Institución Universitaria

Diseño de un sistema de gestión de seguridad de la información con base en la gestión de riesgos y el manejo de incidentes, que se ajuste a las necesidades de una empresa del sector público de la ciudad de Quibdó

Yeisson Bejarano Córdoba

Instituto Tecnológico Metropolitano
Facultad de Ingeniería
Medellín, Colombia
2021

Diseño de un sistema de gestión de seguridad de la información con base en la gestión de riesgos y el manejo de incidentes, que se ajuste a las necesidades de una empresa del sector público de la ciudad de Quibdó

Yeisson Bejarano Córdoba

Tesis o trabajo de investigación presentado como requisito parcial para optar al título de:
Magister en Seguridad Informática

Director:
Msc: Milton Javier Mateus Hernández

Línea de Investigación:
Ciencias Computacionales
Grupo de Investigación en automática, Electrónica y Ciencias Computacionales del ITM
Instituto Tecnológico Metropolitano
Facultad ingeniería
Medellín, Colombia
2021

Dedicatoria o lema

A mi hijo Jhossuar Smith Bejarano Ramos que es mi motor e inspiración para seguir adelante con mis sueños y brindarle un mejor porvenir, a mis familiares por sus apoyos incondicionales y sus palabras de aliento que no me dejaron desfallecer en todo este proceso, y a todas las personas que de otra manera estuvieron pendiente de mí en todo este trasegar.

Agradecimientos

Agradezco al señor todo poderoso por haberme brindado la oportunidad de tener vida y seguir con mis sueños adelante, a la entidad que hizo posible que este estudio se realizara, al grupo de profesores que impartieron todo su conocimiento a lo largo de este proceso formativo, al grupo de compañeros que me todo que siempre mostraron la mejor disposición para conmigo.

A mi familia por su apoyo incondicional, paciencia y por ser el motor para superarme cada día.

Resumen

Este proyecto de investigación fue desarrollado en cuatro fases con el objetivo principal de diseñar un sistema de gestión de seguridad de la información basado en la gestión de riesgos, que, ajustado a las necesidades de una empresa del sector público, permita el manejo de incidentes de seguridad y la mitigación de los riesgos en la afectación de la información, la contextualización del documento se da a través del marco teórico y el estado del arte, los cuales brindan los cimientos para la estructuración de la metodología. Luego, se consolida el segundo capítulo correspondiente a la metodología, el cual comprende cuatro fases, estas inician con un diagnóstico inicial implementado en la entidad, se realiza la identificación del inventario de activos, entrevista a los funcionarios y un análisis de brecha; en la fase 2, se caracterizan las metodologías para la determinación del riesgo tecnológico, registrando el estudio de los atributos seleccionados, indispensables en la gestión y se realiza un análisis de las ocho metodologías que son trasversales y que fueron tomadas como referencia; en la fase 3 se conforma la metodología propuesta, la cual consta de siete pasos (alcance, identificación de activos, vulnerabilidades, amenazas, riesgos, controles y manejo de incidentes); finalmente se lleva a cabo la fase 4 en donde se socializa la metodología a los funcionarios encargados de la TIC y se realiza una encuesta de satisfacción. Como resultado final, se podrá observar el diseño de un SGSI riesgo para una entidad gubernamental del departamento del Chocó con el objetivo de minimizar los riesgos, amenazas o vulnerabilidades entre otros que se pueden presentar.

Palabras clave: Controles, gestión de riesgos, Sistema de gestión de seguridad de la información, Seguridad informática, vulnerabilidades

Abstract

This research project was carried out in four phases to design an information security management system based on risk management. This design, adjusted to the needs of a public sector company, looks forward to manage security incidents and mitigate the risks that impact information. This design is based on the risk management applied to a public organization. This document is put into a context through the theoretical framework and the state of the art, which provide the foundation to structure the methodology. The second chapter corresponds to the methodology used to build the methodology used for the design. It comprises four phases, which begin with an initial diagnosis implemented in the entity, followed by the identification of the asset inventory, then an interview with the officials and a gap analysis. In phase 2, eight of the available methodologies for determining technological risk are summarized to find and identify attributes to be considered in the analysis, in order to select the components to be used in the methodology to be designed. In phase 3 the proposed methodology is developed, it comprises six steps (scope definition, asset's inventory, vulnerabilities identification, threats valuation, risks evaluation and controls definition); finally, in phase four the methodology is shared with the officials in charge of ICT and a satisfaction survey is carried out. The final result is the design of a ISMS (Information security management system) applied in a government office in Choco, which will provide tools that looks forward to reduce the risks, threats or vulnerabilities that may arise.

Keywords: Information security management system, risk management.

Contenido

Lista de figuras

Lista de tablas

Tabla de Anexos

Introducción

Para realizar este proyecto, se hizo indispensable la creación de un objetivo general el cual fue: Diseñar un sistema de gestión de seguridad de la información basado en la gestión de riesgos, que, ajustado a las necesidades de una empresa del sector público, permita el manejo de incidentes de seguridad y la mitigación de los riesgos en la afectación de la información.

Para el desarrollo de este objetivo general, se plantearon cuatro objetivos específicos que se trabajaron al interior del documento en cuatro fases respectivamente, dando como resultado la creación de la metodología propia para la entidad objeto de estudio, buscando así un manejo de incidentes de seguridad y la mitigación de los riesgos en la afectación de la información, a continuación, los objetivos específicos:

1. Identificar el estado actual de una empresa del sector público en materia de gestión de seguridad de la información.
2. Identificar características de metodologías para la determinación del riesgo tecnológico que permitan mitigar los riesgos que afectan la información dentro del manejo de incidentes.
3. Proponer una metodología de control de riesgo de la información, para facilitar su clasificación, control y manejo de incidentes de seguridad.
4. Evaluar la metodología propuesta a través de un estudio de caso

Posterior a ello encontrarán el apartado de metodología, esta se encuentra dividida en cuatro fases que corresponden al desarrollo de los objetivos, la primera fase por su parte se encuentra comprendida entre la entrevista a funcionarios de una entidad pública encargados del área, un inventario de activos y un análisis GAP, generando como resultado que la entidad no cuenta con ningún SGSI toda vez que este no ha sido implementado, el trabajo solo muestra el diseño de este sistema

En la fase 2 se desarrollaron dos actividades, que dieron sustento a la consolidación de la metodología, estas consistieron básicamente en el análisis de cada uno de los atributos seleccionados conforme a las metodologías que serían objeto de estudio, esto diseñado desde la transversalidad de los atributos en función de las metodologías, esto género como resultado la elección de las herramientas a trabajar según las necesidades propias de la empresa.

Así mismo, la fase tres diseña la metodología, en ella se establece el alcance el cual se trabaja a través del método de las elipses [1] en donde se puede evidenciar cual es la interacción de la entidad conforme a sus diferentes activos, usuarios y en general, todas aquellas personas que se benefician o usan los activos de la entidad. Después se lleva a cabo la identificación de los diferentes formatos que serían utilizados en cada uno de los atributos permitiendo de esta manera llegar a la fase tres en donde se da la consolidación de la metodología ajustada a las necesidades de la empresa.

Arrojando como conclusiones que en la entidad encuestada no existen políticas y estrategias que orienten las actuaciones de control y la falta de precaución cuando guardan cotidianamente la información, igualmente se presentan exceso de confianza en los criterios utilizados para el control de la seguridad, confusión por parte de los funcionarios encargados de la seguridad al tener una equivocada interpretación de tipo conceptual entre seguridad informática y seguridad de la información; con lo anterior se ve la necesidad de que las empresas del sector público tengan la implementación del sistema de seguridad.

A pesar de que en el Chocó de conformidad con los registros del Ministerio de las TIC se ha destinado unos recursos de un total de $162.236.000 millones en tecnología, de los cuales se han ejecutado hasta el mes de junio del 2019 solo $ 62 millones, el desarrollo de las TICS aun es incipiente ya que solo ha llegado a algunas zonas del departamento, y en materia

de seguridad informática, falta de una adecuada implementación y capacitación del recurso humano. [2]

Es de señalar también que esta investigación es relevante, ya que en ella se dan los elementos teóricos y prácticos que posibiliten el conocimiento de herramientas y técnicas para prevenir los riesgos; de igual forma con el diseño de un sistema de gestión de seguridad de la información ajustado a las necesidades de una empresa del sector público, se facilitó establecer, aplicar e implementar políticas y estrategias donde se incluyan las diferentes actuaciones para el control de cada caso, al mismo tiempo en ella se identificaron controles de seguridad, procesos y procedimientos que faciliten la identificación de los posibles riesgos a los que se puede ver expuesto el SGSI. [2]

Se propuso entonces el diseño de un sistema de gestión de la seguridad de la información como una alternativa de solución frente a los problemas ocasionados en algunas organizaciones de Quibdó relacionados con: errores técnicos del sistemas y fallos en la seguridad de la información debido al error humano, como consecuencia de que no se investiga ni se hacen oportunos seguimientos a las situaciones problemáticas presentadas, de ser implementada, se facilitaron diversas actividades que le competen al recurso de TI encargado de dicha operación, de tal manera que se pueda garantizar un control efectivo y eficaz de la información al contribuir con la disminución gradual de la pérdida de información al interior de las organizaciones.

1 . Capítulo I - Marco teórico y estado del arte

1.1. Marco teórico

Desde el punto de vista conceptual el autor [3] afirma que el marco teórico es la recopilación de antecedentes, investigaciones previas y consideraciones teóricas en las que se sustenta un proyecto de investigación, análisis, hipótesis o experimento, permitiendo la interpretación de los resultados y la formulación de conclusiones, este a su vez puede ser llamado marco de referencia.

Por otro lado, al hablar de metodología [4] se establece una serie de métodos y técnicas de rigor científico que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado teóricamente válido. En este sentido, la metodología funciona como el soporte conceptual que rige la manera en que aplicamos los procedimientos en una investigación

Es de anotar que un marco de referencia y metodología de desarrollo son partes vitales dentro de la planeación de un proyecto de investigación y esto a su vez permite tener un panorama de los procesos que hay que realizar para la consecución de los objetivos planteados, lo mismo sucede con el desarrollo de SGSI en un sector público [2] definido este como el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea, habilitando las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad de la información.

