# ANÁLISIS PARA LA IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN A UNA ENTIDAD PÚBLICA DEL ORDEN TERRITORIAL EN EL DEPARTAMENTO DEL VALLE DEL CAUCA.

**JHON JAIRO MONTOYA CORTES**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**
**ESCUELA DE CIENCIAS BÁSICAS DE LAS TECNOLOGÍAS Y LA INGENIERÍA**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**PALMIRA**
**2020**

# ANALISIS PARA LA IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN A UNA ENTIDAD PÚBLICA DEL ORDEN TERRITORIAL EN EL DEPARTAMENTO DEL VALLE DEL CAUCA.

**JHON JAIRO MONTOYA CORTES**

Trabajo de grado para optar **por título:**
**Especialista en Seguridad Informática**

**Director de Proyecto:**
**Ing. Joel Carroll Vargas M.Sc**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**
**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**
**ESPECIALIZACION EN SEGURIDAD INFORMÁTICA**
**PALMIRA**
**2020**

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

El Cerrito Valle, 01 de agosto de 2020

## DEDICATORIA

Dedico este trabajo primeramente a Dios Nuestro Padre Celestial, por haberme dado las fuerzas, la salud y la sabiduría para seguir adelante con este proyecto de vida. A mi esposa Millerlandy por ser esa ayuda idónea e incondicional y a mi hijo Juan Manuel por ser mi fuente de motivación constante y por la comprensión del tiempo invertido durante el estudio y que no pude dedicarles para disfrutar en familia.

**JHON JAIRO MONTOYA CORTES**

## AGRADECIMIENTOS

Agradezco primeramente a Nuestro Señor Jesucristo por ser el Señor de mi vida y quien me sostiene en todo momento, a mi familia, a mis padres y a mis hermanos, quienes siempre me han apoyado para salir adelante. Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, y principalmente al grupo de profesores que me han orientado a lo largo de mi carrera, en especial al Ingeniero y Magister Joel Carroll Vargas, quien fue mi director del trabajo de grado y a la Ingeniera y Magister Katerine Márceles, quien fue asignada como jurado de grado para la sustentación de este proyecto.

**JHON JAIRO MONTOYA CORTES**

**CONTENIDO**

Pág.

INTRODUCCIÓN ..... 13
1. DEFINICIÓN DEL PROBLEMA ..... 14
1.1. ANTECEDENTES DEL PROBLEMA ..... 14
1.2. FORMULACIÓN DEL PROBLEMA ..... 15
2. JUSTIFICACIÓN ..... 16
3. OBJETIVOS ..... 18
3.1. OBJETIVO GENERAL ..... 18
3.2. OBJETIVOS ESPECÍFICOS ..... 18
4. MARCO REFERENCIAL ..... 19
4.1. MARCO TEÓRICO ..... 19
4.1.1 Importancia de un MSPI dentro de una organización. ..... 22
4.1.2 Requerimiento de análisis y evaluación de riesgo activos de información. ..... 23
4.1.3 Impacto de un plan de tratamiento del riesgo en una organización ..... 23
4.2. MARCO HISTORICO ..... 24
4.2.1. Estructura Organizacional del Área de Informática. ..... 25
4.3. ANTECEDENTES ..... 26
4.4 . MARCO LEGAL ..... 28
4.5 MARCO CONCEPTUAL ..... 30
4.5.1. Modelo de seguridad de la información ..... 30
4.5.2. Gestión del riesgo ..... 30
4.5.3. Sistema de gestión de seguridad de la información ..... 30
4.5.4. Plan de tratamiento del riesgo ..... 30
4.5.5 Metodología de gestión de riesgo informático ..... 31
5. DISEÑO METODOLOGICO ..... 32
6. DESARROLLO DE LOS OBJETIVOS ..... 34
6.1. FASE 1: REALIZAR LA VALORACION A LOS ACTIVOS Y CLASIFICAR LOS RIESGOS CON BASE A LA DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACION. ..... 34
6.1.1. Conclusiones primer objetivo. ..... 45

6.2. FASE 2: DETECTAR LAS POSIBLES AMENAZAS Y VULNERABILIDADES CON BASE A LOS RIESGOS IDENTIFICADOS EN LA ENTIDAD. ..... 46
6.2.1. Conclusiones segundo objetivo. ..... 51
6.3. FASE 3: DISEÑAR UNA MATRIZ CON EL PLAN DE TRATAMIENTO DE LOS RIESGOS DETECTADOS EN LA ENTIDAD. ..... 52
6.3.1. Conclusiones tercer objetivo. ..... 61
7. CONCLUSIONES ..... 62
8. RECOMENDACIONES ..... 63
BIBLIOGRAFIA ..... 64

## LISTA DE FIGURAS

Pág.

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información. .....20
Figura 2. Estructura Organizacional del Área de Informática. .....25

## LISTA DE TABLAS

Pág.

Tabla 1. Tabla comparativa por tipo de análisis (cuantitativo, cualitativo y mixto). 35
Tabla 2. Tabla comparativa por elementos de la metodología. .....36
Tabla 3. Tabla comparativa por objetivos de seguridad.....37
Tabla 4. Tabla de resultados.....37
Tabla 5. Probabilidad del Riesgo. .....40
Tabla 6. Impacto del Riesgo. .....41
Tabla 7. Modelo del Riesgo. .....41
Tabla 8. Valoración del Riesgo. .....42
Tabla 9. Valorización cualitativa y clasificación de activos. .....43
Tabla 10. Valoración cuantitativa y clasificación de los riesgos. .....44
Tabla 11. Identificación de amenazas y vulnerabilidades. .....49
Tabla 12. Identificación de amenazas y vulnerabilidades. .....50
Tabla 13. Probabilidad de Vulneración. .....52
Tabla 14. Criticidad Neta. .....53
Tabla 15. Calificación de Gestión. .....53
Tabla 16. Controles o Salvaguardas Actuales. .....54
Tabla 17. Criticidad Residual. .....55
Tabla 18. Nivel de Aceptación. .....55
Tabla 19. Matriz plan de tratamiento del riesgo. .....56
Tabla 20. Matriz plan de tratamiento del riesgo. .....57
Tabla 21. Controles para el plan de tratamiento del riesgo.....58
Tabla 22. Controles para el plan de tratamiento del riesgo.....59
Tabla 23. Controles para el plan de tratamiento del riesgo.....60

## GLOSARIO

A continuación, se presentan algunos conceptos relacionados con el tema del proyecto de investigación:

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

**Riesgo:** Posibilidad de que se produzca un contratiempo o amenaza y se pueda presentar perdida de información.

**Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## RESUMEN

Este proyecto aplicado está enfocado a realizar un análisis para la implementación de un modelo de seguridad y privacidad de la información a una entidad pública real, haciendo uso de las guías que establece el Ministerio de las Tecnologías de la información y comunicaciones para las entidades públicas del orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital. Este proyecto busca generar la confidencialidad, integridad y disponibilidad sobre la información de una entidad pública del orden territorial en el departamento del Valle del Cauca.

Durante el desarrollo de este proyecto, utilizando la metodología Magerit se realizó una valoración a los activos y se clasificaron los riesgos, logrando identificar que en la entidad se presentan varias clases de riesgos como son: la modificación no autorizada de la información, divulgación no autorizada de información confidencial, acceso no autorizado a la información, indisponibilidad de la información entre otros, comprometiendo la disponibilidad, confidencialidad e integridad de la información. Con base a los riesgos identificados se detectaron las posibles amenazas y vulnerabilidades, y se realizó una matriz con el plan de tratamiento de los riesgos.

## ABSTRACT

This project is focused to perform an analysis for the implementation of a security and privacy model for the information to a real public entity, using the guides established by Ministry of Information and Communication Technologies. For the public entities of the national and territorial order, just like online government service providers and third parties who wish adopt the security and privacy model of the information in the framework of the digital government strategy. This project looks to guarantee the confidentiality, integrity and availabily of information of a public entity of the territorial order in the department of Valle del Cauca.

During the development of this project, using the Margerit methodology, assets were evaluated and risks were classified managing to identify that the entity presents many types of risk such as unauthorized modification of information, unauthorized disclosure of confidential information, unauthorized access to information, unavailability of information among others, compromising the availability, confidentiality and integrity of the information. Based on the risks identified potential threats and vulnerabilities were detected, and a matrix was made with the risk treatment plan.

# INTRODUCCIÓN

El presente trabajo de investigación está elaborado con el objetivo fundamental de ofrecer a una entidad pública del orden territorial en el departamento del Valle del Cauca, un análisis para la implementación de un modelo de seguridad y privacidad de la información que genere la confidencialidad, integridad y disponibilidad de la información.

La tecnología cada día avanza a grandes pasos y esto hace que la información manejada sea mucho mayor, por ejemplo: cuando se usa el celular, la tablet, el portátil o el equipo de escritorio en las empresas, se está procesando mucha información por las redes locales o por el internet. Esto hace que los delincuentes informáticos se enfoquen en estudiar las vulnerabilidades de las redes y realicen diferentes ataques para lograr apoderarse o secuestrar la información importante de las empresas, haciendo que se pierda la confidencialidad, integridad y disponibilidad de la información que es el activo más valioso e importante para las empresas, ya que es allí donde tienen la información de sus clientes o proveedores y si llega a manos de la competencia, sería un riesgo enorme. Para ampliar más esta información de cómo los delincuentes informáticos se pueden apoderar de la información, se toma el informe realizado por la empresa ESET “La seguridad como rehén tendencias 2017”[1]

Por todo lo anterior, se vé necesario a realizar un análisis para la implementación de un modelo de seguridad y privacidad de la información en una entidad pública del orden territorial en el departamento del Valle del Cauca que por motivos de seguridad para evitar posibles ataques cibernéticos no se puede revelar su nombre, a la cual se le realizará un análisis de los riesgos, amenazas, vulnerabilidades, y se establecerán unas políticas que permitan mantener la confidencialidad, integridad y disponibilidad de la información.

[1] ESED. TENDENCIAS 2017. La seguridad como Rehén. [Consultado el 21 de enero de 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1. ANTECEDENTES DEL PROBLEMA

La entidad pública del orden territorial ubicada en el departamento del Valle del Cauca, que por motivos de seguridad no se revela su nombre para evitar posibles ataques cibernéticos, la cual tiene como objetivos principales velar por el bienestar de la comunidad, promover la prosperidad general y garantizar el cumplimiento de los principios, derechos y deberes, contenidos en la Constitución Política de Colombia, promover la participación ciudadana en todos los aspectos económicos, políticos, administrativos, culturales en pro de mejorar la calidad de vida y las condiciones de todos los habitantes.

Actualmente el sistema de información de la entidad estatal presenta falencias que pueden hacer vulnerable la información. Dentro de los inconvenientes más representativos en la entidad, se encuentran los siguientes:

**No se cuenta con un servidor de controlador de dominio local:** la entidad no cuenta con un servidor de dominio que permita establecer mecanismos de seguridad en cuanto al uso de los equipos tecnológicos por parte de los usuarios, como por ejemplo: establecer contraseñas de acceso que se tengan que renovar cada determinado tiempo, horarios de uso de los equipos y acceso a carpetas compartidas con permisos de edición o solo lectura de acuerdo a los permisos habilitados al usuario.

**Los usuarios acceden a páginas que no están relacionadas con sus actividades:** muy a menudo los usuarios de los equipos tecnológicos acceden a páginas web con contenidos que no se requieren para el desarrollo de sus actividades laborales, haciendo más vulnerable la información, y consumiendo recursos como el ancho de banda, ya que por medio de estos sitios web no seguros se puede presentar descarga de virus o algún tipo de software con código malicioso como un malware o spyware.

