roadmap de los planes de acción que se proponen para los controles de cada activo.

## Fase 5: Documentos clave del SGSI

Las políticas de alto nivel establecen y confirman el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del SGSI. (ISO27000, 2005)

### Metodología

En la fase 5 se definieron las políticas de alto nivel del sistema de gestión de seguridad de la información del ISP tomando como referencia la norma ISO27002 (Asociación Española de Normalización, 2017), las mismas que deben ser aprobadas por la alta dirección de la organización. Una vez que las políticas se encuentren aprobadas deberán ser socializadas a todo el personal del ISP.

### Referencia Anexos

En el anexo Politicas.docx puede encontrar las políticas de seguridad que se propusieron para la organización.

## CONCLUSIONES Y RECOMENDACIONES

## CONCLUSIONES

El desarrollo del sistema de gestión de seguridad de la información del ISP permitió conocer las falencias que presenta, en el análisis se encontraron varias cláusulas se encuentran implementadas pero la organización aun no las ha documentado, por tal motivo hay varias oportunidades de mejora en el ISP.

La clasificación de la información permitió a la organización conocer los diferentes tipos de información existentes que puede tener una entidad. Con esto se pudo observar que cada tipo de información requiere diferentes criterios de protección.

El inventario de activos de información permitió conocer el tipo de información que maneja cada activo de esta manera se pudo determinar cuáles son los más críticos y por ende cuales son los que requieren ser intervenidos.

El análisis de las amenazas y vulnerabilidades permitió conocer los riesgos a los que está expuesta la organización proponer un plan de acción para mejorar los controles de la organización permitiéndole reducir las brechas de seguridad a las que el ISP se encuentra expuesto.

## RECOMENDACIONES

Realizar un análisis sobre los demás activos críticos de la organización para así tener una completa visión de todos los riesgos a los que la organización puede estar expuesta.

Implementar el área de seguridad en la organización y a su vez contratar servicios profesionales para el seguimiento de las mejoras continuas y planes de acción propuestos.

Conocer los marcos de referencia para saber cuáles son los que se pueden utilizar y que se puedan ajustar a la organización, con la finalidad de utilizar las mejores prácticas que ayuden al análisis.

## BIBLIOGRAFIA


Alonso, C. (02 de 04 de 2020). *Apetito del riesgo. Gestión de Riesgos corporativos*. Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/apetito-del-riesgo/

Asociación Española de Normalización. (2017). *ISO/IEC 27001:2013.* Madrid.

Asociación Española de Normalización. (2017). *ISO/IEC 27002:2013.* Madrid.

Center for Internet Security. (2022). *CIS Critical Security Controls Version 8.* Obtenido de Center for Internet Security : https://www.cisecurity.org/controls/v8

ISACA. (2018). Cobit 2019: Objetivos de gobierno y gestión.

ISO27000. (2005). *iso27000.es*. Obtenido de https://www.iso27000.es/sgsi.html

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

# ANEXOS

## Proyecto CAPSTONE.xlsx

Proyecto CAPSTONE.xlsx

## Políticas.docx

Politicas.docx

## Caso de Negocios.pptx

Caso de Negocios.pptx

## Enlace carpeta compartida

Proyecto CAPSTONE