1.1.1. Análisis de brecha o análisis GAP

Esta es una herramienta utilizada para medir el grado de cumplimiento de un estándar con respecto a sus requisitos o componentes, denominados controles, para esto se hace necesario medir los controles, lo que resulta de gran utilidad para muchos aspectos como

la identificación de controles existentes para la determinación de la probabilidad de ocurrencia de las amenazas y por ende en el cálculo de riesgo [1]

Por lo general cuando las organizaciones optan por adoptar algún estándar, estas no parten de (cero), por el contrario, ven o consideran un grado de madurez frente al mismo y por esto lo siguen con el firme propósito de adoptarlo de manera formal, ya sea por cumplimientos de exigencias de entes de nivel o para el cumplimiento de exigencias del mercado para las del sector privado. Por esto realizar el Análisis GAP es un buen punto de partida para medir el estado actual, así como para proyectar el grado que se quiere alcanzar en el tiempo [1].

1.1.2. Análisis de riesgo

El análisis de riesgo debe ser entendido como un componente del SGSI que tiene como propósito establecer cuáles son los elementos dentro del sistema que requieren protección sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo [1].

1.1.3. ACCOUNTABILITY (Guía para la implementación del principio de responsabilidad demostrada)

En esta norma se enfatiza el rol del responsable del tratamiento como el llamado a implementar medidas dentro de la organización que le permitirán cumplir con el resto de principios consagrados en el instrumento, esta norma presenta como enfoque, el compromiso que debe tener la entidad con los estándares de protección para garantizarle a los ciudadanos un tratamiento idóneo sobre su información personal. [5].

1.1.4. Estándares internacionales

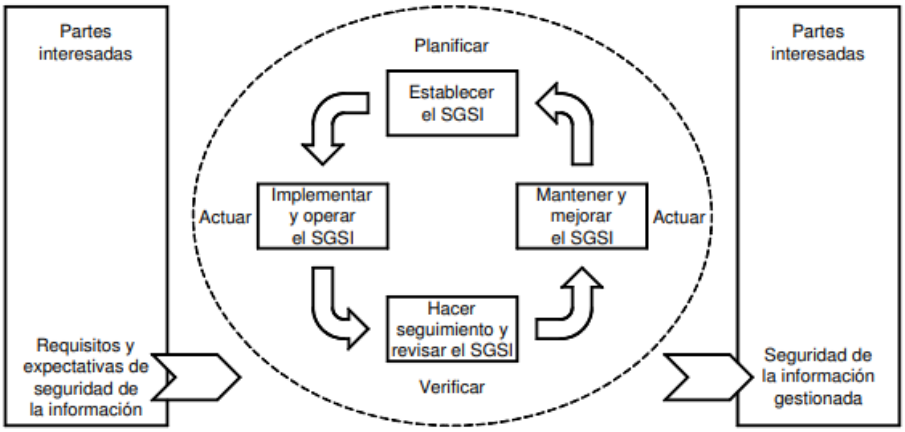
- NORMA ISO/ IEC 27001: 2013

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades, objetivos, requisitos de seguridad, procesos empleados y el tamaño y estructura de la organización. [6].

Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo, además que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple y por esto es que la norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas. [6].

Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. Es así como la ilustración Nro. 1(Modelo PHVA aplicado a los procesos SGSI) muestra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. [6].

Figura 1-1. "Modelo PHVA aplicado a los procesos SGSI" [6].



1.1.5. FRAAP (Facilitated Risk Analysis and Assessment Process)

Estas es una metodología que fue diseñada como un proceso que involucra un análisis de un sistema, aplicación, plataforma, proceso de negocio o segmento de operación de negocio a la vez. Al convocar un equipo de expertos interno, el FRAAP se basará en la propia gente de la organización para completar el proceso de evaluación de riesgos [7].

1.1.6. Guía para la administración del riesgo y el diseño de controles en entidades públicas

El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones diseñan esta guía como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo, así como el control en todos los niveles de la entidad pública, brindando seguridad razonable frente al logro de sus objetivos [8].

1.1.7. Sistema de gestión de la seguridad de la información (SGSI)

Es común que las organizaciones se enfrenten a problemas asociados a la implementación de modelos de seguridad, dado que las organizaciones están obligadas a implementar sistemas por exigencia por el Gobierno, consolidando una implementación que debe ser realizada a través de modelos internacionales que requieren alto grado de conocimiento técnico y de experiencia, por lo cual, la problemática establece no poder contar con ese conocimiento para dar cumplimiento a la legislación.

Un SGSI es la unión de políticas, procedimientos y directrices junto a los recursos y actividades que se administran de manera colectiva en una organización, con el fin de proteger sus activos informáticos esenciales, por esto, desde el estándar internacional ISO/IEC 27001 se considera como un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro, entre otras) [6].

El alcance de un SGSI debe ser definido dependiendo de la identificación y ubicación de activos informáticos por esto se deben establecer funciones específicas de un grupo u organización, todo esto porque se debe tener presente que el SGSI trabaja con base a tres criterios que son considerados los pilares en materia de seguridad, los cuales son:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados [5].
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. [5].
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. [5].

1.1.8. Metodologías de riesgos

Estas hacen parte de una disciplina que se articula desde los Sistemas de Gestión de Seguridad Informática SGSI en las organizaciones, realizando unos importantes escaneos de vulnerabilidades mediante modelos y procesos para, proponer una forma más segura de cuidar la información y los recursos, con el objetivo principal de realizar una planificación de la reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información. [6]

Algunas de estas metodologías son:

1.1.9. Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Esta metodología es desarrollada por el Consejo Superior de Administración Electrónica y en ella resaltan dos objetivos principales, uno de los cuales es estudiar los riesgos que soporta un sistema de información y el entorno asociado a este, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados [9].

1.1.10. NORMA TÉCNICA NTC/ IEC ISO 27005

Esta norma lo que hace es proporcionar directrices para la gestión del riesgo en la seguridad de la información de una organización, sin embargo, aunque esta norma no brinda ninguna metodología específica para la gestión del riesgo, pero si permite implementar los requisitos de un sistema de gestión basado en metodologías existentes. [1].

1.1.11. NORMA TÉCNICA COLOMBIANA NTC- ISO 31000

Esta norma brinda principios y directrices generales sobre la gestión de riesgo, puede ser utilizada para cualquier tipo de empresa y puede ser aplicada durante todo el proceso en

actividades como estrategias, decisiones, operaciones, procesos, funciones, productos o servicios y también puede aplicarse a cualquier tipo de riesgo sin importar su naturaleza o las consecuencias que de este se genere. [10].

1.1.12. NIST Rist Management Framework For Information System And Organizate

Este es un Marco de ciber seguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework, fue elaborado bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio. [11].

1.1.13. OCTAVE

Esta metodología describe un conjunto de criterios para desarrollar métodos que se adhieran a guías específicas de evaluación y administración de riesgos, a su vez evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos, buscando como objetivo concientizar a la organización en cuanto a que la seguridad informática no es un asunto solamente técnico, y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos [8].

1.1.14. Incidentes de seguridad de la información

Este hace referencia a un evento o una serie de eventos de seguridad de la información no deseados o inesperados que pueden perjudicar las operaciones del negocio amenazando

la seguridad de la información, es de resaltar que esta norma es aplicada solamente a medianas y grandes empresas y se implementa en relación a la situación de riesgo

1.2. 1.2. Estado del Arte

El primer documento que se referencia en el estado del arte, es una investigación que busca evaluar los riesgos en una organización frente a su Ciberseguridad en Australia occidental, para esto se diseñó una herramienta de valoración para determinar la comprensión de los riesgos, este documento se denomina "Una revisión de seguridad del gobierno local utilizando NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST [11]: un estudio de caso" los investigadores Ibrahim, Valli, I McAteer, & Chaudhry, utilizaron el National Institute Of Standards And Technology Nist National Institute Of Standards And Technologynational Institute Of Standards And Technologycsf[1]para evaluar los riesgos de Ciberseguridad de una organización del gobierno local en Australia Occidental y al mismo tiempo implementaron el sistema en el que fue posible la disminución de los riesgos en un 80% [12].Esto les permitió diseñar una herramienta de evaluación dirigida a tres niveles de participantes dentro de la organización, es decir, ejecutivo, de gestión y técnico, tuvo como razón fundamental determinar la comprensión de los riesgos de Ciberseguridad en toda la organización [12].

Por otro lado se encuentra la investigación realizada por los autores Khajouei, Kazemi, &Moosavirad, llamaron su investigación, "Clasificación de los controles de seguridad de la información mediante el proceso de jerarquía analítica difusa" en donde se busca a través de diferentes metodologías, establecer un procedimiento cimentado en la mitigación de los riesgos más mínimos que se puedan generar dentro de una organización, como

[1] Instituto Nacional de Normas y Tecnología

resultado se observa que la mitigación no es del todo efectiva puesto que de manera diaria se generan riesgos diferentes [12].

Otra investigación publicada es la de un Diseño de un sistema de gestión de seguridad de la información ajustado a las necesidades de la corporación Médica Clínica vida de Quibdó, [7] quien solo tomo como referencia el marco Cyber Seguridad de la NIST, proponiendo 5 funciones relacionadas con la gestión de riesgos de seguridad de la información, logrando con esto identificar el estado actual de la Clínica Vida en materia de Gestión de Seguridad de la Información, permitiendo diseñar una propuesta de implementación del Sistema de Gestión de Seguridad de la Información ajustada a los hallazgos detectadas en el diagnóstico previamente realizado, obteniendo todos los pormenores necesarios del área de infraestructura de la Clínica para ubicar y valorar los riesgos y vulnerabilidades, construyendo un modelo basado en las necesidades reales de la Clínica. [13].

A nivel local también se puede señalar que existe otra investigación llamada "Metodología de Análisis de Riesgos Informáticos" escrito por Jorge Esteban Eterovic en el que se muestra que el análisis de riesgos es el primer punto de la gestión de la seguridad de la información de una organización, y es necesario para realizar la gestión de los riesgos, es decir, tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos, es decir realizar la gestión de riesgos [14].

En este documento se evalúan diferentes metodologías o estándares que más se ajusten y a partir de esto evalúan cuales son las falencias que se pueden presentar dentro de los atributos evaluados en cada trabajo, se puede identificar que ellos al trabajar con una sola metodología no tienen en cuenta las fortalezas y debilidades de otras normas o estándares, generando así una visión muy sesgada o limitada, por esta razón, en este proyecto de grado lo que se hace es recopilar y estudiar diferentes metodología y el estándar ISO 27001 lo

que permite una mirada más amplia, evaluando diferentes atributos frente a el sistema de gestión y seguridad informática [14, p. 07] [7].