**No se cuentan con unas políticas de Backup de la información definidas:** la entidad no ha definido unas políticas para la generación del backup como son (frecuencia, tipo de backup, persona responsable, medios de almacenamiento, entre otros), generando un riesgo de pérdida de información.

**No se cuenta con una licencia propia de un software antivirus que proteja la información:** Actualmente se utiliza un software antivirus gratuito que no garantiza la protección de la información por parte de un proveedor especializado en software antivirus y que brinde soporte para tal fin.

## 1.2. FORMULACIÓN DEL PROBLEMA

¿Cuál sería la metodología adecuada para implementar un modelo de seguridad y privacidad de la información a una entidad pública del orden territorial en el departamento del Valle del Cauca que cumpla con la normatividad, estándares y que disminuya la probabilidad de pérdida de la información en la entidad?

Antes de identificar la metodología adecuada para la implementación de un modelo de seguridad de la información, es necesario también responder las siguientes preguntas:

¿En qué nivel de seguridad y privacidad se encuentra actualmente el proceso de la información y cuáles son los riesgos inherentes a estos niveles en una entidad pública del orden territorial en el departamento del Valle del Cauca?; ¿Por qué se pueden presentar las deficiencias que hacen vulnerable la información en esta entidad pública del orden territorial?; ¿Cuáles deberían ser las medidas correctivas y preventivas para dar seguimiento a estas deficiencias en pro de un óptimo sistema de seguridad y privacidad de la información en dicha entidad?

Estos interrogantes son importantes de resolver, ya que por medio de sus respuestas se puede saber sí la entidad está aplicando una metodología que permita establecer un nivel de seguridad de la información, donde no se ponga en riesgo la confidencialidad, disponibilidad e integridad de la misma.

## 2. JUSTIFICACIÓN

El ministerio de las TIC´S mediante el decreto 2573 de 2014, de la mano con los entes de control encargados de vigilar y procurar el buen uso de los recursos y bienes públicos; además de contribuir a la modernización del Estado, mediante acciones de mejoramiento continuo en las distintas entidades públicas y de ejercer un control disciplinario, como son la contraloría general y procuraduría, están exigiendo a las entidades públicas del orden nacional y territorial, el fortalecimiento de los procesos de Seguridad y Privacidad de la Información, la cual hace parte de la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión, y que además conlleva todo un despliegue de recursos tanto económicos, financieros y estratégicos para poder garantizar que lo que se planeó en el Plan Estratégico de Tecnologías de la Información demuestre condiciones de confidencialidad, integridad y disponibilidad.

Por lo anterior, y debido a que la entidad pública no cuenta con un plan o modelo de gestión de la información y actualmente tiene muchas deficiencias en la seguridad de la misma, se hace necesario entonces realizar un análisis para la implementación de un modelo de seguridad y privacidad de la información que le permita a la entidad pública saber en qué estado se encuentra en cuanto a la seguridad de la información y cuáles serían los activos de información que más requieren atención según las amenazas y vulnerabilidades detectadas, para establecer un plan de tratamiento, que les facilite la planificación para la puesta en marcha del modelo de seguridad de la información con base a los resultados obtenidos en la fase de diagnóstico.

Adicionalmente se requiere brindar solución a los siguientes inconvenientes planteados como son:

**Instalación de un controlador de dominio:** se plantea unos procesos a implementar para uso de los usuarios que brinden mayor seguridad a la información. En este caso se hace necesario que los usuarios internos deban renovar cada determinado tiempo sus contraseñas para evitar que personas ajenas a la entidad tengan acceso a ellas. La implementación de horarios de uso de los equipos y la restricción a determinada información y el acceso a carpetas compartidas con permisos de edición o sólo lectura de acuerdo a los niveles de autorización establecidos por la entidad.

**Los usuarios acceden a páginas que no están relacionadas con sus actividades:** se deben establecer procedimientos para restringir el uso por parte

del personal tanto interno como externo de sitios web no seguros, para evitar que se puedan presentar descarga de virus o algún tipo de software con código malicioso como un malware o spyware.

**No se cuentan con unas políticas de Backup de la información definidas:** se debe implementar un procedimiento para la realización del backup de los servidores. Se hace necesario la designación del personal encargado, los horarios establecidos y los medios definidos para tal fin, evitando la pérdida de la información.

**No se cuenta con una licencia propia de un software antivirus que proteja la información:** Se recomienda la adquisición de un software antivirus de excelente calidad que proporcione mayor protección del sistema de información.

# 3. OBJETIVOS

## 3.1. OBJETIVO GENERAL

Realizar un análisis para la implementación de un Modelo de Seguridad y Privacidad de la Información con base a los lineamientos de Gobierno Digital del Ministerio de las TIC utilizando la norma ISO/IEC 27001:2013, que permita detectar los posibles riesgos de seguridad de la información que presenta la entidad, con el fin de facilitar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad pública.

## 3.2. OBJETIVOS ESPECÍFICOS

- Realizar una valoración a los activos con que cuenta actualmente la entidad, y clasificar los riesgos con base a la disponibilidad, confidencialidad e integridad de la información.

- Detectar las posibles amenazas y vulnerabilidades con base a los riesgos identificados en la entidad.

- Diseñar una matriz con el plan de tratamiento de los riesgos detectados en la entidad.

# 4. MARCO REFERENCIAL

## 4.1. MARCO TEÓRICO

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la política digital: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.[2]

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.[2]

Dentro de este proyecto se tiene en cuenta diferentes fuentes de información, entre ellas los manuales para la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio de las Tecnologías de la Información - MINTIC fuentes en línea principalmente trabajos de grado y libros que tratan el tema de los Modelos de Seguridad y Privacidad de la Información.

La norma ISO/IEC 27001:2013 estipula que debe utilizarse un método de análisis de riesgo; sin embargo, no se propone ningún método específico, aparte de la integración del proceso recursivo PDCA (Plan, Do, Check, Act) del modelo definido para la creación del SGSI.[3]

El ciclo de operación del Modelo de Seguridad y Privacidad de la Información, se basa en 5 fases que lo comprenden:

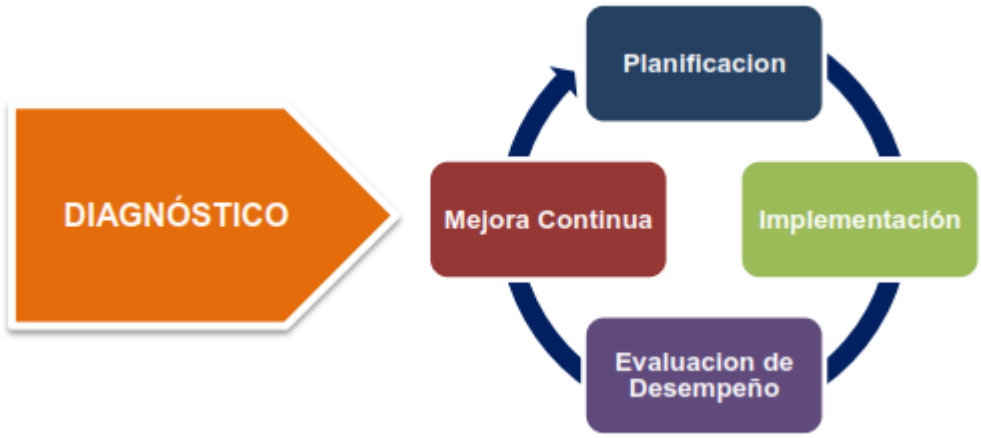
Se inicia con una fase de diagnóstico, donde se debe emplear el modelo PHVA que es el de Planear, Hacer, Verificar y Actuar.

---

[2] MINTIC, Modelo de seguridad. Fortalecimiento de la gestión TI en el estado. [en línea]. Bogotá DC. [consultado 01, febrero, 2020]. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

[3] CASTO, Pablo, Metodología Magerit. [en línea]. (septiembre 2014). [Consultado: 02 de noviembre de 2019]. Disponible en: http://gr2dest.org/metodologia-de-analisis-de-riesgosmagerit/

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información.




Fuente: MinTIC. Modelo de seguridad y privacidad de la información [en línea]. Seguridad y privacidad de la información. Bogotá. (29 de julio de 2016). [Consultado: 30 de enero de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

En esta primera fase que es de **DIAGNÓSTICO** se deben realizar las siguientes etapas:

- Verificar el estado actual en el que está la entidad referente a la seguridad y privacidad de la información.
- Identificar el nivel de madurez en el que se encuentra la entidad referente a la seguridad y privacidad de la información.
- Levantar la información necesaria para la implementación, como por ejemplo: identificar las vulnerabilidades que puedan servir de insumo para la siguiente fase que es la de planificación.

Después de la fase de diagnóstico se debe seguir con la segunda fase que es la de **PLANIFICACIÓN**, la cual se inicia con los resultados obtenidos de la etapa anterior que era la de diagnóstico, y de esta manera proceder a la elaboración del plan de seguridad y privacidad de la información, teniendo en cuenta que este se debe alinear con el objetivo misional de la entidad.

Se deben tener en cuenta unas recomendaciones para lograr desarrollar el alcance y los límites del Modelo de Seguridad y Privacidad de la Información - MSPI como, por ejemplo: procesos, servicios, sistemas de información, terceros relacionados, ubicaciones físicas y procesos que pueden impactar directamente la consecución de objetivos misionales. Para esto se establecen las siguientes metas:

- Crear un manual con las políticas de seguridad y privacidad de la información, las cuales deben estar aprobadas y socializadas por la alta dirección de la entidad al interior de la misma.
- Establecer unos procedimientos los cuales deben ser debidamente documentados, aprobados y socializados por el comité que integra los sistemas de gestión en la entidad.
- Elaborar un acto administrativo donde se establezcan los roles y las responsabilidades del personal encargado de la Seguridad y Privacidad de la Información, el cual debe ser revisado y aprobado por la alta dirección.
- Realizar un inventario de los activos de información, aplicando una metodología para identificación, clasificación y valoración, el cual debe ser validado por el comité de Seguridad de la Información y revisado por la alta gerencia.
- Integrar el Modelo de Seguridad y Privacidad de la Información con el Sistema de Gestión Documental de la entidad.
- Realizar la identificación, valoración y tratamiento de riesgos, haciendo documentos donde se evidencie la metodología, el análisis y evaluación de los riesgos, el plan de tratamiento, la declaración de aplicabilidad, los cuales deben ser revisados por la alta gerencia.
- Elaborar un documento con el plan de comunicación, sensibilización y capacitación.
- Elaborar un plan de diagnóstico para la transición de IPv4 a IPv6.

Luego de la fase de planificación se debe seguir con la tercera fase que es la de **IMPLEMENTACIÓN**, la cual se debe llevar a cabo después de la planificación que se realizó en la fase anterior. Para esto se deben establecer las siguientes metas:

- Elaborar documento con la planificación y control operacional, el cual debe ser revisado y aprobado por la alta dirección.
- Elaborar un informe de la ejecución del plan de tratamiento de riesgos, el cual debe ser aprobado por el dueño de cada uno de los procesos.
- Elaborar un documento donde se describan los indicadores de gestión de Seguridad y Privacidad de la Información.

- Elaborar un documento que muestre las estrategias del plan de implementación de IPv6 en la entidad, el cual debe ser aprobado por la oficina o persona encargada del área de sistemas.

La cuarta fase es la de **EVALUACION DE DESEMPEÑO** que consiste en realizar un seguimiento y monitoreo al MSPI con base a los resultados que estarían arrojando los indicadores de la seguridad de la información.

Las metas, resultados e instrumentos de esta fase consisten en:

- Un plan de revisión y seguimiento a la implementación del modelo, donde se debe obtener un documento que contenga el plan de seguimiento y revisión del MSPI el cual debe estar revisado y aprobado por la alta dirección.
- Un plan de ejecución de las auditorias, al cual se le debe generar un documento con el plan de ejecución de las auditorias y revisiones independientes al modelo, el cual debe ser revisado y aprobado por la Alta Dirección.

La quinta y última fase es la de **MEJORA CONTINUA** donde la entidad consolida los resultados obtenidos de la fase anterior para lograr diseñar un plan de mejoramiento continuo al modelo de seguridad y privacidad de la información que permita tomar acciones al instante para mitigar las debilidades que se identificaron, y para ello se debe crear los siguientes documentos:

- Documento con el plan de mejoramiento.
- Documento con el plan de comunicación de resultados.

**4.1.1 Importancia de un MSPI dentro de una organización.** Es muy importante que las empresas u organizaciones tengan muy claro que se debe implementar un modelo de seguridad y privacidad de la información, ya que la información está clasificada como un activo intangible que se debe proteger y preservar, además toda empresa debe conocer el nivel de seguridad y privacidad de la información que maneja porque es de vital importancia que se promuevan condiciones de ciberseguridad en cada uno de los dispositivos conectados a la red de datos que posee la empresa. Cuando las organizaciones implementan un MSPI están preservando la confidencialidad, integridad, disponibilidad y privacidad de la información.

**4.1.2 Requerimiento de análisis y evaluación de riesgo activos de información.** Los sistemas de información, al igual que los datos que se manejan en ellos son activos de información muy valiosos para las organizaciones, y por eso es muy importante que se cuenten con mecanismos de protección frente a posibles ataques o intrusiones que aprovechen las vulnerabilidades en su sistema de seguridad. Para minimizar el impacto que esto puede ocasionar se debe descubrir las vulnerabilidades y amenazas de una manera efectiva, realizando procesos diagnósticos que permitan establecer el estado actual de la seguridad de la información en la organización.

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación.

El diagnóstico permitirá en un futuro el diseño, implementación e implantación de un Sistema de Gestión de Seguridad de la Información - SGSI alineado al estándar ISO/IEC 27001, capaz de controlar las vulnerabilidades, amenazas y los riesgos de seguridad a que se ve expuesta la organización. [4]

**4.1.3 Impacto de un plan de tratamiento del riesgo en una organización.** Luego de haber realizado un análisis y evaluación de riesgo a los activos de información en la organización, se debe establecer un plan de tratamiento del riesgo, donde se deberá seleccionar la opción del tratamiento que se aplicará a cada uno, bien sea que se evite o no se proceda con la actividad o la acción que está dando origen a ese riesgo, también se puede transferir o compartir el riesgo entregándoselo a un tercero, otra opción sería reducirlo o mitigarlo, implementando controles o medidas que logren reducir la probabilidad o el impacto que ese riesgo pueda causar, y la última opción sería retenerlo o aceptarlo sin implementar medidas de control adicionales, pero si monitorizándolo constantemente para que no se vaya a incrementar. De esta manera se estaría generando un gran impacto en la organización al implementar un plan de

[4] SOLARTE SOLARTE, Francisco J, ENRIQUEZ ROSERO, Edgar R y BENAVIDES RUANO Miriam del C. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, 2015. [Consultado el 12 de diciembre de 2020]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/download/456/321

tratamiento del riesgo con cualquiera de las opciones de tratamiento mencionadas anteriormente, teniendo en cuenta el costo/beneficio.

## 4.2. MARCO HISTORICO

La entidad pública que por motivos de seguridad no se revela su nombre para evitar posibles ataques cibernéticos, tiene como misión asegurar el bienestar de la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución, facilitando la participación ciudadana en las decisiones que los afectan y en la vida económica, política, administrativa y cultural, para mejorar la calidad de vida y las condiciones económicas de todos los habitantes principales, y cuya visión es ser una entidad pública líder, competitiva, con un modelo de desarrollo institucional que promueve la democratización de la gestión pública y la optimización de mecanismos de información, concertación y consenso, con acreditados niveles de confianza y transparencia en la gestión de lo público, mediante prácticas de gobernanza, buen gobierno y de gerencia pública, con evaluación y mejora permanente de los procesos, trámites administrativos simplificados en la prestación de los servicios públicos, cuenta con el siguiente personal en la oficina de Sistemas, la cual está adscrita a la oficina de personal.

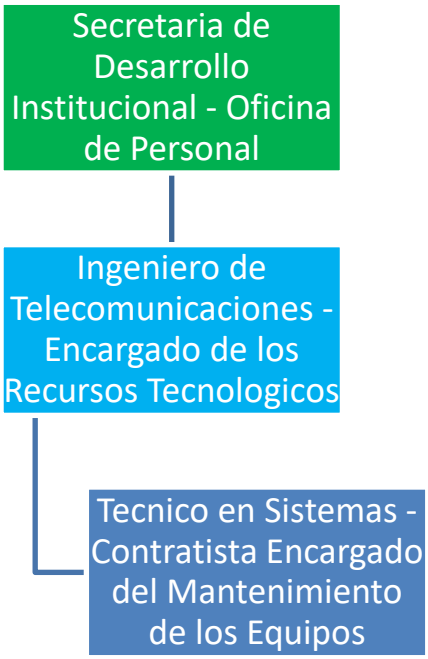
Un funcionario de planta, nombrado en provisionalidad el cual es Ingeniero de Telecomunicaciones, pero esta como Técnico Administrativo y cumple funciones de soporte técnico a toda la infraestructura tecnológica.

Un contratista por prestación de servicios, el cual se encarga de realizar el mantenimiento preventivo y correctivo a los equipos de cómputo que tiene la entidad.

### 4.2.1. Estructura Organizacional del Área de Informática.

El recurso humano del área de informática es como se evidencia en la Figura 2.

Figura 2. Estructura Organizacional del Área de Informática.




Fuente: Propia del autor.

## 4.3. ANTECEDENTES

Proyecto “Diagnóstico y Planificación de la Implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca – CAR” presentado por María Yohanna Villamil Ávila[5] a la Universidad Católica de Colombia en el año 2017 para optar al título de Especialista en Seguridad de la Información, con el propósito de implementar un Modelo de Seguridad y Privacidad de la información (MSPI) que cumpla con los lineamientos y procesos misionales determinados por MinTIC y por las buenas prácticas expresadas en la norma 27001:2013. Se busca minimizar el riesgo en las funciones más importantes en el área de Tecnologías de la Información y las Comunicaciones de la Corporación autónoma Regional de Cundinamarca (CAR), proteger los activos de información y tecnológicos, en el área de Tecnologías de la Información y las Comunicaciones de la Corporación autónoma Regional de Cundinamarca (CAR), fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, contratistas, pasantes y/o terceros en el área de Tecnologías de la Información y las Comunicaciones de la Corporación autónoma Regional de Cundinamarca (CAR). Aplica la metodología Octave Allegro, y se centra en los activos de información de la oficina de TI. A partir de este trabajo se retoma la importancia del diagnóstico para la implementación del Modelo de Seguridad y Privacidad de la información, haciendo uso del modelo (PHVA).

Proyecto “Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información” presentado por Hina Luz Garavito Robles[6] a la Universidad Nacional Abierta y a Distancia en el año 2015 para optar al título de Especialista en Seguridad Informática, con el propósito de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos, se hace necesario establecer políticas y controles de mejoramiento de los procesos de seguridad de la información. Aplica la metodología Magerit y concluye que los

[5] VILLAMIL AVILA, María Y. Diagnóstico y Planificación de la Implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca – Car. repository.ucatolica.edu.co. 2017. [Consultado el 08 de febrero de 2020]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15320/1/Trabajo%20de%20Grado%20Esp.%20Seguridad%20d%20ela%20Informaci%C3%B3n.docx.pdf

[6] GARAVITO ROBLES, Hina L. Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información. stadium.unad.edu.co. 2015. [Consultado el 08 de febrero de 2020]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3423/1/37511933.pdf

controles de seguridad de la información buscan disminuir el riesgo actual a su nivel mínimo, y que la entidad actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas y de todo el personal es posible contrarrestar. A partir de este trabajo se retoma la importancia de realizar un análisis del riesgo para la implementación de un Modelo de Seguridad y Privacidad de la Información en las entidades del estado, aplicando la metodología Magerit.

Proyecto "Diseño de un Modelo de Gestión de la Seguridad de la Información en el área de Talento Humano de la Secretaría de Educación" presentado por Emilio Antonio Sánchez Pacheco y Faver Lisandro Rebolledo Hinojosa[7] a la Institución Universitaria Politécnico Gran Colombiano en el año 2017 para optar al título de Especialista en Seguridad de la Información, con el propósito de definir una política de seguridad que le permita a la Secretaria de Educación Departamental implementar unos controles y medidas para mitigar los riegos de pérdida parcial o total de información valiosa para el buen funcionamiento de ella, con el objetivo de mantener la integridad, confidencialidad y disponibilidad de la información, utilizando el modelo aplicado por el Ministerio de las TIC para que las entidades del estado tengan una guía, contribuyendo a la transparencia en gestión pública, y promoviendo el uso de las mejores prácticas de protección de la información. Concluye que es de suma importancia que la entidad cuente con claras y precisas políticas de seguridad de información, como también que estén bien estructuradas, porque estas guiaran la conducta personal y profesional de todos los funcionarios de la secretaría, haciendo que la entidad trabaje bajo las mejores prácticas de seguridad y cumplimiento de los requisitos legales a los cuales está obligada. A partir de este trabajo se retoma la importancia de establecer políticas de seguridad de la información, aplicando controles y medidas que permitan reducir los riesgos de perdida de información.

[7] SANCHEZ PACHECO, Emilio A y REBOLLEDO HINOJOSA, Faver L. Diseño de un Modelo de Gestión de la Seguridad de la Información en el Área de Talento Humano de la Secretaría de Educación. *repository.poligran.edu.co.* 2017. [Consultado el 08 de febrero de 2020]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/1039/DISE%C3%91O%20DE%20UN%20MODELO%20DE%20GESTI%C3%93N%20DE%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20EN%20EL%20%C3%81....pdf?sequence=1&isAllowed=y

## 4.4. MARCO LEGAL

El análisis para la implementación del Modelo de Seguridad y Privacidad de la Información a una entidad pública del orden territorial, se basa en el siguiente marco normativo:

Ley 527 de 1999, [8] Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, de igual manera introduce la definición de la firma electrónica como mecanismo de autenticidad, confidencialidad y disponibilidad de la información y el concepto de equivalente funcional como validez jurídica.

Ley 1581 de 2012, [9] Ley de tipo Estatutaria que reglamenta el Artículo 15 de la Constitución política, el cual se refiere a la intimidad de las personas y el Habeas Data. Por medio de esta norma se dictan además otras disposiciones generales en la protección de datos de tipo personal.

Decreto 2573 de 2014, [10] "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea", se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.* Dicho Decreto define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Este Decreto busca además construir un estado abierto, transparente, eficiente y más participativo.

Ley 1712 de 2014, [11] *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras*

[8] Congreso. Diario Oficial [en línea]. Ley 527 de 1999. Bogotá. (21 de agosto de 1999). [Consultado: 10 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

[9] Función Pública. Gestor Normativo [en línea]. Ley 1581 de 2012. Bogotá. (18 de octubre de 2012). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[10] MinTIC. Decreto Numero 2573 de 2014. [en línea]. Bogotá (12 de diciembre de 2014). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

[11] Congreso. Diario Oficial [en línea]. Ley 1712 de 2014. Bogotá. (06 de marzo de 2014). [Consultado: 10 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

*disposiciones".* Esta Ley regula el derecho de acceso a la información pública que tiene toda persona y crea excepciones a la publicidad de la misma.