El trabajo realizado por el colegio oficial de ingenieros en comunicación, plantean una propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) en cumplimento de la norma internacional adoptada para Colombia NTC-ISO 27001:2013 en la infraestructura del centro de datos de la Alcaldía de Medellín, tomando como punto de partida la determinación de una metodología de riesgos propia y la verificación de requisitos del estándar según el estado actual de la entidad. [15] [1].

Arrojando como resultado que en la propuesta de metodología propia se indican aspectos clave a tener en cuenta y se describen de manera metodológica y secuencial con el fin de que el documento pueda emplearse como primera referencia en el momento en que la entidad decida emprender la implementación. Finalmente, se presenta un análisis técnico y económico que entregue elementos necesarios para realizar una evaluación de la factibilidad desde la óptica abordada, para ello utilizaron un proceso complejo de jerarquía analítica para priorizar y seleccionar dominios gerenciales efectivos y controlar los objetivos en los controles de seguridad de la información. [15].

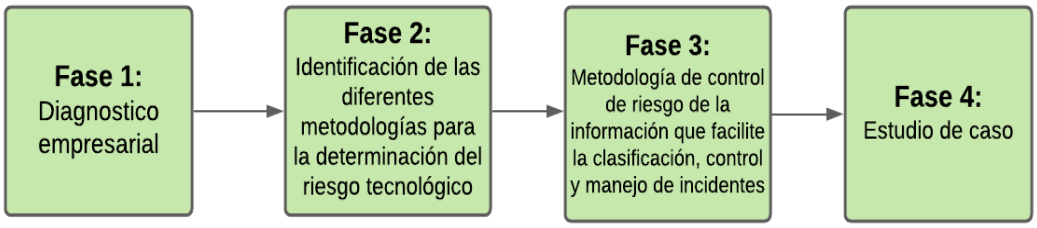
De acuerdo con los resultados, el control de acceso, la adquisición, el desarrollo y el mantenimiento de sistemas de información tuvieron las más altas prioridades entre los controles de seguridad de la información en los dominios gerenciales. Por otro lado, la gestión de la continuidad del negocio y la gestión de activos tuvieron las prioridades más bajas entre los controles de seguridad de la información estudiados. Además, se encontró que, entre 39 objetivos de control, la gestión de acceso de usuarios y la gestión de entrega de servicios de terceros tienen las prioridades más altas y más bajas, respectivamente. [15]. Los autores Béatrix y Mesquidaen su trabajo, “Integrando la gestión de riesgos en la configuración de TI desde las normas ISO y las perspectivas de los sistemas de gestión”, analizan las actividades de gestión de riesgos en varias normas ISO seleccionadas para

proporcionar la base para mejorar, coordinar e interpelar las actividades de gestión de riesgos en entornos de TI para diversos fines relacionados con la gestión de calidad, gestión de proyectos, gestión de servicios de TI y gestión de la seguridad de la información, todo esto lo hacen basándose en el estándar internacional NORMA TÉCNICA COLOMBIANA NTC-31000, y por esto realizan una comparación con el objetivo de identificar actividades relacionadas con la gestión de riesgos en la estructura ISO de alto nivel para estándares de sistemas de gestión, ISO 9001, ISO 21500, ISO / IEC 20000-1 e ISO / IEC 27001. [16] [9] [7] [1].

2. Capítulo II - Metodología

Para el cumplimiento de los objetivos se inició con el desarrollo de cuatro fases las cuales se describen a continuación, cada fase contempla un objetivo específico.

Figura 2-1. Diseño metodológico.



2.1. Fase 1: Diagnóstico empresarial

Antes de iniciar con el análisis del riesgos, cabe decir que asegurar en un 100% la información en una organización es imposible de realizar, es común escuchar en estos ámbitos el concepto de garantizar la Integridad, Disponibilidad y Confidencialidad de la información, pero lo que es cierto es que un modelo para un Sistema de Gestión de Seguridad de la Información, pretende es la reducción del riesgo asociado a los activos de información mediante la administración de este, con esta fase, se llevó cabo un diagnóstico empresarial, el cual se identifica como se encuentra la entidad frente a la seguridad informática.

Este proyecto de grado fue realizado en un caso de estudio en una entidad del Estado, sin embargo, no es posible mencionar su nombre, pues se debe manejar completa confidencialidad, pero si se puede afirmar que ellos deben contar con una dependencia de tecnologías de información y comunicación, en adelante TIC, y es precisamente en esta oficina en la que se realizó el estudio del cual se hablará.

2.1.1. Fase 1-1: Entrevista con un funcionario encargado del área TIC

Para poder efectuar el primer acercamiento, fue importante la realización de una entrevista abierta, entendida esta como una técnica cualitativa de investigación en la cual se propicia una conversación no estructurada entre una persona que entrevista y un entrevistado, esta se encuentra basada en preguntas generadas espontáneamente como parte de la interacción comunicacional, gracias a la cual fue posible identificar cuáles eran los riesgos que presentaba la entidad en seguridad de la información.

Las preguntas, que se le realizaron al entrevistado fueron generales, entre las cuales se cuestionó sobre los inventarios de activos a nivel de tecnología en la empresa, cantidad y tipo de elemento, se preguntó si contaban con antivirus actualizado y paquetes ofimáticos con licencia, si contaban con un sistema de gestión de seguridad de la información (SGSI), entre otras.

Las preguntas formuladas fueron:

1. ¿Cuáles son los activos tecnológicos de la empresa?
2. ¿Qué cantidad tienen de cada equipo?
3. ¿Dónde es la ubicación física de cada equipo?
4. ¿Cuentan con Sistema de Gestión de Seguridad de información?
5. ¿Cuenta con antivirus y programas actualizado y licenciado?
7. ¿Qué tipos de incidentes informáticos han tenido?
8. ¿Qué tipo de infraestructura tecnológica están utilizando?

Gracias a esta entrevista, contestada por el funcionario encargado de esta dependencia, fue posible percibir un panorama general del estado en el que se encuentra la entidad; es de resaltar que esta actividad puede considerarse también preliminar de la siguiente, pues gracias a este acercamiento es que se consolida el inventario de activos, del que se hablará a continuación.

2.1.2. Fase 1-2: inventario de activos

El inventario de activos, compone la segunda actividad de esta primera fase, al realizar un pequeño acercamiento a la entidad, se consolida este formato, definido como una lista de todos aquellos recursos que tienen valor para una organización y necesitan ser protegidos de potenciales riesgos.

Este inventario, se elaboró conforme a una identificación de los activos informáticos en el área específica de las TIC en la empresa pública objeto de estudio, que permitió crear una base de datos de los activos, el primer elemento a consolidar fue el "identificador" este hizo referencia a la numeración interna que permite tanto contabilizar los activos como discriminarlo por cada uno de los mismos, la casilla siguiente dejó ver el "nombre del activo" en donde se describía que tipo de elemento es, la "cantidad" de ese activo, la "categoría" es decir si es Hardware o Software, el "propietario" que en este caso es el área a la que pertenece el activo, es decir el departamento de las TIC, el "responsable" en donde se pueden encontrar cuatro funcionarios que utilizan parte de los equipos y llevan el control de los otros, la "ubicación física" muestra donde está ubicado el activo, según el estudio puede evidenciarse que se encuentran entre las sede principal y el edificio de la secretaria de salud la "descripción" del mismo corresponde al equipo como tal.

Este inventario permite dar cuenta de las posibles falencias que se presentan frente a la seguridad y el control que se da dentro de una empresa, esta es considerada como una herramienta de análisis para comparar el estado y desempeño real de una organización, respecto a uno o más puntos de referencia seleccionados, en este caso, se realizaron los controles basados en la norma NTC ISO/ IEC 27002 el cual es el anexo A de la norma ISO/IEC 27001:2013.

Para la consolidación de la información anteriormente mencionada, se estableció la siguiente tabla (ver Tabla 2-1. Inventario de activos) para la recolección de la información de los activos informáticos de la organización:

Tabla 2-1. Inventario de activos. Fuente: Elaboración propia.

Nombre Activos	Cantidad	Categoría	Descripción

2.1.3. Fase 1-3: Análisis de brecha

Esta actividad se identificó el estado en el que se encuentra la organización objeto de estudio en cuanto gestión de riesgo, basado en la ISO/ IEC 27002 entendido como el anexo A en la norma ISO/ IEC 27001: 2013.

Este anexo A se encuentra divido en 14 dominios, estos a su vez en 34 objetivos de Control, distribuidos en 114 Controles, a estos últimos son a los que se debería hacer una medición dentro del análisis GAP, dado que serían desde los cuales parte la organización en el ámbito de seguridad de la información y por tanto la forma como se puede abordar. Adicionalmente, contribuye al desarrollo de la Declaración de Aplicabilidad [7].

2.1.3.1. Identificar los ítems a medir

Se debe tener claramente definidos los ítems a medir y los componentes que se deben documentar para un mejor análisis posterior a la medición. Por esto se debe tener clara la información requerida para tal fin y se recomienda tener una plantilla en la que se integren los siguientes datos:

Dominio (Sesión): Se debe tomar de los 14 dominios descritos en el Anexo A. del estándar 27001:2013 [7].

Control: Corresponde a la descripción del control de los 114 definidos en el Anexo A.

Escala de medición: La medición de este elemento se hace conforme a una medición cuantitativa y cualitativa

Se debe definir una escala a evaluar, en este caso se proponen 6 niveles del 0 al 5, presentando su definición y descripción de cada valor, con el propósito de identificar en cada uno de los 114 controles su grado de madurez de acuerdo a la organización y el alcance definido dentro de la infraestructura del Centro de Datos.

Tabla 2-2. Escala de valoración. Fuente: Elaboración propia.

Escala de valoración		
% de cumplimiento	Cuantitativo	Cualitativo

La escala que se plantea para el análisis de este tipo de controles en gestión del riesgo, es basada en una calificación del 0 al 5, esta escala de calificación es tomada de la norma NTC-ISO-IEC 27002 anexo A de la norma NTC-ISO-IEC 27001:2013 en el que se establecen escala de números, porcentajes y a el dominio que hace referencia al nombre de la sección, las cuales van desde "0 – inexistente" hasta "5- optimizado con un cumplimiento al 100%"al valor de la escala de cumplimiento nivel numérico se consigna el porcentaje que va desde 0 equivalente como ya se dijo a inexistente hasta el 100% correspondiente a optimizado. [1].

Observaciones: En este campo se recomienda diligenciar, la ubicación de las evidencias sobre el control, tales como documentación o acciones realizadas, actas de reuniones, políticas internas, o cualquier información que pueda evidenciar el estado del mismo.

Con el fin de consolidar los ítems antes mencionados se construyó la siguiente tabla (Tabla 2-3) basado en la norma EIC/ISO 27002 Anexo A de la EIC/ISO 27001:2013

Tabla 2-3. Análisis de brecha (GAP). Fuente: Elaboración propia.

Sección	Control	Cualitativo	Cuantitativo	% de cumplimiento	Observación

2.1.3.2. Ponderación de los valores definidos

Teniendo valorados cada uno de los 114 controles, se continúa con la ponderación, por cada uno de los objetivos de control y posteriormente se obtendrá de igual manera un valor por cada dominio.

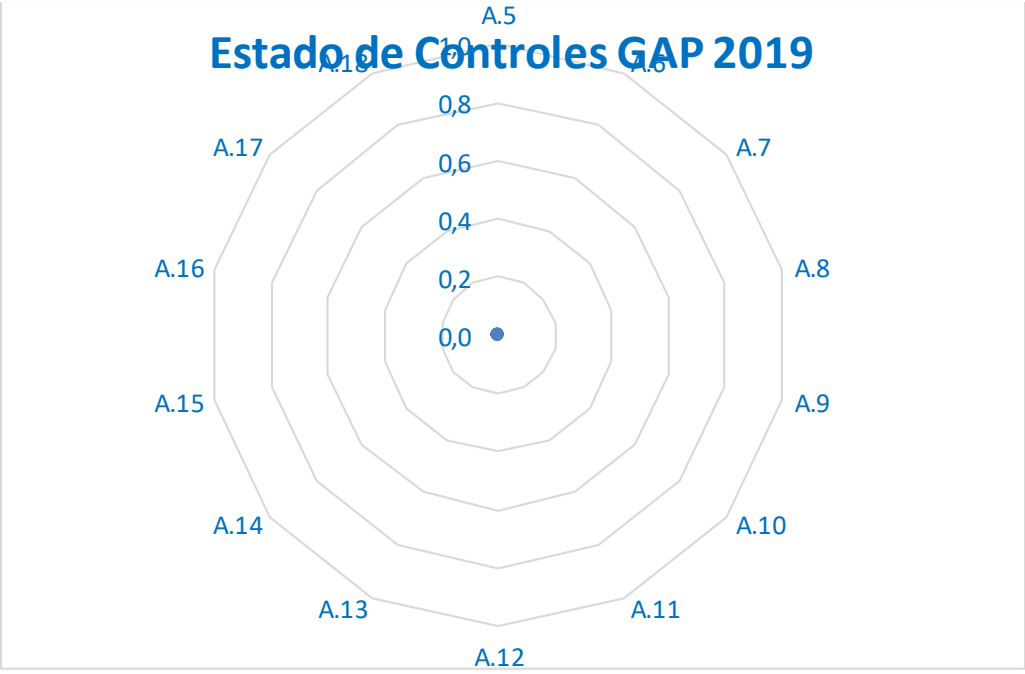
Entendido esto, se puede recordar que el análisis GAP, es una herramienta utilizada para medir el grado de cumplimiento de un estándar con respecto a sus requisitos, por tanto, el estándar ISO-IEC 27002 Anexo A de la norma ISO-IEC 27001:2013 permitió consolidar los estados de controles en materia de seguridad informática en la organización (Ver Tabla 2-4 Estado de controles). [1].

Tabla 2-4. Estado de controles. Fuente: Elaboración propia.

Sección	Dominio	Valor	Estado	Porcentaje de cumplimiento

Luego de ponderar los objetivos, se recomienda graficar los valores obtenidos por cada dominio, como se muestra a continuación. Gracias a esto se puede crear una telaraña permitiendo visualizar el estado de la empresa:

Figura 2-2. Estado de controles (Telaraña). Fuente: Elaboración propia.



2.2. Fase 2: características de las metodologías para la determinación del riesgo tecnológico

En esta fase se revisaron diferentes metodologías existentes, con el fin de identificar criterios basados en una metodología de análisis de riesgo como inventario de activos, vulnerabilidades, amenazas, riesgos, controles que sirvieron como elementos principales para la construcción de una nueva metodología que se ajuste a los requerimientos de una empresa del sector público. [1]

Es compatible con los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminólogas descritos en ISO / IEC 27001 e ISO/IEC 27002 es importante para una comprensión completa. [1]

2.2.1. Fase 2-1: identificar las metodologías objeto de estudio con base al análisis de riesgos

Esta fase permitió consolidar los atributos que son transversales en la mayoría de las metodologías de análisis de riesgo seleccionadas como objeto de estudio, generando de esta manera una uniformidad frente a los temas que se tienen en cuenta al momento de diagnosticar, auditar o evaluar una empresa, estos atributos o elementos integrantes de las metodologías, lo que permitió fue el diagnóstico paralelo de los diferentes elementos que fueron tenidos en cuenta en la empresa objeto de estudio.

Por esta razón, a continuación, se va a hablar de los diferentes atributos que fueron seleccionados dentro de este diseño, los cuales serán explicados de manera detallada en la tabla 2-5 (Ver Tabla 2-5 - Revisión de metodología de análisis de riesgos).

	ATRIBUTOS																
	Aplica Sector - Gobierno pública o privada		Quien la Genera de orden local o internacional		Tamaño – Empresa			Inventarios Activos				Vulnerabilidades	Amenazas	Riesgo		Controles		
Metodologías	Si	No	Local	Internacional	Grande	Mediana	Pequeña	Clasificación	Valoración I	Valoración C	Valoración D			Probabilidad	Impacto	Clasificación	Diseño	Evaluación

Tabla 2-5. Revisión de metodología de análisis de riesgos. Fuente: Elaboración propia.

El objetivo de esta tabla (Tabla 2-5) se centra en la consolidación de los atributos que fueron analizado a través de las diferentes metodologías de análisis de riesgo, para que de esta manera sea posible identificar cuáles son los atributos que manejan las metodologías estudiadas y cuáles son los elementos que se encuentran integrados.

Los diferentes ítems de la tabla anterior se deben diligenciar de la siguiente manera:

- **Metodologías:** En donde se establecen los nombres de las metodologías de análisis riesgo que fueron utilizados como objeto de estudio, con base a un elemento identificador común entre ellas.
- **Aplica al sector Gobierno (pública o privada):** consistió en determinar en qué sector (privado y público) es obligatorio el cumplimiento de las metodologías estudiadas
- **Quien la genera de orden local o internacional** Consistió en establecer si la metodología es generada por un orden nacional o internacional
- **Tamaño empresa (Grande, mediano y pequeña)** Si la metodología está diseñada para operar en empresas grandes, medianas o pequeñas.
- **Inventario de activos:** Se analizó cada una de las metodologías de análisis de riesgo conforme a si hace una clasificación y valoración (se realiza de acuerdo a su confidencialidad, disponibilidad e integridad) de sus activos.
- **Vulnerabilidades:** Se analizaron las diferentes metodologías con base en si se realizan clasificación de las vulnerabilidades que pueden tener los diferentes activos
- **Amenazas:** Se analizaron las diferentes metodologías de análisis de riesgo conforme a las amenazas que se puedan generar en los activos
- **Riesgos** Se analizaron las diferentes metodologías de análisis de riesgo conforme a los riesgos que se puedan generar en los activos teniendo en cuenta su probabilidad e impacto
- **Controles:** Se analizaron las diferentes metodologías frente a los controles que se realizan a los activos teniendo en cuenta la clasificación, diseño y evaluación.

Se debe señalar que la Tabla 2-5 fue construida conforme a los elementos citados anteriormente que para el caso de estudio son denominados atributos.

La forma en cómo esta tabla se diligencio responde a los siguientes parámetros:

SI: aplica.

NO: No aplica

2.2.2. Fase 2-2: revisión de las metodologías de análisis de riesgo con base a los criterios inventario de activos, vulnerabilidades, amenazas, controles y riesgos

La construcción de esta fase consistió en realizar una revisión de los atributos, de acuerdo con las metodologías identificadas en la fase 2.1, teniendo como elementos identificadores inventario de activos, vulnerabilidad, amenazas, riesgos y controles; de las metodologías que detallen la manera o la forma de trabajar con dichos atributos, los cuales se tomaron como referencia para la construcción de la metodología propia.

Por cada una de las metodologías identificadas, se realizó un análisis de los atributos (inventario de activos, vulnerabilidades, amenazas, controles y riesgos) conforme a esto se efectúo una valoración por cada uno de ellos, la cual fue trasversal a todas las metodologías, con base a esto se realizó el proceso de revisión a través de las tablas, 8, 9, 10 y 11 las cuales serán diligenciadas de la siguiente manera:

- **Metodología**: Corresponde al nombre de la metodología revisada
- Inventario de activo: lo comprende la clasificación que hace referencia al tipo de activo y la valoración que hace relación a la valoración del activo conforme a la disponibilidad, confidencialidad e integridad.
- **Valoración**: hace relación a la métrica de valor que tomo el atributo evaluado conforme a la metodología revisada, el cual se compone de porcentaje de cumplimiento, nivel y estado de conformidad. Es de resaltar que este apartado es trasversal a todas las tablas pues es el que evalúa si el atributo es elegible o no de acuerdo con la metodología, así:

Tabla 2-6. Valoración. Fuente: Elaboración propia.

Puntuación	% de cumplimiento	Nivel	Estado
0	0%	NULA	NO ELEGIBLE
1	10% - 29%	BAJA	
2	30% - 39%	MEDIA	ELEGIBLE
3	40% - 50%	ALTA	

Esta métrica de valoración se identifica de la siguiente manera:

- **Puntuación**: Nivel mínimo y máximo que puede tomar un atributo evaluado
- **% de cumplimiento**: Escala de valor que toma un atributo evaluado
- **Nivel**: son los niveles de estado que puede tomar un atributo evaluado los cuales se determinan como nulos, bajo, medio y alto
- **Estado**: hace relación a si puede ser elegible o no el atributo de la metodología revisada

Las siguientes tablas se conformaron para evaluar la revisión de los atributos (inventario de activos, vulnerabilidades, amenazas, riesgos y controles) por cada una de las metodologías revisadas.