Decreto 103 de 2015, [12] *"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"*. Este Decreto reglamenta la publicación y divulgación de la información pública, la gestión de solicitud de información pública y la gestión de la información clasificada y reservada.

Decreto 1078 de 2015, [13] "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL*. Este Decreto trata de la estructura organizacional del sector de tecnologías de la información y las comunicaciones.

Ley 1915 de 2018, [14] *"Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos"*. Adiciona facultades a los autores para prohibir o autorizar la reproducción temporal o permanente en forma electrónica, y que aplica igualmente a los artistas y titulares de derechos conexos frente a sus obras.

[12] Presidencia. [en línea]. Decreto 103 de 2015. Bogotá. (20 de enero de 2015). [Consultado: 10 de septiembre de 2020]. Disponible en: http://wsp.presidencia.gov.co/secretaria-transparencia/Prensa/2015/Documents/decreto_presidencial_103_del_20_de_enero_2015.pdf

[13] MinTIC. Decreto Numero 1078 de 2015. [en línea]. Bogotá (26 de mayo de 2015). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

[14] Función Pública. Gestor Normativo [en línea]. Ley 1915 de 2018. Bogotá. (12 de julio de 2018). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87419

## 4.5 MARCO CONCEPTUAL

**4.5.1. Modelo de seguridad de la información:** También conocido por sus siglas como MSPI, es una herramienta e instrumento de evaluación que permite identificar el nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información, conduciendo a la preservación de la disponibilidad, integridad y confidencialidad de la información, permitiendo garantizar la privacidad de los datos por medio de la aplicación de un proceso de gestión del riesgo.[15]

**4.5.2. Gestión del riesgo:** Es el proceso mediante el cual se gestionan, minimizan, transfieren o eliminan los riesgos que afectan a los activos de información. Los riesgos se pueden afrontar utilizando las siguientes opciones como son: eliminar el riesgo, transferir el riesgo, asumir el riesgo o mitigar el riesgo.[16]

**4.5.3. Sistema de gestión de seguridad de la información:** También conocido por sus siglas como SGSI, es un conjunto de elementos que interactúan y se relacionan entre sí, y que tienen que ver con las políticas, responsabilidades, procesos, planificación de las actividades, estructura organizativa y recursos que utiliza la empresa o entidad para establecer una política con unos objetivos de seguridad de la información. El término SGSI es utilizado principalmente por la norma ISO/IEC 27001 y especifica los requisitos para establecer, implantar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información utilizando el ciclo PHVA (Planear, Hacer, Verificar y Actuar), buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información.[17]

**4.5.4. Plan de tratamiento del riesgo:** Evalúa las posibles acciones que se deben tomar para mitigar los riesgos que existen y se organizan en forma de medidas de

---

[15] MinTIC. Modelo de seguridad y privacidad de la información [en línea]. Seguridad y privacidad de la información. Bogotá. (29 de julio de 2016). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[16] EALDE. Gestión de Riesgos [en línea]. La Gestión de Riesgos en un SGSI. (12 de junio de 2017). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.ealde.es/gestion-de-riesgos-sgsi/#:~:text=La%20implantaci%C3%B3n%20de%20un%20Sistema,de%20la%20Gesti%C3%B3n%20de%20Riesgos.&text=El%20Risk%20Management%20es%20el,de%20informaci%C3%B3n%20de%20la%20empresa.

[17] MinTIC. Modelo de seguridad y privacidad de la información [en línea]. Seguridad y privacidad de la información. Bogotá. (29 de julio de 2016). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

seguridad, definiendo para cada una de ellas el nombre de la medida, su objetivo, la justificación, el responsable de la medida y la prioridad.[18]

**4.5.5 Metodología de gestión de riesgo informático:** Permite establecer el método de análisis que se aplica a la gestión del riesgo informático. Este método forma una disciplina que puede ser articulada desde los sistemas de gestión de seguridad informática SGSI en las empresas, realizando escaneos de vulnerabilidades importantes y utilizando una serie de modelos y procesos, que permitan proponer de forma más segura el cuidado de la información y los recursos de las tecnologías de la información. Dentro de los objetivos que se tienen en las metodologías de análisis de riegos se encuentran la planificación de la reducción de los riesgos, la prevención de accidentes, la detección y visualización de las debilidades que existen y la ayuda en la toma de decisiones en cuanto a la seguridad de la información. Existen diferentes metodologías para la gestión y análisis del riesgo informático, entre las más destacadas tenemos: Octave, Mehari, Magerit, Coras, Cramm, Ebios y NIST SP 800:30.

[18] MinTIC. Sistema de Gestión de Seguridad de la Información [en línea]. Informe Tratamiento de Riesgos. Bogotá. (12 de diciembre de 2019). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020_u20200902.pdf

# 5. DISEÑO METODOLOGICO

En virtud de que el proyecto se desarrolló bajo una metodología de tipo aplicada y descriptiva, debido a los diferentes análisis de información que se necesitan para poder desarrollar y alcanzar los objetivos que se tienen propuestos, el método de investigación que se utilizará en el presente proyecto será de tipo descriptivo.

El método descriptivo es uno de los métodos cualitativos utilizado en investigaciones, cuyo objetivo es evaluar algunas características de una población o situación particular.

En la investigación descriptiva, tal como lo indica su nombre, el objetivo es describir el estado y/o comportamiento de una serie de variables. El método descriptivo orienta al investigador durante el método científico en la búsqueda de las respuestas a preguntas como: quién, qué, cuándo, dónde, sin importar el por qué.[19]

Dentro de las características más representativas del método descriptivo son:

– El método descriptivo atiende a una metodología cualitativa.

– Es un primer abordaje al objeto de estudio y funciona como un catalizador de nuevas investigaciones.

– Se puede obtener varios datos precisos sobre el objeto de estudio.

– Se requiere observación atenta y un registro fidedigno de lo observado.

– No permite proyecciones ni generalizaciones.

– Aplica diferentes técnicas e instrumentos al momento de la recolección de datos: encuestas, entrevistas, documentación, observación participante, etc.

Este proyecto aplicado a partir de la metodología que se va a utilizar, se enfocará en la fase 1 de diagnóstico del ciclo de operación del Modelo de Seguridad y Privacidad de la Información y se desarrollará en tres fases, centrándose en tres objetivos, los cuales permiten concientizar sobre la existencia de los riesgos y de la necesidad que estos puedan ser atajados a tiempo, ofrecer un método sistemático que permita analizar tales riesgos, y por ultimo ayudar a identificar y

[19] YANEZ, Deisy. Método descriptivo: características, etapas y ejemplos. Lifeder.com. [consultado el 12 de diciembre de 2020]. Disponible en: https://www.lifeder.com/metodo-descriptivo/

hacer la planeación de las medidas oportunas para mantener los riesgos bajo control.

Se desarrollará en tres fases que consisten en:

- Realización de una valoración a los activos con que cuenta la entidad y clasificación de los riesgos con base a la disponibilidad, confidencialidad e integridad de la información.

- Detectar las posibles amenazas y vulnerabilidades con base a los riesgos identificados en la entidad.

- Diseñar una matriz con el plan de tratamiento de los riesgos detectados en la entidad.

# 6. DESARROLLO DE LOS OBJETIVOS

## 6.1. FASE 1: REALIZAR LA VALORACION A LOS ACTIVOS Y CLASIFICAR LOS RIESGOS CON BASE A LA DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACION.

Existen diferentes metodologías para el análisis de riesgos como octave, magerit, mehari, cobit, coras, cobra, cramm y ebios. Para saber cuál de las anteriores metodologías se utilizará, se debe realizar un análisis comparativo de las diferentes metodologías. A continuación, se realizará una tabla comparativa con 5 metodologías para el tratamiento de riesgos como son: COBIT, CRAMM, COBRA, MAGERIT Y OCTAVE.

Para la realización de las tablas comparativas que permitirán soportar la selección de la metodología adecuada, se decidió tener en cuenta las siguientes características.

- **Tipo de análisis:** Lo que se quiere lograr con esta tabla, es verificar si cada una de las diferentes metodologías dentro de su planteamiento de análisis incluye los métodos cuantitativo, cualitativo o mixto, dándole un valor a su aplicabilidad entre completo y No tiene cuando su valor equivale a 0.

- **Elementos de la metodología:** Lo que se quiere lograr con esta tabla, es verificar si cada una de las diferentes metodologías incluyen y analizan la mayor cantidad de elementos como son: las amenazas, las vulnerabilidades, los activos, las salvaguardas, las dependencias, los procesos, haciendo una valoración de su análisis en cada uno de ellos entre su nivel completo hasta No tiene cuando su valor equivale a 0.

- **Objetivos de seguridad:** Lo que se quiere lograr con esta tabla, es verificar si cada una de las diferentes metodologías incluyen en una mayor proporción los objetos de seguridad como son: integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información, realizando una valoración de su análisis en cada uno de los objetos entre su nivel completo hasta No tiene cuando su valor equivale a 0.

Como se evidencia en las siguientes tablas, el respectivo estudio, basado en el autor Ruge Pinzón:

Tabla 1. Tabla comparativa por tipo de análisis (cuantitativo, cualitativo y mixto).

| NOMBRE | TIPO DE ANALISIS | | | TOTAL |
|---|---|---|---|---|
| | CUANTITATIVO | CUALITATIVO | MIXTO | |
| COBRA | 3,32 | 3,32 | 1,66 | 8,3 |
| COBIT | 6,66 | 6,66 | 4,98 | 18,3 |
| CRAMM | 6,66 | 6,66 | 0 | 13,32 |
| MAGERIT | 6,66 | 6,66 | 0 | 13,32 |
| OCTAVE | 3,32 | 3,32 | 3,32 | 9,96 |

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32 Pobre: 1,66 No tiene: 0

Fuente: RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.[20]

[20] RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.

Tabla 2. Tabla comparativa por elementos de la metodología.

| NOMBRE | ELEMENTOS DE LA METODOLOGÍA | | | | | | | TOTAL |
|---|---|---|---|---|---|---|---|---|
| | PROCESOS | ACTIVOS | RECURSOS | DEPENDENCIAS | VULNERABILIDADES | AMENAZAS | SALVAGUARDAS | |
| COBRA | 0 | 4,98 | 4,98 | 3,32 | 3,32 | 3,32 | 3,32 | 23.34 |
| COBIT | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 46,62 |
| CRAMM | 0 | 6,66 | 0 | 6,66 | 6,66 | 6,66 | 6,66 | 33,3 |
| MAGERIT | 0 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 39,96 |
| OCTAVE | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 46,62 |

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32 Pobre: 1,66 No tiene: 0

Fuente: RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.[21]

[21] RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.

Tabla 3. Tabla comparativa por objetivos de seguridad.

| NOMBRE | OBJETIVOS DE SEGURIDAD | | | | | TOTAL |
|---|---|---|---|---|---|---|
| | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD | AUTENTICIDAD | TRAZABILIDAD | |
| COBRA | 4,98 | 4,98 | 4,98 | 0 | 0 | 14,94 |
| COBIT | 6,66 | 6,66 | 6,66 | 0 | 0 | 19,98 |
| CRAMM | 6,66 | 6,66 | 6,66 | 0 | 0 | 19,98 |
| MAGERIT | 6,66 | 6,66 | 6,66 | 6,66 | 6,66 | 33,3 |
| OCTAVE | 6,66 | 6,66 | 6,66 | 0 | 0 | 19,98 |

Fuente: Análisis de riesgos de seguridad de la información.[14]

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32 Pobre: 1,66 No tiene: 0

Fuente: RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.[22]

Luego de haber realizado un análisis comparativo de las diferentes metodologías, se procedió a realizar la sumatoria de las tres tablas, con base al valor total por cada metodología y arrojando los siguientes resultados:

Tabla 4. Tabla de resultados.

| Metodología | Sumatoria de tablas |
|---|---|
| COBRA | 46,48 |
| COBIT | 84,9 |
| CRAMM | 66,6 |
| MAGERIT | 86,58 |
| OCTAVE | 76,56 |

Fuente: Propia del autor.