2.2.2.1. Inventario de activos

Tabla 2-7. Revisión de la metodología de riesgos conforme a los activos. Fuente: Elaboración propia

Metodología	Inventario de activos				Valoración		
	Clasificación	Valoración			% de cumplimiento	Nivel	Estado
		Disponibilidad	Confidencialidad	Integridad			

El objetivo de esta tabla (Tabla 2-7) es unificar la revisión metodológica que fue realizada a los activos frente a las metodologías de análisis de riesgo, de esta manera es posible identificar el porcentaje y nivel de cumplimiento para de esta manera establecer si es

elegible o no, permitiendo de esta manera identificar cual es la metodología que mayor detalla o guía en cómo deben ser manejados los atributos

2.2.2.2. Vulnerabilidades:

La siguiente tabla es realizada con el fin de identificar la valoración de vulnerabilidades frente a cada una de las metodologías analizadas, para de esta manera saber cuál es la metodología elegible y cuál debe ser la manera de trabajar las vulnerabilidades del SGSI

Tabla 2-8. Revisión de la metodología de riesgos conforme a las vulnerabilidades. Fuente: Elaboración propia.

Metodología	Vulnerabilidades	Valoración		
		% de cumplimiento	Nivel	Estado

2.2.2.3. Amenazas:

Al igual que en la tabla anterior, lo que se busca es poder identificar cual es la metodología que mejor consagra el atributo analizado pues de esta manera se accede a información profunda sobre el tratamiento que se les da a las amenazas, con el objetivo de disminuirlas

Tabla 2-9. Revisión de la metodología de riesgo conforme a las amenazas. Fuente: Elaboración propia.

Metodología	Amenazas	Valoración		
		% de cumplimiento	Nivel	Estado

- 2.2.2.4. Riesgos:

Con esta tabla se identifica cual es la metodología que mejor consagra o detalla los riesgos, identificando como se trabaja, mide o controla la probabilidad de ocurrencia y el impacto que puedan generar.

Tabla 2-10. Revisión de la metodología de riesgo conforme al riesgo. Fuente: Elaboración propia.

Metodología	Riesgo		Valoración		
			% de cumplimiento	Nivel	Estado
	Probabilidad	Impacto			

- 2.2.2.5. Controles

Lo que se busca con esta tabla es identificar que metodología consagra de una manera más completa o detallada los controles, estudiando, definiendo o desarrollando los elementos como clasificación, diseño y evaluación de controles.

Tabla 2-11. Revisión de la metodología de riesgo conforme a los controles. Fuente: Elaboración propia.

Metodología	Controles			Valoración	Nivel	Estado
				% de cumplimiento		
	Clasificación	Diseño	Evaluación			

El objetivo de esta tabla es establecer que metodología es más profunda frente a la identificación, clasificación y como deben ser trabajados los controles. A partir de las metodologías estudiadas con base al análisis realizado por cada una de las mismas, se pudo identificar los atributos que integrarán la nueva metodología conforme al estado elegible, como se representa en la siguiente tabla:

Tabla 2-12. Resultado final conforme a la revisión de las metodologías de análisis de riesgo conforme a los atributos evaluados. Fuente: Elaboración propia.

NOMBRE DE METODOLOGÍA	ATRIBUTOS	ESTADO

1.3. 2.3. Fase 3: Creación de la metodología propia de análisis de riesgo para una entidad del sector público

2.3.1 Consolidación metodología propia

El desarrollo de la metodología propuesta se realiza mediante la elección de los mejores atributos de cada una de las diferentes metodologías de análisis de riesgos Identificadas en la fase 2, la cual facilita la identificación de los siguientes atributos: Alcance, Identificación del inventario de activos, Identificación de vulnerabilidades, Identificación de amenazas, Identificación de riesgos, Identificación de controles y Manejo de incidentes. De otro lado con la aplicación del proceso metodológico se facilita obtener elementos valiosos para identificar y formular acciones frente a la mitigación del riesgo, siendo esta una metodología de tipo cualitativa que puede ser utilizada en organizaciones y empresas del sector público.

A continuación, se relaciona el paso a paso de los 7 atributos relacionados anteriormente:

2.3.2 Alcance

Con el propósito de establecer los límites y la aplicabilidad de la metodología propuesta se parte del alcance de la misma, para la búsqueda de la identificación de los activos el cual aplica a todas las entidades públicas así:

Para el cumplimiento del propósito del alcance se utiliza el método de las elipses concéntricas el cual se construye a través de tres pasos:

- Paso 1.

Se describe la información que se ha de ubicar en la elipse más interna, para ello se debe determinar los procesos y/o subprocesos, lo que comúnmente se conoce como servicios, esto para ayudar en adelante a la identificación de los activos de información.

- Paso 2.

En la elipse intermedia se identifican los procesos internos propios de la entidad con los cuales se interactúa constantemente.

- Paso 3.

En la elipse más externa, se identifican todas aquellas entidades externas con las cuales se tenga una interacción.

2.3.3 Identificación de Inventario de activos

Posterior a la construcción del alcance se pasa a la identificación del inventario de activo con la finalidad de conocer la relación de los recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y requieran protección de potenciales riesgos.

Para el desarrollo de este atributo se utiliza las fichas de la metodología magerit la cual describe la manera como se debe diligenciar el inventario de activo conforme a los siguientes aspectos que se identifican en las fichas: Activos esenciales de información, Activos esenciales de servicios, Datos / información, Servicios, Aplicaciones / Software, Equipamiento informático (hardware) Redes de comunicación, Soporte de información, Instalaciones y Personal.

Ahora bien, en los diferentes formatos cada uno incluye aspecto como:

- **Código:** sirve para identificar el activo
- **Nombre:** en esta se incluye el nombre del activo

- **Descripción:** se describe la característica del activo
- **Propietario:** se coloca el nombre de la persona que tiene asignado el activo
- **Responsable:** se coloca el nombre de la persona que está a cargo del activo

2.3.4 Identificación de Vulnerabilidades

Una vez realizado el inventario de activos se pasa al atributo vulnerabilidades para reportar las debilidades que ponen en riesgo la seguridad de la información, en este caso se utiliza el anexo de (D) de la norma IEC/ISO 27005 el cual detalla la forma y la manera en cómo se debe reportar las vulnerabilidades que se consigna dentro de la estructura de la organización, dicho formato está estructurado de la siguiente manera:

- **Tipo:** este campo clasifica el tipo de activo con base a (hardware, software, red, personal, lugar, organización) de cuerdo a la vulnerabilidad que se puede dar.
- **Vulnerabilidad:** en este campo se identifica la vulnerabilidad que presenta el activo identificado.
- **Amenaza:** este campo se relaciona la amenaza de acuerdo a la vulnerabilidad que presenta el activo.

2.3.5 Identificación de Amenazas

Posterior a la identificación de las vulnerabilidades se pasa al atributo identificación de amenazas, con el propósito de conocer el tipo de amenaza que puede estar expuesto en los diferentes activos informáticos.

La identificación de amenaza se trabaja conforme a los lineamientos de la metodología Magerit la cual trabaja con base a los formatos identificados como desastre natural, de origen industrial, errores y fallos no intencionados y ataquen intencionados.
A continuación, se describen los campos que conforman los formatos de forma general:

- **Código:** descripción sucinta de lo que puede pasar conforme al tipo de amenaza.

- **Tipos de activos:** en este capo se describe que puede verse afectado por este tipo de amenaza.
- **Dimensiones:** este campo describe la amenaza de acuerdo a la afectación que tuvo el activo con relación a la (integridad, confidencialidad y disponibilidad).

Descripción: este campo describe lo que le sucedió al activo con base a la amenaza

2.3.6 Identificación de Riesgo

Posterior a la identificación de amenazas se pasa a la identificación del riesgo donde se identifica como la probabilidad de que una amenaza se convierta en un desastre, la identificación del riesgo se trabaja con base a la guía para la administración del riesgo y el diseño de controles en entidades púbicas (DAFF) incluyendo criterios de evaluación de probabilidad e impactó, estos criterios se detallan en las tablas siguientes:

Tabla 2-13. Criterio para calificar la probabilidad. Fuente: Elaboración propia.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Tabla 2-14. Criterios para calificar el impacto. Fuente: Elaboración propia.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Una vez identificado los criterios de valoración de la probabilidad y el impacto se consolida el nivel de riego del activo donde. De acuerdo a lo anterior se describe a continuación los campos que conforman el nivel de riesgo del activo:

- **Riesgo:** el riesgo se califica teniendo en cuenta la valoración de afectación del activo con base a la integridad, confidencialidad y disponibilidad
- **Activo:** es este campo se coloca el nombre del activo
- **Amenaza:** nombre de la amenaza que afecta al activo
- **Vulnerabilidad:** nombre de la vulnerabilidad que presenta el activo
- **Probabilidad:** se califica con base a los criterios de valoración de la probabilidad (insignificante, menor, moderado, mayor y catastrófico).
- **Impacto:** se califica con base a los criterios de valoración de impacto (insignificante, menor, moderado, mayor y catastrófico).
- **Zona de riesgo:** se califica con base a los criterios de valoración de (extremo = rojo, alto = naranja, moderado = amarillo, bajo = verde).

2.3.7 Identificación de Controles

Una vez que se ha detallado una lista de amenazas se debe revisar cada amenaza para determinar si existe controles existentes que aborden el problema de la amenaza con miras a la disminución progresiva del riesgo. La metodología con la que se trabaja la identificación de controles es la FRAAP la cual se detalla a continuación los ítems que integran su plantilla así:

- **Atributo**: en este campo se relaciona los controles con base a la integridad, confidencialidad y disponibilidad
- **Amenaza:** se describe las diferentes amenazas conforme al atributo
- **Control existente:** en este campo se relacionan los controles existentes que tenga aplicados para el control de la amenaza.

2.3.8 Manejo de incidentes

Para trabajar el manejo de incidentes se seleccionó la norma ISO/IEC 27035 por considerarla la que más se ajusta al proceso metodológico, debido a que facilita el cumplimiento del objetivo de la investigación y del mismo modo se articula con LA NORMA ISO/IEC 27001, conforme a estos se trabaja con el anexo D de la norma, el cual se detallan a continuación los campos que la integran:

- Número del incidente: se le asigna un numero para llevar el reporte de incidentes presentados
- Detalles del miembro del punto de contacto: este ítem lo conforman varios campos relacionados con los datos de la persona que reporta el incidente
- Detalles del miembro de ISIRT: este ítem se llena con la información de los datos personales del miembro del grupo de incidente que está conformado dentro de la organización
- Descripción de incidentes de seguridad de la información: en este campo se detalla la información del incidente teniendo en cuenta que ocurrió, como ocurrió, porque ocurrió, entre otras.
- Detalles del incidente de seguridad de la información: en este ítem se consigna la información que tiene que ver con la fecha y hora en la que ocurrió el incidente, fecha y hora en la que se descubrió el incidente, fecha y hora en la que se reportó el incidente, identificación y numero de contacto de la persona que hace el reporte.