[22] RUGE PINZON, Jeison N. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto de Colombia. Bogotá 2012.

**Conclusiones:** Con base a las anteriores tablas se puede concluir lo siguiente:

- La metodología más completa con base a las tres características analizadas es MAGERIT, la cual arrojo un valor total en la sumatoria de las tres tablas de 86,58.

- La metodología que ofrece un mayor tipo de análisis cuantitativo, cualitativo y mixto es COBIT.

- Las metodologías que ofrecen un análisis más completo de elementos como los activos, vulnerabilidades, amenazas, salvaguardas y otros son: COBIT, MAGERIT Y OCTAVE.

- La metodología que incluye en mayor proporción los objetos de seguridad como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad es MAGERIT.

Con base a las anteriores conclusiones, se tomó la decisión de utilizar la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que permite cubrir los objetos de seguridad como son la confidencialidad, integridad y disponibilidad de la información, y que además se tienen como uno de los objetivos en el desarrollo de este proyecto y cuenta con una fase de análisis y gestión de riesgos; además de buscar como objetivo en sus diferentes versiones la evaluación, homologación y certificación de seguridad de sistemas de información según la norma ISO/IEC 27001:2013. Dentro de sus ventajas es que después de la metodología COBIT, es una de las que utiliza también un completo análisis de riesgo cuantitativo y cualitativo, además es libre y no requiere autorización para su uso y posee una buena base documental que consta de tres libros: El método, Catálogo de elementos y Guía de técnicas, que son de acceso público.

Luego de haber definido la metodología de análisis de riesgos que se va a utilizar en el desarrollo de este proyecto, se comienza a levantar la información de los activos que serán aplicados a los procesos con los que cuenta actualmente la entidad, que se manejan en la oficina de sistemas y se realiza una valoración cualitativa y cuantitativa, utilizando para ello el catálogo de elementos de la metodología Magerit. Los activos son un componente o funcionalidad de un sistema de información, el cual puede ser susceptible a ser atacado accidentalmente o deliberadamente, trayendo consecuencias para la organización o entidad.

Los activos incluyen: información, servicios, datos, equipos (hardware), aplicaciones (software), recursos administrativos, comunicaciones, recursos físicos y recursos humanos. En los sistemas de información existen dos cosas esenciales que son: la información que maneja la entidad y los servicios que esta presta.

A continuación, se describirán los activos de información que serán analizados en el desarrollo del presente proyecto.

**[K] Claves Criptográficas**. Estas se emplean para proteger o autenticar a las partes, combinando secretos e información pública y son esenciales para garantizar el funcionamiento de los mecanismos criptográficos. Uno de los activos de información que será analizado es una firma digital [sign] claves de firma, que se utiliza en una dependencia de la entidad.

**[S] Servicios**. Es una función que satisface las necesidades de los usuarios de ese servicio. Aquí se pueden contemplar los servicios prestados por el sistema. Uno de los activos de información que será analizado y se encuentra clasificado como un servicio es la página web de la entidad, la cual se tiene identificada como [www] página web.

**[HW] Equipamiento Informático (hardware)**. Se refiere a los medios materiales, físicos, los cuales están destinados a soportar directa o indirectamente los servicios que presta la organización.

Los activos que se encuentran clasificados en este tipo y que serán analizados son:

[firewall] cortafuegos, [pc] informática personal (equipos de cómputo), [switch] conmutadores (switches), [wap] punto de acceso inalámbrico.

**[COM] Redes de Comunicaciones**. Son medios de transporte que llevan datos de un sitio a otro. Se incluyen instalaciones dedicadas como servicios de comunicaciones contratados a terceros. El activo que será analizado es [wifi] red inalámbrica.

**[SW] Software – Aplicaciones Informáticas**. Se refiere a tareas automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos y permiten la explotación de la información para la prestación de los servicios.

Los activos que se encuentran clasificados en este tipo y que serán analizados son:

[app] servidor de aplicaciones (Equipos de cómputo para la gestión de la base de datos del sisben, equipo de cómputo para gestión del sistema contable SINAP, equipo de cómputo para gestión del sistema integrado de organismos de transito SIOT).

**[P] Personal**. Personal relacionado con los sistemas de información. El activo que se encuentra clasificado en este tipo y que será analizado es: [adm] administradores de sistemas (Técnicos de Mantenimiento).

A continuación, se anexan las tablas con la metodología para realizar la valoración del riesgo a los activos de información de la entidad.

Es importante anotar que se toma como referencia un instrumento entregado en la asignatura de análisis y evaluación de riesgos para realizar no solamente la clasificación del activo, sino a su vez la evaluación del riesgo de cada uno de los activos. Por lo cual se tiene en cuenta la tabla 5 que está relacionada con la probabilidad del riesgo, la tabla 6 que muestra el impacto del riesgo y la tabla 7 que muestra el modelo de riesgo. Luego se encuentra la evaluación de cada uno de los aspectos anteriores en la matriz de levantamiento de información donde se muestra la tabla 9 con la valoración cualitativa y la tabla 10 con la valoración cuantitativa del riesgo.

Tabla 5. Probabilidad del Riesgo.

| | **Nomenclatura** | **Categoría** | **Valoración** |
|---|---|---|---|
| **Probabilidad** | MA | Prácticamente Seguro | 5 |
| | A | Probable | 4 |
| | M | Posible | 3 |
| | B | Poco Probable | 2 |
| | MB | Muy Raro | 1 |

Fuente: Propia del autor.

Tabla 6. Impacto del Riesgo.

| | Nomenclatura | Categoría | Valoración |
|---|---|---|---|
| **Impacto** | MA | Muy Alto | 5 |
| | A | Alto | 4 |
| | M | Medio | 3 |
| | B | Bajo | 2 |
| | MB | Muy Bajo | 1 |

Fuente: Propia del autor.

Tabla 7. Modelo del Riesgo.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Impacto** | MA | | | | | |
| | A | | | | | |
| | M | | | | | |
| | B | | | | | |
| | MB | | | | | |
| **Riesgo** | | MB | B | M | A | MA |
| | | **Probabilidad** | | | | |

Fuente: Propia del autor.

Tabla 8. Valoración del Riesgo.

| | Nomenclatura | Categoría | Valoración |
|---|---|---|---|
| Valoración del Riesgo | MA | Critico | 21 a 25 |
| | A | Importante | 16 a 20 |
| | M | Apreciable | 10 a 15 |
| | B | Bajo | 5 a 9 |
| | MB | Despreciable | 1 a 4 |

Fuente: Propia del autor.

A continuación, se presenta la tabla 9 que muestra los activos de información, el tipo de activo y la valoración del riesgo de forma cualitativa, teniendo en cuenta las dimensiones de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad de la información que maneja cada uno de los activos, dándoles una valoración a los riesgos en las escalas de MA (Critico), A (Importante), M (Apreciable), B (Bajo) y MB (Despreciable).

Tabla 9. Valorización cualitativa y clasificación de activos.

**MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS**
**SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2013**

Empresa:

| LEVANTAMIENTO DE INFORMACIÓN, INVENTARIO Y CLASIFICACIÓN DE ACTIVOS - SEGURIDAD DE LA INFORMACIÓN | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Nombre Entrevistado 1: | [redacted] | Cargo | Tecnico Administrativo | Proceso | |
| 2 | Nombre Entrevistado 2: | [redacted] | Cargo | Jefe Oficina Asesora de Planeación | Proceso | |
| 3 | Nombre Entrevistado 3: | [redacted] | Cargo | Secretaria de Salud | Proceso | |
| 4 | Nombre Entrevistado 4: | [redacted] | Cargo | Secretaria de Tránsito | Proceso | |
| 5 | Nombre Entrevistado 5: | [redacted] | Cargo | Oficina de Sistemas | Proceso | |

**INFORMACIÓN DE LOS ACTIVOS**

| No. | DATOS DEL ACTIVO DE INFORMACION | | | TIPO | | | | | | | | | | DIMENSION | | | | | ATRIBUTOS | | | | | | | | | UBICACIÓN | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Nombre del activo de información | Proceso propietario del activo | Responsable | [D] DATOS | [K] CLAVES CRIPTOGRÁFICAS | [S] SERVICIOS | [SW] SOFTWARE | [HW] EQUIPAMIENTO INFORMÁTICO | [COM] REDES DE COMUNICACIONES | [Media] SOPORTE DE INFORMACIÓN | [AUX] EQUIPAMIENTO AUXILIAR | [L] INSTALACIONES | [P] PERSONAL | Dimensión Autenticidad(B / M /A / MA/ MB) | Dimensión Trazabilidad (B / M /A / MA/ MB) | Dimensión Confidencialidad (B / M /A / MA/ MB) | Dimensión Integridad (B / M /A / MA/ MB) | Dimensión Disponibilidad (B / M /A / MA/ MB) | ¿Es activo de información de terceros o de clientes que debe protegerse? | ¿Activo de información que debe ser restringido a un número limitado de empleados? | Activo de información que debe ser restringido personas externas | Activo de información que puede ser alterado comprometido para fraudes ó corrupción | Activo de información que es muy crítico para las operaciones internas | Activo de información que es muy crítico para servicio hacia terceros | Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera: | | | Físico | Electrónico |
| | | | | | | | | | | | | | | | | | | | | | | | | | Leve | Importante | Grave | | |
| 1 | [www] Página Web | Oficina de Comunicaciones | Privado | | | X | | | | | | | | MA | A | M | A | MA | NO | SI | SI | SI | NO | SI | | X | | X | |
| 2 | [app] servidor de aplicaciones Equipos de cómputo para gestión de la base de datos del SISBEN | Oficina Asesora de Planeación | Privado | | | | X | | | | | | | M | A | A | MA | MA | SI | SI | SI | SI | SI | NO | X | | | X | |
| 3 | [app] servidor de aplicaciones Equipos de cómputo para gestión del Sistema contable - SINAP | Secretaria de Hacienda | Privado | | | | X | | | | | | | A | A | A | MA | MA | SI | SI | SI | SI | SI | SI | | | X | X | |
| 4 | [wifi] red inalambrica | Oficina de Sistemas | Privado | | | | | | X | | | | | M | B | A | A | A | NO | SI | SI | SI | NO | NO | | X | | X | |
| 5 | [sign] claves de firma | Secretaria de Salud | Privado | | X | | | | | | | | | MA | M | MA | A | A | NO | SI | SI | SI | SI | NO | | X | | X | X |
| 6 | [firewall] cortafuegos Endian | Oficina de Sistemas | Privado | | | | | X | | | | | | M | B | A | MA | MA | NO | SI | SI | SI | SI | SI | | X | | X | |
| 7 | [pc] informática personal Equipos de Computo | Oficina de Sistemas | Varios | | | | | X | | | | | | M | M | A | A | A | NO | SI | SI | SI | SI | NO | | | X | X | |
| 8 | [switch] conmutadores Switches | Oficina de Sistemas | Privado | | | | | X | | | | | | M | M | A | A | MA | NO | SI | SI | NO | SI | NO | | | | X | |
| 9 | [adm] administradores de sistemas Técnicos de mantenimiento | Oficina de Sistemas | Privado | | | | | | | | | | X | A | M | A | A | A | NO | SI | SI | SI | NO | NO | | X | | X | |
| 10 | [app] servidor de aplicaciones Equipo de cómputo para gestión del Sistema Integrado de Organismos de Transito - SIOT | Secretaria de Transito | Privado | | | | X | | | | | | | A | A | A | MA | MA | SI | SI | SI | SI | SI | SI | | | X | X | |
| 11 | [wap] punto de acceso inalámbrico | Oficina de Sistemas | Privado | | | | | X | | | | | | M | M | A | A | M | NO | SI | SI | NO | NO | NO | X | | | X | |

Fuente: Propia del autor.