2.3. Fase 4. Estudio de caso

Para la validación de la metodología, se realizaron 3 actividades, la primera fue socializar la metodología de gestión de riesgo, como segundo la encuesta de entendimiento de la metodología propuesta y como tercera la aplicación de la metodología propuesta, dichos procesos se detallaron de la siguiente manera:

2.3.1 Fase 4-1. Socialización de la metodología de gestión de riesgos

La socialización de la metodología se realizó mediante una video conferencia con los encargados del área de las TIC de la entidad objeto de estudio, debido a la situación de salud que afecta a la población en la actualidad, que impide las reuniones presenciales, en la cual se trató el siguiente tema:

Explicación de los diferentes formatos que componen la metodología propuesta y su forma de diligenciamiento

2.3.2 Fase 4-2. Entendimiento de la metodología propuesta

El cuestionario tiene como objetivo verificar el nivel de entendimiento de la metodología de gestión de riesgos. En este sentido es importante que la respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

El cuestionario se diseñó teniendo en cuenta 7 preguntas con su nivel de valoración. Con el propósito de diligenciarla esta se llenó de acuerdo a la escala que va de 1 a 5, donde 1 es totalmente en desacuerdo, y 5 totalmente de acuerdo, el cual fue compartido de forma virtual, estando estructurada de la siguiente forma:

Tabla 2-15. Aplicación de la metodología propuesta. Fuente: Elaboración propia.

N°	PREGUNTAS	NIVEL DE VALORACIÓN				
		1	2	3	4	5
1	¿Las fases en las que se estructura esta metodología son comprensibles y se ajusta a un adecuado entendimiento?					
2	¿La identificación de las elipses en sus diferentes pasos ayuda a la identificación de los procesos propios de la entidad?					
3	¿La identificación del inventario de activos es comprensible y se ajusta a las necesidades de la empresa?					
4	¿La identificación de las vulnerabilidades a través de los dos formatos utilizados, permitió analizar las causas fundamentales de vulnerabilidades?					
5	¿La identificación de las amenazas a través de los códigos son comprensibles y de fácil manejo?					
6	¿La identificación de los controles permitió evaluar los riesgos de una manera más precisa y clara?					
7	¿La etapa de identificación de riesgos permitió la consolidación, identificación de los diferentes riesgos (incluyendo el residual)?					

2.3.3 Fase 4-4 Aplicación de la metodología propuesta

Después de haber realizado las actividades anteriores se inicia la actividad de aplicar la metodología propuesta, iniciando esta con la designación de un funcionario del área TIC

para que realice las diferentes etapas que conforma la metodología propuesta para la entidad objeto de estudio.

El funcionario designado desarrollo la metodología comenzando por la primer etapa denominada Alcance donde definió la cobertura del SGSI aplicando el método de las elipses.

- Para la segunda etapa denominada inventario de activos el funcionario designado del área TIC realizo el inventario de activo conforme a los formatos de la metodología magerit donde realizo la identificación y descripción del activo o conforme a los formatos.
- En la tercer etapa denominada identificación de vulnerabilidades el funcionario del área TIC realizo la identificación de vulnerabilidades teniendo en cuenta los formatos de la norma IEC/ISO 27005 donde realizó la descripción de las vulnerabilidades de los activos del área objeto de estudio.
- La cuarta etapa denominada identificación de amenazas el funcionario del área TIC realizo la identificación de la amenaza teniendo en cuenta los formatos de la metodología magerit donde se realizó la descripción de la amenaza de los activos del área objeto de estudio.
- En la quinta etapa denominada identificación del riesgo el funcionario del área TIC realizo la identificación del riesgo teniendo en cuenta los formatos de la metodología DAFF donde realizó la descripción del riesgo de los activos del área objeto de estudio.
- La sexta etapa denominada identificación de controles el funcionario del área TIC realizo la identificación de controles aplicados teniendo en cuanta el formato de la metodología FRAAP donde realizo la identificación de controles existentes en los activos del área objeto de estudio.
- Por último, la séptima etapa denominada manejo de incidentes donde el funcionario del área TIC realizo la identificación de un incidente de seguridad

teniendo en cuenta los formatos de la metodología ISO/IEC 27035 con base al anexo D aplicado a los activos del área objeto de estudio.

3. Capítulo III - Resultados

A continuación, se describen los diferentes resultados obtenidos de acuerdo a la metodología planteada

3.1. Fase 1. Diagnostico empresarial

3.1.1 Fase 1-1: Entrevistas con funcionario encargado del TIC

Con base al diseño de la entrevista estructurada que se le realizo al encargado del área de las TIC de la empresa del sector público, se obtuvieron los siguientes resultados de acuerdo al siguiente esquema (ver Tabla 3-1 entrevista funcionario):

Tabla 3-1. Entrevista funcionario. Fuente: elaboración propia.

Número	Pregunta	Respuesta
1	¿Cuáles son los activos tecnológicos de la empresa?	Dentro de la empresa se encuentran varios equipos de cómputos, dispositivos de interconexión, servidores y software necesario para el desarrollo de las funciones
2	¿Qué cantidad tienen de cada equipo?	Es variado, se encuentran dentro del activo también aires acondicionados, portátiles y equipos fijos, todo ellos son destinados para una función en específico dependiendo de los funcionarios que lo utilicen
3	¿Dónde es la ubicación física de cada equipo?	La ubicación de estos equipos se encuentra en diferentes sectores, básicamente son dos, en el edificio la confianza y el antiguo edificio de la salud que es precisamente donde se encuentra el área de TIC
4	¿Cuentan con Sistema de Gestión de Seguridad de Información?	No, la mitigación del riesgo se realiza creando contraseñas y visitando solo lugares seguros, además cuenta la dependencia con una red interna en la que se comparte la

		información entre los empleados de cada una de las dependencias, lo que genera autonomía en las redes
5	¿Cuenta con antivirus y programas actualizado y licenciado?	Cada uno de los equipos tienen antivirus, pero sin renovación de la licencia.
6	¿Qué tipos de incidentes informáticos han tenido?	El único recurrente es el malware
7	¿Qué tipo de infraestructura tecnológica están utilizando?	Todos los procesos se manejan de forma independiente debido a que no cuentan con una infraestructura, y esto hace que los procesos queden más expuestos a vulnerabilidades que luego se puedan aprovechar como una amenaza hacia los sistemas tecnológicos con lo que cuenta la entidad.

3.1.2 Fase 1-2: Inventario de activos

De acuerdo al diseño utilizado para el levantamiento de información de activos que están bajo el dominio del área de las TIC fue posible discriminar todos los equipos que hacen parte de ella, utilizando el siguiente formato (ver tabla 3-2) donde se evidencian los siguientes resultados obtenidos:

Tabla 3-2. Inventario de activos. Fuente: Elaboración propia.

Nombre Activos	Cantidad	Categoría	Descripción
SWITCH HP 48 PUERTOS	3	Hardware	Administración De Cámara, Dispositivos Ap.
SWITCH HP 24 PUERTOS	2	Hardware	Administración De Cámara, Dispositivos Ap.
AP WIKITI	2	Hardware	Administración De Wifi
ROUTER - MEDIA COMER	1	Hardware	Administración De Internet
MEDIA COMER –INTERNET	1	Servicios	Proveedor De Servicio De Internet
GABINETE –RACK	1	Hardware	Alojamiento De Dispositivos
MESA DE ESCRITORIO CAFÉ	1	Servicios	Mesa Donde Reposa Un Computador
AIRE ACONDICIONADO _SAMSUNG	1	Hardware	Suministra Aire En El Espacio De Oficina Tic
NVR-HIKVISION - 16 PUERTOS	1	Hardware	Administración De Las Cámara Ip
CAMARAS IP - -HIKVISION	7	Hardware	Visualización De Videos
CAMARAS IP - -HIKVISION	1	Hardware	Visualización De Videos

ROURTER MIKROTIC	1	Hardware	Administración Del Dhcp
COMPUTADOR DE ESCRITORIO HP	1	Hardware	Utilización De Copias De Seguridad, Clonación De Disco
COMPUTADOR PORTATIL HP	1	Hardware	Administración De Servicios
WINBOX	1	Software	Software Para Revisar El Estado De Las Mikrotic
UBENT DISCOVERIS	1	Software	Revisión Del Estados De Los Radios
PUTTY VERSION 0.72	1	Software	Administración Del Ssh
DNS - 343-B1	1	Software	Administración Servicio Nat - Copia De Seguridad
TFTP2	1	Software	Subida Del Firewall Cuando Se Cae
RUFU - MEMORIA	1	Software	Realización De Memorias Bootebles
VIDEO ADMIN - BASES DE DATOS	1	Software	Administración Del Control De Acceso De Funcionarios

SERVIDOR_01_DELL_MODELO_ POWEREDGE R70 (FIREWALL)	1	Hardware	Administra El Firewall De Internet
Servidor_03_Dell_Modelo_pow erEdge R70 (PCT)	1	Hardware	Administración Del Software Financiero
ROURTER MIKROTIC	1	Hardware	Administración De Red Wifi Cuarto Piso
AP MIKROTIC	3	Hardware	Provee Servicio Inalámbrico
GABINETE -RACK-3	1	Hardware	Alojamiento De Dispositivos RourteMickotic - 2 Switch 24 P. Hp
GABINETE -RACK -2	1	Hardware	Alojamiento De Dispositivos 2 Switch Hp De 24 P.
GABINETE -RACK -1	1	Hardware	Alojamiento De Los Dos Servidores Dell, 2 Switch 24 P. Hp
IMPRESORA - HP LASERJET PRO MFP-M127	1	Hardware	Impresiones De Documentos De Las Dependencia Tic
LENOVO BLANCO TODO EN UNO DE 22Pulg	1	Hardware	Oficios Varios De La Oficina

HP 21 Pulg TODO EN UNO	1	Hardware	Administración Pagina Web Del Ministerio Tic
LENOVO NEGRO TODO EN UNO DE 22Pulg	1	Hardware	Administración Sistemas Financieros, Y Sistemas De Información
BASE DE DATOS SQL Version 11	1		Servidor Pct
KASPERKY	200		Antivirus

3.1.3 Fase 1-3: Identificación de los ítems a medir

Los ítems a medir que fueron tomados en cuenta para los resultados, fueron evaluados conforme a la escala de valoración que hace parte como uno de los ítems del análisis de brecha (GAP) (ver Tabla 3-3):

Tabla 3-3. Escala de valoración. Fuente: Elaboración propia.

Escala de valoración		
%de cumplimiento	Cuantitativo	Cualitativo
0%	0	Inexistente
10%	1	Inicial que está en un proceso apenas de implementación,
50%	2	Reproducible/intuitivo conoce mínimamente el control, pero no lo tiene en ejecución, es decir no se ha implementado
90%	3	Proceso definido: hace referencia a la implementación incompleto
95%	4	Gestionado y medible, es ya está implementado y lo dirige
100%	5	Optimizado es que todos los controles se encuentran implementados y conoce del tema, sabe cómo funciona, conoce la importancia de implementar los controles, es decir, el control está en ejecución

Teniendo en cuenta la escala de evaluación, se empezarán a mostrar los resultados obtenidos dentro del análisis realizado a la empresa, logrando consolidar de esta manera, a través del nivel de cumplimiento, las falencias en las que puede incurrir dicha empresa. Gracias al diseño estructurado basado en la norma ISO/IEC 27002 anexo A de la norma ISO/IEC 27001:2013 fue posible obtener los siguientes resultados en materia de controles

aplicados o no aplicados en la entidad pública objeto de estudio, determinando así que tan cerca está la organización en materia de seguridad informática, las cuales se consolidaron en las siguientes tablas de resultados:

Tabla 3-4. Políticas de seguridad. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.5	Políticas de Seguridad	1,0	Inicial	10%	No existen politicas de seguridad en la infraestructura de red, que actualmente tienen en ejecucion
A.5.1	Orientación de la Dirección para la Gestión de la seguridad de la información	0,0	Inexistente	0%	
A.5.1.1	Políticas para la seguridad de la información	0	Inexistente	0%	las politicas minimas que tienen no son concertadas con la alta
A.5.1.2	Revisión de las políticas para la seguridad de la información	0	Inexistente	0%	

Frente a las políticas de seguridad y sus implicaciones, se debe resaltar solamente que cumple con un 10%, siguiendo la escala antes mencionada, se encuentra la empresa en un nivel inicial frente a la mitigación de riesgo, consolidando la orientación de la dirección para la gestión y se crean las políticas para la seguridad y la revisión de las mismas, ya que estas son inexistentes.

En cuanto a la organización interna, se evidencia una calificación cualitativa inexistente, ya que los roles y responsabilidad no se encuentran bien definidas, en consecuencia, no existe separación de deberes y el contacto con las autoridades es poca, frente a los celulares que deben integrar el inventario de activos, encontramos que, para esta empresa, estos elementos son inexistentes

Tabla 3-5. Organización de la Seguridad de la Información. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.6.1	Organización Interna	0,0	Inexistente	0%	
A.6.1.1	Roles y Responsabilidad para la seguridad de la Información	2	Reproducible / intuitivo	50%	
A.6.1.2	Separación de deberes	2	Reproducible / intuitivo	50%	
0	Contacto con las autoridades	2	Reproducible / intuitivo	50%	
A.6.1.4	Contacto con grupos de interés especial	0	Inexistente	0%	
A.6.1.5	Seguridad de la información en la gestión de proyectos	2	Reproducible / intuitivo	50%	
A.6.2	Dispositivos móviles y teletrabajo	0,0	Inexistente	0%	
A.6.2.1	Política de dispositivos móviles	0	Inexistente	0%	
A.6.2.2	Teletrabajo	0	Inexistente	0%	

Frente a la organización interna, los resultados arrojan que la organización tiene este acápite como inexistente, lo que impide el contacto con grupos de interés, dispositivos móviles, políticas de dispositivos, teletrabajo, son herramientas con las que debería contar toda la empresa del Estado, sin embargo para el estudio en mención, no existe, frente a los roles y responsabilidad para la seguridad de la información, la separación y el contacto con las autoridades y la seguridad frente a la información de los proyectos, si se evidencia un avance, aunque solo del 50%, es decir, se debe fortalecer este componente en la organización interna.

Tabla 3-6. Política de seguridad. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.7	Seguridad de los Recursos Humanos	0,3	Inexistente	0%	
A.7.1	Antes de asumir el empleo	0,0	Inexistente	0%	
A.7.1.1	Seleccion	0	Inexistente	0%	
A.7.1.2	Términos y condiciones de empleo	1	Inicial	10%	
A.7.2	Durante la ejecución del empleo	0,0	Inexistente	0%	
A.7.2.1	Responsabilidades de la dirección	0	Inexistente	0%	
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	0	Inexistente	0%	
A.7.2.3	Proceso disciplinario	0	Inexistente	0%	
A.7.3	Terminación y cambio de empleo	1	Inicial	10%	
A.7.3.1	Terminación o cambio de responsabilidades de empleo	1	Inicial	10%	

Frente a la seguridad de los recursos humanos, también se evidencia una inexistencia del componente, esto se debe a que solo se encuentra en una etapa inicial puesto que n son capacitados para asumir el empleo, los términos y condiciones, las responsabilidades de la dirección y en general, los ítems evaluados de esta sección no han sido trabajados.

Tabla 3-7. Gestión de Activos. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.8	Gestión de Activos	1,9	Inicial	10%	
A.8.1	Responsabilidad de los activos	2,0	Reproducible / intuitivo	50%	
A.8.1.1	Inventario de Activos	1	Inicial	10%	
A.8.1.2	Propiedad de los activos	2	Reproducible / intuitivo	50%	
A.8.1.3	Uso aceptable de los activos	1	Inicial	10%	
A.8.1.4	Devolución de activos	0	Inexistente	0%	
A.8.2	Clasificación de la información	1,7	Inicial	10%	
A.8.2.1	Clasificación de la información	2	Reproducible / intuitivo	50%	
A.8.2.2	Etiquetado de la información	2	Reproducible / intuitivo	50%	
A.8.2.3	Manejo de activos	1	Inicial	10%	
A.8.3	Manejo de medios	2,0	Reproducible / intuitivo	50%	
A.8.3.1	Gestión de medios removibles	0	Inexistente	0%	
A.8.3.2	Disposición de los medios	0	Inexistente	0%	
A.8.3.3	Transferencia de medios fisicos	0	Inexistente	0%	

Frente a la gestión de activos, es evidentemente uno de los acápites que más evolución representa, esto se debe a que, aunque la mayoría de los componentes se encuentra en una etapa inicial, es la responsabilidad de activos, la clasificación de la información, el etiquetado de la misma y el manejo de los medios, son elementos reproducibles, es decir, lo que pueden servir de base para la elaboración de estrategias que permitan fortalecer los demás elementos que hasta el momento se encuentran inexistentes

Por esto la estrategia para la implementación de la tecnología, deben estar actualizados pues los ítems evaluados rescatan información valiosa porque da un panorama actualizado de los activos de la empresa.

Tabla 3-8. Políticas de seguridad. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.9	Control de acceso	0,3	Inexistente	0%	
A.9.1	Requisitos del negocio para el control de acceso	1,0	Inicial	10%	
A.9.1.1	Politica de control de acceso	0	Inexistente	0%	
A.9.1.2	Acceso a redes y a servicios en red	0	Inexistente	0%	
A.9.2	Gestión de acceso de usuario	0,0	Inexistente	0%	
A.9.2.1	Registro y cancelación del registro de usuarios	0	Inexistente	0%	
A.9.2.2	Suministro de acceso de usuarios	0	Inexistente	0%	
A.9.2.3	Gestión de derechos de acceso privilegiado	0	Inexistente	0%	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	0	Inexistente	0%	
A.9.2.5	Revisión de los derechos de acceso de usuarios	0	Inexistente	0%	
A.9.2.6	Retiro o ajuste de los de derechos de acceso	0	Inexistente	0%	
A.9.3	Responsabilidades de usuario	0,0	Inexistente	0%	
A.9.3.1	Uso de información de autenticación secreta	0	Inexistente	0%	
A.9.4	Control de acceso al sistemas y aplicaciones	0,2	Inexistente	0%	
A.9.4.3	Sistema de gestión de contraseñas	1	Inicial	10%	
A.9.4.4	Uso de programas utilitarios privilegiados	0	Inexistente	0%	
A.9.4.5	Control de acceso a códigos fuente de programas	0	Inexistente	0%	
A.9.4.1	Restricciones de acceso a la información	0	Inexistente	0%	
A.9.4.2	Procedimiento de ingreso seguro	0	Inexistente	0%	

Al igual que los componentes anteriores, el resultado de la evaluación de esta sección también arroja como resultados elementos inexistentes, esto dificulta la seguridad frente al acceso de la información, cuando realmente no existen elementos de protección, los diferentes hackers, ingenieros, virus o demás elementos externos o internos que pueden generar daños dentro de la organización, son más propensos a delitos informáticos, ya que al igual que en todos los casos la empresa estaría en constante inseguridad frente a la protección de sus datos.

Tabla 3-9. Sección A 10. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.10	Criptografía	0,0	Inexistente	0%	
A.10.1	Controles criptográficos	0,0	Inexistente	0%	
A.10.1.1	Política sobre el uso de controles criptográficos	0	Inexistente	0%	
A.10.1.2	Gestión de llaves	0	Inexistente	0%	

Frente a la criptografía, el análisis también arroja ser inexistente, esto es importante ya que, gracias a este elemento, es posible lograr una mayor seguridad dentro de la

información que se distribuye o se maneja dentro de la empresa, bajo esta lógica, este componente también debe ser estructurado desde la seguridad de los usuarios y los empleados de la entidad.

Tabla 3-10. Sección A 11. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.11	Seguridad física y del entorno	1,4	Inicial	10%	
A.11.1	Áreas seguras	2,0	Reproducible / intuitivo	50%	
A.11.1.1	Perímetro de seguridad física	2	Reproducible / intuitivo	50%	
A.11.1.2	Controles de acceso físicos	2	Reproducible / intuitivo	50%	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	2	Reproducible / intuitivo	50%	
A.11.1.4	Protección contra las amenazas externas y ambientales	1	Inicial	10%	
A.11.1.5	Trabajo en áreas seguras	1	Inicial	10%	
A.11.1.6	Áreas de despacho y carga.	1	Inicial	10%	
A.11.2	Equipos	0,8	Inexistente	0%	
A.11.2.7	Disposición segura o reutilización de equipos	2	Reproducible / intuitivo	50%	
A.11.2.8	Equipo de usuario desatendido	1	Inicial	10%	
A.11.2.9	Política de escritorio limpio y pantalla limpia	0	Inexistente	0%	
A.11.2.1	Ubicacion y protección de los equipos	0	Inexistente	0%	
A.11.2.2	Servicios de suministro	1	Inicial	10%	
A.11.2.3	Seguridad del cableado	0	Inexistente	0%	
A.11.2.4	Mantenimiento de equipos	1	Inicial	10%	
A.11.2.5	Retiro de activos	1	Inicial	10%	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	1	Inicial	10%	

Esta sección, hace parte de la seguridad física y del entorno, a nivel general, se puede establecer que esta se encuentra en una etapa inicial, mostrando que, muchos de sus elementos se están ejecutando de manera intuitiva, sin embargo, falta fortalecer diferentes componentes como la seguridad del cableado y las políticas de escritorio y pantalla limpia, además de la ubicación y la protección de los equipos.