A continuación, se presenta la tabla 10 que muestra la valoración del riesgo de forma cuantitativa, clasificando los riesgos en crítico, importante, apreciable, bajo y despreciable, teniendo en cuenta la autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad de la información.

Tabla 10. Valoración cuantitativa y clasificación de los riesgos.

**Resumen de Valoración de Riesgos de los Activos**

**METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO**

| VALORACIÓN DEL RIESGO | | | |
|---|---|---|---|
| Valoracion del riesgo | Nomenclatura | Categoría | Valoración |
| | MA | Critico | 21 a 25 |
| | A | Importante | 16 a 20 |
| | M | Apreciable | 10 a 15 |
| | B | Bajo | 5 a 9 |
| | MB | Despreciable | 1 a 4 |

| Nombre | Riesgo | AUTENTICIDAD | TRAZABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD | VALOR |
|---|---|---|---|---|---|---|---|
| [www] Página Web | CRITICO | 25 | 20 | 15 | 20 | 25 | 21 |
| [app] servidor de aplicaciones Equipos de cómputo para gestión de la base de datos del SISBEN | CRITICO | 15 | 20 | 20 | 25 | 25 | 21 |
| [app] servidor de aplicaciones Equipos de cómputo para gestión del Sistema contable - SINAP | CRITICO | 20 | 20 | 20 | 25 | 25 | 22 |
| [wifi] red inalambrica | IMPORTANTE | 15 | 9 | 20 | 20 | 20 | 17 |
| [sign] claves de firma | CRITICO | 25 | 15 | 25 | 20 | 20 | 21 |
| [firewall] cortafuegos | IMPORTANTE | 15 | 9 | 20 | 25 | 25 | 19 |
| [pc] informática personal Equipos de Computo | IMPORTANTE | 15 | 15 | 20 | 20 | 20 | 18 |
| [switch] conmutadores Switches | IMPORTANTE | 15 | 15 | 20 | 20 | 25 | 19 |
| [adm] administradores de sistemas Técnicos de mantenimiento | IMPORTANTE | 20 | 15 | 20 | 20 | 20 | 19 |
| [app] servidor de aplicaciones Equipo de cómputo para gestión del Sistema Integrado de Organismos de Transito - SIOT | CRITICO | 20 | 20 | 20 | 25 | 25 | 22 |
| [wap] punto de acceso inalámbrico | IMPORTANTE | 15 | 15 | 20 | 20 | 15 | 17 |

Fuente: Propia del autor.

### 6.1.1. Conclusiones primer objetivo.

Con base a la información de los activos que se analizaron en la matriz de levantamiento de la información, y utilizando las tablas anteriores, se logró realizar la valoración cualitativa de cada uno de los activos, identificando según las dimensiones de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, que hay algunos activos que tienen un nivel de riesgo muy alto, los cuales son: la página web, el servidor de aplicaciones del sisbén, el servidor de aplicaciones del SINAP, la firma digital, y el servidor de aplicaciones SIOT de la secretaria de tránsito, y otros activos que tienen un nivel de riesgo alto como son: la red inalámbrica, el firewall o cortafuegos, los equipos de cómputo, los conmutadores o switches, los administradores de sistemas, y los puntos de acceso inalámbrico, convirtiéndose de esta manera en unas amenazas para la seguridad de la información. También se logró establecer unos atributos para saber si eran activos de información de terceros que debía protegerse, activo de información que debe ser restringido a un número limitado de empleados, activo de información que debe ser restringido a personas externas, activo de información que puede ser alterado o comprometido para fraudes ó corrupción, activo de información que es muy crítico para las operaciones internas o activo de información que es muy crítico para el servicio hacia terceros y de qué forma impactaría (leve, importante o grave), si se llegara a modificar por alguna persona, sin la debida autorización, y por ultimo saber si el activo era físico o electrónico.

Por este motivo, se hizo necesario realizar una valoración cuantitativa de los activos que permitió hacer una valoración medible de los riesgos con base a la tabla 8 de valoración del riesgo donde se establecen unos rangos y la tabla 9 de valoración cualitativa, para de esta manera saber cuáles se encuentran en estado CRITICO o IMPORTANTE, teniendo en cuenta que en los campos que aparecía **MA** en la valoración cualitativa se reemplazó por el 25, donde aparecía **A** se reemplazó por el 20, donde aparecía **M** se reemplazó por el 15, donde aparecía **B** se reemplazó por el 9 y donde aparecía **MB** se reemplazó por el 4, luego se sumaron los valores de cada dimensión y se dividieron en la cantidad de dimensiones, que en este caso son 5 y de esta forma se halló el valor promedio el cual es el que nos establece los niveles de riesgo según la tabla 8. De esta manera se ha cumplido con el primer objetivo.

## 6.2. FASE 2: DETECTAR LAS POSIBLES AMENAZAS Y VULNERABILIDADES CON BASE A LOS RIESGOS IDENTIFICADOS EN LA ENTIDAD.

Luego de haber realizado la valoración de los activos y la clasificación de los riesgos, se detectan las posibles amenazas y vulnerabilidades con base a los riesgos identificados para cada uno de los activos de información como lo muestra a continuación la tabla 11 y 12, donde se puede observar lo que se describe a continuación:

- El activo de información [S] servicios cuyo nombre es [www] página web, tiene una valoración del riesgo en 21 lo que indica que su riesgo es CRITICO, una amenaza con base a la metodología Magerit clasificada como [E2] Errores del administrador y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso la información no actualizada a tiempo o información errada en la página web.

- El activo de información [SW] software cuyo nombre es [app] servidor de aplicaciones, equipo de cómputo para gestión de la base de datos de SISBEN tiene una valoración del riesgo en 21 lo que indica que su riesgo es CRITICO, una amenaza con base a la metodología Magerit clasificada como [E19] Fugas de información y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso la información puede ser utilizada por personas ajenas para hacer proselitismo político.

- El activo de información [SW] software cuyo nombre es [app] servidor de aplicaciones, equipo de cómputo para gestión del sistema contable SINAP tiene una valoración del riesgo en 22 lo que indica que su riesgo es CRITICO, una amenaza con base a la metodología Magerit clasificada como [E20] Vulnerabilidades de los programas (software) y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso se presentan errores en el software constantemente y algunas veces arroja información inconsistente.

- El activo de información [COM] redes de comunicaciones cuyo nombre es [wifi] red inalámbrica tiene una valoración del riesgo en 17 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit clasificada como [A14] Interceptación de información (escucha) y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso

por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información.

- El activo de información [K] claves criptográficas cuyo nombre es [sign] claves de firma tiene una valoración del riesgo en 21 lo que indica que su riesgo es CRITICO, una amenaza con base a la metodología Magerit clasificada como [E15] Alteración accidental de la información y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso por no proteger bien la firma digital, puede caer en manos extrañas y hacerse uso indebido de la firma digital.

- El activo de información [HW] equipamento informático cuyo nombre es [firewall] cortafuegos tiene una valoración del riesgo en 19 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit clasificada como [E4] Errores de configuración y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso la información puede ser encaminada hacia personas que no deberían utilizarla por los problemas de configuración del firewall.

- El activo de información [HW] equipamento informático cuyo nombre es [pc] informática personal, equipos de cómputo tiene una valoración del riesgo en 18 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit clasificada como [A15] Modificación deliberada de la información y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso se puede presentar perdida de información o alteración de la misma, debido a que es manipulada por otras personas y muchas veces los equipos no tienen contraseña.

- El activo de información [HW] equipamento informático cuyo nombre es [switch] conmutadores switches tiene una valoración del riesgo en 19 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit clasificada como [A14] Interceptación de información (escucha) y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información.

- El activo de información [P] personal cuyo nombre es [adm] administradores de sistemas tiene una valoración del riesgo en 19 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit

clasificada como [E28] Indisponibilidad del personal y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso solo hay una persona para la administración de la red y un contratista para el soporte técnico, haciendo que se retrasen procesos por estar muy ocupados.

- El activo de información [SW] software cuyo nombre es [app] servidor de aplicaciones, equipo de cómputo para gestión del sistema integrado de transito SIOT tiene una valoración del riesgo en 22 lo que indica que su riesgo es CRITICO, una amenaza con base a la metodología Magerit clasificada como [I7] Condiciones inadecuadas de temperatura o humedad y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso los equipos pueden fallar por exceso de calor o dañarse algún componente electrónico por humedad.

- El activo de información [HW] equipamento informático cuyo nombre es [wap] punto de acceso inalámbrico tiene una valoración del riesgo en 17 lo que indica que su riesgo es IMPORTANTE, una amenaza con base a la metodología Magerit clasificada como [A14] Interceptación de información (escucha) y una vulnerabilidad que nos dice a qué se debe esa amenaza, en este caso por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información.

A continuación, se visualiza en las tablas 11 y 12 la identificación de cada Amenaza asociada a una vulnerabilidad relacionada con su activo de información.

Tabla 11. Identificación de amenazas y vulnerabilidades.

| Activos de Informacion | No. De Amenazas y Vulnerabilidades | Nombre del activo de información | VALORACIÓN DEL RIESGO DE LOS ACTIVOS | Amenazas Metodologia Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| [S] SERVICIOS | 1 | [www] Página Web | 21 | [E2] Errores del administrador | Información no actualizada a tiempo o información errada en la pagina web. |
| [SW] SOFTWARE | 2 | [app] servidor de aplicaciones Equipos de cómputo para gestión de la base de datos del SISBEN | 21 | [E19] Fugas de información | La información puede ser utilizada por personas ajenas para hacer procelitismo politico. |
| [SW] SOFTWARE | 3 | [app] servidor de aplicaciones Equipos de cómputo para gestión del Sistema contable - SINAP | 22 | [E20] Vulnerabilidades de los programas (software) | Se presentan errores en el software constantemente. A veces arroja información inconsistente. |
| [COM] REDES DE COMUNICACIONES | 4 | [wifi] red inalambrica | 17 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información |
| [K] CLAVES CRIPTOGRAFICAS | 5 | [sign] claves de firma | 21 | [E15] Alteración accidental de la información | Por no proteger bien la firma digital puede caer en manos extrañas y hacerse uso indebido de la firma digital. |

Fuente: Propia del autor.

Tabla 12. Identificación de amenazas y vulnerabilidades.

| Activos de Informacion | No. De Amenazas y Vulnerabilidades | Nombre del activo de información | VALORACIÓN DEL RIESGO DE LOS ACTIVOS | Amenazas Metodologia Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| [HW] EQUIPAMENTO INFORMÁTICO | 6 | [firewall] cortafuegos Endian | 19 | [E4] Errores de configuración | La información puede ser encaminada hacia personas que no deberían utilizarla por los problemas de configuración del firewall |
| [HW] EQUIPAMENTO INFORMÁTICO | 7 | [pc] informática personal Equipos de Computo | 18 | [A15] Modificación deliberada de la información | Se puede presentar perdida de información o alteración de la misma, debido a que es manipulada por otras personas y muchas veces los equipos no tienen contraseña. |
| [HW] EQUIPAMENTO INFORMÁTICO | 8 | [switch] conmutadores Switches | 19 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información |
| [P] PERSONAL | 9 | [adm] administradores de sistemas Técnicos de mantenimiento | 19 | [E28] Indisponibilidad del personal | Solo hay una persona para la administración de la red y un contratista para el soporte tecnico, haciendo que se retrasen procesos por estar muy ocupados. |
| [SW] SOFTWARE | 10 | [app] servidor de aplicaciones Equipo de cómputo para gestión del Sistema Integrado de Organismos de Transito - SIOT | 22 | [I7] Condiciones inadecuadas de temperatura o humedad | Los equipos pueden fallar por exceso de calor o dañarse algún componente electrónico por humedad. |
| [HW] EQUIPAMENTO INFORMÁTICO | 11 | [wap] punto de acceso inalámbrico | 17 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información |

Fuente: Propia del autor.

### 6.2.1. Conclusiones segundo objetivo.

Con base a la valoración cuantitativa que se realizó en el primer objetivo, se logró establecer cuáles son los activos de información que se encuentran en un nivel de riesgo CRITICO y cuáles en un nivel IMPORTANTE, para de esta manera identificar las amenazas y vulnerabilidades que estos presentan, y así poder realizar un análisis de los riesgos para establecer el plan de tratamiento que se debe aplicar.

Los activos de información que obtuvieron una valoración del riesgo en categoría **CRITICA** fueron:

- [www] página web
- [app] servidor de aplicaciones (equipos de cómputo para gestión de la base de datos del SISBEN).
- [app] servidor de aplicaciones (equipos de cómputo para gestión del sistema contable SINAP).
- [sign] claves de firma.
- [app] servidor de aplicaciones (equipos de cómputo para gestión del sistema integrado de transito - SIOT).

Los activos de información que obtuvieron una valoración del riesgo en categoría **IMPORTANTE** fueron:

- [wifi] red inalámbrica.
- [firewall] cortafuegos Endian.
- [pc] informática personal Equipos de Cómputo.
- [switch] conmutadores Switches.
- [adm] administradores de sistemas - Técnicos de mantenimiento.
- [wap] punto de acceso inalámbrico.

Luego de haber detectado las posibles amenazas y vulnerabilidades a los anteriores activos de información con su clasificación de riesgo, se estableció que hay que diseñar una matriz con el plan de tratamiento para todos los activos de información a los cuales se les detecto los riesgos, aplicando las salvaguardas y los controles con base a la metodología MAGERIT.

## 6.3. FASE 3: DISEÑAR UNA MATRIZ CON EL PLAN DE TRATAMIENTO DE LOS RIESGOS DETECTADOS EN LA ENTIDAD.

Para el desarrollo del tercer objetivo, que consiste en diseñar una matriz con el plan de tratamiento de los riesgos detectados en la entidad, se utilizó un instrumento entregado en la asignatura de análisis y evaluación de riesgos que a continuación se explicará de donde se obtienen sus valores.

Luego de haber identificado las amenazas y vulnerabilidades en la anterior tabla, se estableció un valor de probabilidad de la vulneración teniendo en cuenta la siguiente escala.

Tabla 13. Probabilidad de Vulneración.

| PROBABILIDAD DE VULNERACION | |
|---|---|
| 1 | Muy Raro |
| 2 | Poco Probable |
| 3 | Posible |
| 4 | Probable |
| 5 | Prácticamente Seguro |

Fuente: Propia del autor.

Teniendo identificado el valor del riesgo y la probabilidad de vulneración, se procedió a calcular el riesgo neto, multiplicando el valor del riesgo por la probabilidad de vulneración. Utilizando la siguiente formula.

**Calculo del riesgo neto**= Valor del riesgo * Probabilidad de vulneración

Luego de haber calculado el riesgo neto, se procede a calcular la criticidad neta, con base al valor obtenido del cálculo del riesgo neto y utilizando las escalas de la siguiente tabla.

Tabla 14. Criticidad Neta.

| CRITICIDAD NETA | |
|---|---|
| 1 a 4 | Despreciable (D) |
| 5 a 9 | Baja (B) |
| 10 a 15 | Apreciable (A) |
| 16 a 20 | Importante (I) |
| 21 a 25 | Critico © |

Fuente: Propia del autor.

Después de tener la criticidad neta, se realiza una calificación de la gestión la cual va de 1 a 4 según la siguiente tabla, y así de esta manera si el valor es mayor que 1, escribir el control o salvaguarda que se está aplicando actualmente al activo de información.

Tabla 15. Calificación de Gestión.

| CALIFICACION DE GESTION | |
|---|---|
| 1 | Control no existe |
| 2 | Existe pero no efectivo |
| 3 | Efectivo pero no documentado |
| 4 | Efectivo y documentado |

Fuente: Propia del autor.

Con base a la tabla anterior, de calificación de la gestión se logró establecer que solo a tres (3) activos de información, se les estaba aplicando un control o salvaguarda, los cuales se relacionan a continuación:

Tabla 16. Controles o Salvaguardas Actuales.

| NOMBRE DEL ACTIVO | CONTROL O SALVAGUARDA |
|---|---|
| [www] Página Web | Una persona es la encargada de actualizar la página. |
| [app] servidor de aplicaciones<br><br>Equipos de cómputo para gestión de la base de datos del SISBEN | Se reportan las fallas en una plataforma JTRAC donde se asignan las solicitudes para soporte técnico. |
| [wifi] red inalámbrica | Tiene contraseña de acceso pero esta podría fácilmente ser manipulada. |

Fuente: Propia del autor.

Teniendo toda la información anterior, las amenazas y vulnerabilidades identificadas con el control que se les esta aplicando actualmente a los activos, se realiza un análisis para el tratamiento del riesgo a todos los activos y en especial, a los que tienen una criticidad neta en estado CRITICO, que permita establecer un plan de tratamiento para esos riesgos y de esa manera mitigar todas las amenazas y vulnerabilidades detectadas. Ese plan de tratamiento del riesgo se puede observar en la tabla 19 y 20 que es la matriz del plan de tratamiento de riesgo.

Otro factor que se debe analizar es el riesgo residual, que es aquel que subsiste luego de haber implementado los controles para tratar los riesgos identificados.

Para calcular el riesgo residual se debe aplicar la siguiente formula.

$$\text{Riesgo Residual} = \frac{\text{Calculo del Riesgo Neto}}{\text{Calificación de Gestión}}$$

Luego de haber calculado el riesgo residual, se establece la criticidad residual con base al valor obtenido en el riesgo residual y teniendo en cuenta los parámetros que se muestran en la siguiente tabla.

Tabla 17. Criticidad Residual.

| CRITICIDAD RESIDUAL | |
|---|---|
| Rango | Valoración |
| 1 a 4 | Despreciable |
| 5 a 9 | Bajo |
| 10 a 15 | Apreciable |
| 16 a 20 | Importante |
| 21 a 25 | Critico |

Fuente: Propia del autor.

Por último, se establece el Nivel de aceptación del riesgo, con base al valor obtenido del riesgo residual y utilizando los siguientes parámetros, según la tabla que se muestra a continuación.

Tabla 18. Nivel de Aceptación.

| NIVEL DE ACEPTACION DEL RIESGO | |
|---|---|
| Rango | Valoración |
| 1 a 5 | Aceptable (A) |
| 6 a 15 | Moderado (M) |
| 16 a 26 | Inaceptable (I) |

Fuente: Propia del autor.

De acuerdo al análisis de riesgos que se les aplicó a los activos de información, se encontraron en su mayoría con un nivel de aceptación de INACEPTABLE y solo uno con nivel MODERADO, lo que quiere decir que es muy importante que se ejecute el plan de tratamiento de esos riesgos para mitigarlos.

A partir de los valores establecidos en las tablas anteriores, estos se tomaron como referencia para hallar los diferentes riesgos como se evidencia en las tablas 19 y 20 de la matriz de tratamiento del riesgo.

Tabla 19. Matriz plan de tratamiento del riesgo.

**MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS**

**IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR**

**INFORMACIÓN DE LOS ACTIVOS DE INFORMACION**

**GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS**

| Activos de Informacion | No. De Amenazas y Vulnerabilidades | Nombre del activo de información | VALORACIÓN DEL RIESGO DE LOS ACTIVOS | Amenazas Metodologia Magerit | Vulnerabilidades | **Probabilidad de vulneración** (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 practicamente seguro) | **Calculo del riesgo neto** (Valoracion del riesgo * probabilidad de vulneración) | **Criticidad neta** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i) 21 a 25 critico(C)) | **Calificación de Gestión** (1 control no existe, 2 existe pero no efectivo, 3 efectivo pero no documentado 4 efectivo y documentado) | Si la opción es 2 - 3 o 4 Indique el Control aplicado actual | TRATAMIENTO DEL RIESGO | **Riesgo residual** (riesgo neto dividido entre la calificación de gestión) | **Criticidad residual** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 critico(C)) | **Niveles de aceptación del riesgo** (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable( |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [S] SERVICIOS | 1 | [www] Página Web | 21 | [E2] Errores del administrador | información no actualizada a tiempo o información errada en la pagina web. | 2 | 42 | C | 3 | Una persona es la encargada de actualizar la pagina. | Contratar una persona que brinde apoyo al administrador de la pagina web para que se pueda tener actualizada la pagina. | 14 | A | M |
| [SW] SOFTWARE | 2 | [app] servidor de aplicaciones Equipos de cómputo para gestión de la base de datos del SISBEN | 21 | [E19] Fugas de información | La información puede ser utilizada por personas ajenas para hacer procelitismo politico. | 4 | 84 | C | 1 | | Se debe asignar una persona responsable de la informacion que se maneja de la base de datos y realizar constantemente auditorias para evitar fugas de información. | 84 | C | I |
| [SW] SOFTWARE | 3 | [app] servidor de aplicaciones Equipos de cómputo para gestión del Sistema contable - SINAP | 22 | [E20] Vulnerabilidades de los programas (software) | Se presentan errores en el software constantemente. A veces arroja información inconsistente. | 3 | 66 | C | 2 | Se reportan las fallas en una plataforma JTRAC donde se asignan las solicitudes para soporte tecnico. | Implantar una medida que permita corregir todas las fallas detectadas al software para mitigar el riesgo de que se presenten errores e inconsistencias en la información o cambiar el software por uno que funcione bien y tenga mejor soporte tecnico. | 33 | C | I |
| [COM] REDES DE COMUNICACIONES | 4 | [wifi] red inalambrica | 17 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información | 5 | 85 | C | 2 | Tiene contraseña de acceso pero esta podria facilmente ser manipulada. | Implantar una medida para mitigarlo, reconfigurando el punto de acceso inalambrico y cambiandolo de segmento de red, para asi evitar la interceptación, ademas de establecer autenticación por MAC, para que solo los equipos registrados puedan acceder al WiFi. | 43 | C | I |
| [K] CLAVES CRIPTOGRAFICAS | 5 | [sign] claves de firma | 21 | [E15] Alteración accidental de la información | Por no proteger bien la firma digital puede caer en manos extrañas y hacerse uso indebido de la firma digital. | 2 | 42 | C | 1 | | Implantar una medida que permita asignarle la firma digital a una sola persona para que la maneje y cuando se requiera hacer uso de ella en alguna dependencia se haga una relación en un formato y se le entregue al solicitante. | 42 | C | I |

Fuente: Propia del autor.

Tabla 20. Matriz plan de tratamiento del riesgo.

| MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS<br>IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR<br>INFORMACIÓN DE LOS ACTIVOS DE INFORMACION<br>GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Activos de Informacion** | **No. De Amenazas y Vulnerabilidades** | **Nombre del activo de información** | **VALORACIÓN DEL RIESGO DE LOS ACTIVOS** | **Amenazas Metodologia Magerit** | **Vulnerabilidades** | **Probabilidad de vulneracion** (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 practicamente seguro) | **Calculo del riesgo neto** (Valoracion del riesgo * probabilidad de vulneración) | **Criticidad neta** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (I), 21 a 25 critico(C)) | **Calificación de Gestión** (1 control no existe, 2 existe pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado) | **Si la opción es 2 - 3 o 4 Indique el Control aplicado actual** | **TRATAMIENTO DEL RIESGO** | **Riesgo residual** (riesgo neto dividido entre la calificación de gestión) | **Criticidad residual** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (I), 21 a 25 critico(C)) | **Niveles de aceptación del riesgo** (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable( |
| [HW] EQUIPAMENTO INFORMÁTICO | 6 | [firewall] cortafuegos<br>Endian | 19 | [E4] Errores de configuración | La información puede ser encaminada hacia personas que no deberían utilizarla por los problemas de configuración del firewall | 5 | 95 | C | 1 | | Reconfigurar el firewall estableciendo nuevas reglas que ayuden a mitigar la falla de seguridad. | 95 | C | I |
| [HW] EQUIPAMENTO INFORMÁTICO | 7 | [pc] informática personal<br>Equipos de Computo | 18 | [A15] Modificación deliberada de la información | Se puede presentar perdida de información o alteración de la misma, debido a que es manipulada por otras personas y muchas veces los equipos no tienen contraseña. | 5 | 90 | C | 1 | | Implantar una medida para mitigarlo, estableciendo medidas de seguridad como la autenticación de usuario por medio de contraseña para el acceso al PC, y prohibir la manipulacion por personal no autorizado. | 90 | C | I |
| [HW] EQUIPAMENTO INFORMÁTICO | 8 | [switch] conmutadores<br>Switches | 19 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información | 5 | 95 | C | 1 | | Implementar una medida para mitigarlo, cambiando el segmento de red al equipo, para evitar interceptaciones y robo de la información. | 95 | C | I |
| [P] PERSONAL | 9 | [adm] administradores de sistemas<br>Técnicos de mantenimiento | 19 | [E28] Indisponibilidad del personal | Solo hay una persona para la administración de la red y un contratista para el soporte tecnico, haciendo que se retrasen procesos por estar muy ocupados. | 3 | 57 | C | 1 | | Contratar mas personal capacitado para que apoye al area de sistemas | 57 | C | I |
| [SW] SOFTWARE | 10 | [app] servidor de aplicaciones<br>Equipo de cómputo para gestión del Sistema Integrado de Organismos de Transito - SIOT | 22 | [I7] Condiciones inadecuadas de temperatura o humedad | Los equipos pueden fallar por exceso de calor o dañarse algún componente electrónico por humedad. | 5 | 110 | C | 1 | | Implantar una medida para mitigarlo, instalando un sistema de aire acondicionado que permita realizar un control adecuado de temperatura. | 110 | C | I |
| [HW] EQUIPAMENTO INFORMÁTICO | 11 | [wap] punto de acceso<br>inalámbrico | 17 | [A14] Interceptación de información (escucha) | Por encontrarse en el mismo segmento, se puede interceptar fácilmente la información por los atacantes y robar información | 5 | 85 | C | 1 | | Implantar una medida para mitigarlo, reconfigurando el punto de acceso inalambrico y cambiandolo de segmento de red, para asi evitar la interceptación, ademas de establecer autenticación por MAC, para que solo los equipos registrados puedan acceder al WiFi. | 85 | C | I |

Fuente: Propia del autor.

En la siguiente tabla se observan los controles nuevos que se deben establecer a los activos de información para el plan de tratamiento del riesgo, con base a la metodología Magerit.

Tabla 21. Controles para el plan de tratamiento del riesgo.

| Nombre del Activo de Información | Código control | Título del control | Descripción del Control |
|---|---|---|---|
| [www] Página Web | A12.4.3 | Registros del administrador y del operador | Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. |
| [app] servidor de aplicaciones Equipos de cómputo para gestión de la base de datos del SISBEN | A9.4.1 | Restricción de acceso a la información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. |
| [app] servidor de aplicaciones Equipos de cómputo para gestión del Sistema contable - SINAP | A.14.2.9 | Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados. |
| [wifi] red inalámbrica | A13.1.2 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. |

Fuente: Propia del autor.

Tabla 22. Controles para el plan de tratamiento del riesgo.

| Nombre del Activo de Información | Código control | Título del control | Descripción del Control |
|---|---|---|---|
| [sign] claves de firma | A10.1.1 | Política sobre el uso de controles criptográficos | Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| [firewall] cortafuegos Endian | A13.1.2 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. |
| [pc] informática personal Equipos de Computo | A9.4.1 | Restricción de acceso a la información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. |
| [switch] conmutadores Switches | A13.1.2 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. |

Fuente: Propia del autor.

Tabla 23. Controles para el plan de tratamiento del riesgo.

| Nombre del Activo de Información | Código control | Título del control | Descripción del Control |
|---|---|---|---|
| [adm] administradores de sistemas Técnicos de mantenimiento | A7.1.1 | Selección | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos. |
| [app] servidor de aplicaciones Equipo de cómputo para gestión del Sistema Integrado de Organismos de Transito - SIOT | A11.1.4 | Protección contra amenazas externas y ambientales. | Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |
| [wap] punto de acceso inalámbrico | A13.1.2 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. |

Fuente: Propia del autor.

### 6.3.1. Conclusiones tercer objetivo.

Con base a la identificación de las amenazas y vulnerabilidades que se detectaron en cada uno de los activos de información, se logró hacer un análisis de los riesgos y establecer un plan de tratamiento a cada uno de los activos, que permitiera mitigar las amenazas y vulnerabilidades que se presentaban y aplicar unos controles nuevos, utilizando la metodología MAGERIT, para de esta manera sugerir a la entidad la implementación de un Modelo de Seguridad y Privacidad de la Información, que permita preservar la confidencialidad, integridad y disponibilidad de la información.

Los controles nuevos que se aplicaron en el plan de tratamiento fueron controles para la seguridad de los servicios de red, restricción de acceso a la información, seguridad de los servicios de red, selección y protección contra amenazas externas y ambientales.

# 7. CONCLUSIONES

Se levantó la información de los activos y se hizo la valoración cualitativa aplicando el catálogo de elementos de la metodología Magerit, el cual maneja una nomenclatura para los activos, además se tuvo en cuenta las dimensiones de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, clasificándolas con una valoración baja, media, alta, muy alta y muy baja.

Se logró determinar el nivel de riesgo de forma cuantitativa, con base a la información obtenida en la valoración cualitativa y aplicando una valoración por rangos que clasificara el nivel de riesgo en depreciable, bajo, apreciable, importante y crítico.

Se identificaron las amenazas y vulnerabilidades, permitiendo de esta manera saber cuáles son los activos que más requieren atención y establecer el plan de tratamiento del riesgo que se le aplicará a cada uno, para de esta manera sugerir la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.

Se diseñó la matriz con el plan de tratamiento de riesgos, con base a las amenazas y vulnerabilidades detectadas, además se establecieron nuevos controles para aplicar a los activos de información, con base a la metodología Magerit.

# 8. RECOMENDACIONES

- Se recomienda a la entidad pública del orden territorial, que con base a este análisis en su fase diagnóstica, debe implementar el plan de tratamiento del riesgo realizado en este proyecto a los activos de información lo más pronto posible, además de iniciar con la planificación e implementación del Modelo de Seguridad y Privacidad de la Información que le permita minimizar las amenazas y vulnerabilidades que se detectaron, aprovechando que se tiene la fase diagnostica desarrollada.

- Se debe entregar una copia de este proyecto al representante legal de la entidad del orden territorial, para que tenga en cuenta este proyecto y aplique los correctivos necesarios lo más pronto posible.

- Se recomienda la instalación de un servidor de dominio, que les permita controlar el acceso a los equipos de cómputo para que solo los funcionarios de la entidad puedan hacer uso de ellos por medio de la autenticación de usuario y contraseña.

- Se debe brindar una capacitación a los funcionarios de la entidad, sobre la importancia de la seguridad informática y del cuidado de la información que ellos manejan.

- Se recomienda la instalación de un firewall IPS/IDS y con filtro de contenido que permita bloquear los intentos de ataque y acceso a la red, además del bloqueo de páginas no productivas como las redes sociales (facebook, twitter, instagram)

- Implementar un sistema de backup que permita minimizar el riesgo de pérdida de información, en caso de un daño en los equipos.

## BIBLIOGRAFIA


Congreso. Diario Oficial [en línea]. Ley 527 de 1999. Bogotá. (21 de agosto de 1999). [Consultado: 10 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso. Diario Oficial [en línea]. Ley 1712 de 2014. Bogotá. (06 de marzo de 2014). [Consultado: 10 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

EALDE. Gestión de Riesgos [en línea]. La Gestión de Riesgos en un SGSI. (12 de junio de 2017). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.ealde.es/gestion-de-riesgos-sgsi/#:~:text=La%20implantaci%C3%B3n%20de%20un%20Sistema,de%20la%20Gesti%C3%B3n%20de%20Riesgos.&text=El%20Risk%20Management%20es%20el,de%20informaci%C3%B3n%20de%20la%20empresa.

ESED. TENDENCIAS 2017. La seguridad como Rehén. [Consultado el 21 de enero de 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

Función Pública. Gestor Normativo [en línea]. Ley 1581 de 2012. Bogotá. (18 de octubre de 2012). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. Gestor Normativo [en línea]. Ley 1915 de 2018. Bogotá. (12 de julio de 2018). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87419

GARAVITO ROBLES, Hina L. Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información. stadium.unad.edu.co. 2015. [Consultado el 08 de febrero de 2020]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3423/1/37511933.pdf

MinTIC. Controles de Seguridad y Privacidad de la Información. 2016. [Consultado el 21 de enero de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MinTIC. Decreto Numero 1078 de 2015. [en línea]. Bogotá (26 de mayo de 2015). [Consultado: 10 de septiembre de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

MinTIC. Instrumento de Evaluación MSPI. 2016. [Consultado el 21 de enero de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

MinTIC. Modelo de Seguridad y Privacidad de la Información. 2016. [Consultado el 21 de enero de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MinTIC. Sistema de Gestión de Seguridad de la Información [en línea]. Informe Tratamiento de Riesgos. Bogotá. (12 de diciembre de 2019). [Consultado: 19 de noviembre de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020_u20200902.pdf

Presidencia. [en línea]. Decreto 103 de 2015. Bogotá. (20 de enero de 2015). [Consultado: 10 de septiembre de 2020]. Disponible en: http://wsp.presidencia.gov.co/secretaria-transparencia/Prensa/2015/Documents/decreto_presidencial_103_del_20_de_enero_2015.pdf

SANCHEZ PACHECO, Emilio A y REBOLLEDO HINOJOSA, Faver L. Diseño de un Modelo de Gestión de la Seguridad de la Información en el Área de Talento Humano de la Secretaría de Educación. *repository.poligran.edu.co.* 2017. [Consultado el 08 de febrero de 2020]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/1039/DISE%C3%91O%20DE%20UN%20MODELO%20DE%20GESTI%C3%93N%20DE%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20EN%20EL%20%C3%81....pdf?sequence=1&isAllowed=y

VILLAMIL AVILA, María Y. Diagnóstico y Planificación de la Implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca – Car. repository.ucatolica.edu.co. 2017. [Consultado el 08 de febrero de 2020]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15320/1/Trabajo%20de%20Grado%20Esp.%20Seguridad%20d%20ela%20Informaci%C3%B3n.docx.pdf