Tabla 3-11. Sección A 12. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.12	Seguridad en las operaciones	0,8	Inexistente	0%	
A.12.1	Procedimientos operacionales y responsabilidades	1,0	Inicial	10%	
A.12.1.1	Procedimientos de operación documentados	1	Inicial	10%	
A.12.1.2	Gestión de cambios	1	Inicial	10%	
A.12.1.3	Gestión de la capacidad	1	Inicial	10%	
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	1	Inicial	10%	
A.12.2	Protección contra códigos maliciosos	0,0	Inexistente	0%	
A.12.2.1	Controles contra códigos maliciosos	0	Inexistente	0%	
A.12.3	Copias de respaldo	2,0	Reproducible / intuitiva	50%	
A.12.3.1	Respaldo de la información	2	Reproducible / intuitivo	50%	
A.12.4	Registro y seguimiento	1,0	Inicial	10%	
A.12.4.1	Registro de eventos	1	Inicial	10%	
A.12.4.2	Protección de la información de registros	1	Inicial	10%	
A.12.4.3	Registros de administración y operador	1	Inicial	10%	
A.12.4.4	Sincronización del relojes	1	Inicial	10%	
A.12.5	Control de software operacional	0,0	Inexistente	0%	
A.12.5.1	Instalación de software en sistemas operativos	0	Inexistente	0%	
A.12.6	Gestión de la vulnerabilidad técnica	0,5	Inexistente	0%	
A.12.6.1	Gestión de las vulnerabilidades técnicas	1	Inicial	10%	
A.12.6.2	Restricciones sobre la instalación de software	0	Inexistente	0%	
A.12.7	Consideraciones sobre auditorías de sistemas de información	1,0	Inicial	10%	

Seguridad en las operaciones, constituye otro de los elementos a reforzar dentro de la empresa del estado, el resultado de la investigación realizada, muestra que está en una etapa inicial, pero tiene unos elementos que ya se están implementando, aunque de manera intuitiva, como la seguridad y el respaldo de la información, esto es bueno porque permite identificar la importancia que los funcionarios le dan a la información que guardan dentro de los equipos tecnológicos que manejan, ya que de esta manera se pueden garantizar la protección de los documentos que guardan.

Tabla 3-12. Sección A 13. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.13	Seguridad de las comunicaciones	0,3	Inexistente	0%	
A.13.1	Gestión de la seguridad de las redes	0,3	Inexistente	0%	
A.13.1.1	Controles de Red	0	Inexistente	0%	
A.13.1.2	Seguridad de los servicios de red	0	Inexistente	0%	
A.13.1.3	Separación en las redes	1	Inicial	10%	
A.13.2	Transferencia de información	0,3	Inexistente	0%	
A.13.2.1	Políticas y procedimientos de transferencia de información	0	Inexistente	0%	
A.13.2.2	Acuerdos sobre transferencia de información	0	Inexistente	0%	
A.13.2.3	Mensajería electrónica	1	Inicial	10%	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	0	Inexistente	0%	

La seguridad en las comunicaciones también arroja como resultado ser inexistente, aunque solamente dos elementos se presentan en etapa inicial son las separaciones de redes y el mensaje electrónica, sin embargo, los demás elementos son inexistentes y es evidente que debe ser creado y fortalecido para poder estructurar el SGSI de la empresa

Tabla 3-13. Sección A 14 Adquisición, desarrollo y mantenimiento de sistemas. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0,1	Inexistente	0%	
A.14.1	Requisitos de seguridad de los sistemas de información	0,0	Inexistente	0%	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	0	Inexistente	0%	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	0	Inexistente	0%	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	0	Inexistente	0%	
A.14.2	Seguridad en los procesos de desarrollo y de soporte	0,2	Inexistente	0%	
A.14.2.1	Política de desarrollo seguro	0	Inexistente	0%	
A.14.2.2	Procedimientos de control de cambios en sistemas	1	Inicial	10%	
A.14.2.3	Revisión técnica de las aplicaciones despues de cambios en la plataforma de operación	0	Inexistente	0%	
A.14.2.4	Restricciones en los cambios a los paquetes de software	1	Inicial	10%	
A.14.2.5	Principios de construcción de los sistemas seguros	0	Inexistente	0%	
A.14.2.6	Ambiente de desarrollo seguro	0	Inexistente	0%	
A.14.2.7	Desarrollo contratado externamente	0	Inexistente	0%	
A.14.2.8	Pruebas de seguridad de sistemas	0	Inexistente	0%	
A.14.2.9	Pruebas de aceptación de sistemas	0	Inexistente	0%	
A.14.3	Datos de prueba	0,0	Inexistente	0%	
A.14.3.1	Protección de datos de prueba	0	Inexistente	0%	

Gracias a este cuadro, es posible evidenciar que la revisión técnica, restricción de cambios, construcciones de sistemas y ambientes seguros, junto con el desarrollo y las pruebas necesarias, es inexistente, evidentemente es importante generar estrategias de cambio y consolidar estas falencias como una de las fortalezas de la empresa.

Tabla 3-14. Sección A 15. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.15	Relaciones con los proveedores	0,0	Inexistente	0%	
A.15.1	Seguridad de la información en las relaciones con los proveedores	0,0	Inexistente	0%	
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	0	Inexistente	0%	
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	0	Inexistente	0%	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	0	Inexistente	0%	
A.15.2	Gestión de la prestación de servicios del proveedores	0,0	Inexistente	0%	
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	0	Inexistente	0%	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	0	Inexistente	0%	

Frente a la relación con los proveedores, es evidente mostrar que estos factores son inexistentes en su totalidad, por esto es importante empezar con la estrategia para consolidar elementos optimizados frente a las relaciones con los proveedores.

Tabla 3-15. Sección 16. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.16	Gestión de incidentes de seguridad de la información	0,0	Inexistente	0%	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la informacion	0,0	Inexistente	0%	
A.16.1.1	Responsabilidades y procedimientos	0	Inexistente	0%	
A.16.1.2	Reporte de eventos de seguridad de la información	0	Inexistente	0%	
A.16.1.3	Reporte de debilidades de seguridad de la información	0	Inexistente	0%	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	0	Inexistente	0%	
A.16.1.5	Respuesta a incidentes de seguridad de la información	0	Inexistente	0%	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	0	Inexistente	0%	
A.16.1.7	Recolección de Datos	0	Inexistente	0%	

La Gestión de incidentes de seguridad de la información, también muestran resultados inexistentes todos los elementos que integran esta sección no arrojan ningún resultado, ya que son elementos que no han sido implementados dentro de la empresa.

Tabla 3-16. Sección A 17. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	0,0	Inexistente	0%	
A.17.1	Continuidad de seguridad de la información	0,0		0%	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	0	Inexistente	0%	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	0	Inexistente	0%	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0	Inexistente	0%	
A.17.2	Redundancias	0,0	Inexistente	0%	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	0	Inexistente	0%	

Ante una herramienta de la seguridad de la información, arrojando como resultado inexistente, ya que no implementan la continuidad, planificación, implementación de la continuidad de la seguridad en la información, y mucho menos la verificación de la misma.

Es importante entonces empezar a replantear las estrategias que se están implementando y al mismo tiempo gestionar espacios, técnicas, y herramientas tanto con los empleados como con directivos y usuarios de la empresa, para que de esta manera se capaciten a las personas para que implementen el SGSI.

Tabla 3-17. Sección 18. Fuente: Elaboración propia.

Sección	Control	Cuantitativo	Cualitativo	% Cumplimiento	Observacion (Breve descripción de la situación)
A.18	Cumplimiento	0,0	Inexistente	0%	
A.18.1	Cumplimiento de requisitos legales y contractuales	0,0	Inexistente	0%	
A.18.1.1	Identificación de la legislación aplicable y requerimientos contractuales	0	Inexistente	0%	
A.18.1.2	Derechos de propiedad intelectual	0	Inexistente	0%	
A.18.1.3	Protección de registros	0	Inexistente	0%	
A.18.1.4	Privacidad y protección de información de datos personales	0	Inexistente	0%	
A.18.1.5	Reglamentación de controles criptográficos	0	Inexistente	0%	
A.18.2	Revisiónes de seguridad de la información	0,0	Inexistente	0%	
A.18.2.1	Revisión independiente de la seguridad de la información	0	Inexistente	0%	
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	0	Inexistente	0%	
A.18.2.3	Revisión del cumplimiento técnico	0	Inexistente	0%	

Este componente también muestra resultados inexistentes, es importante empezar a generar estrategias de protección de datos, ya que son elementos que se desconocen o no se emplean, pero ahora, debido a la necesidad tan inminente que existe frente a la protección de los datos personales, se deben corregir estas falencias para que de esta manera tanto los usuarios como los trabajadores se encuentren protegidos dentro de las instalaciones de la empresa.

Los datos anteriormente analizados, fueron obtenidos mediante la aplicación de la observación, auditoria e implementación de la lista de chequeo que permitió identificar las diferentes falencias que se presentan dentro de la empresa, es importante aclarar que la información recolectada dentro del análisis de estos factores, solamente serán tenidos en cuenta como un análisis académico, y no será utilizado en ningún momento como elemento de juicio para la administración.

Evidentemente, es importante resaltar que la empresa del Estado, no implementa el SGSI pues, aunque la normatividad reporta existir desde hace muchos años, la implementación de este tipo de sistemas apenas está empezando a ser utilizada y necesaria, pues cada vez más se están presentando delitos informáticos a las empresas públicas del país.

3.1.3.1 Ponderación de los valores definidos

Gracias al análisis de cada una de las secciones aplicadas en el análisis de brecha (GAP) fue posible la consolidación de cada uno de los dominios aplicados en materia de seguridad informática en la organización arrojando los resultados de los controles en la siguiente tabla (ver tabla 3-18. Resultados GAP):

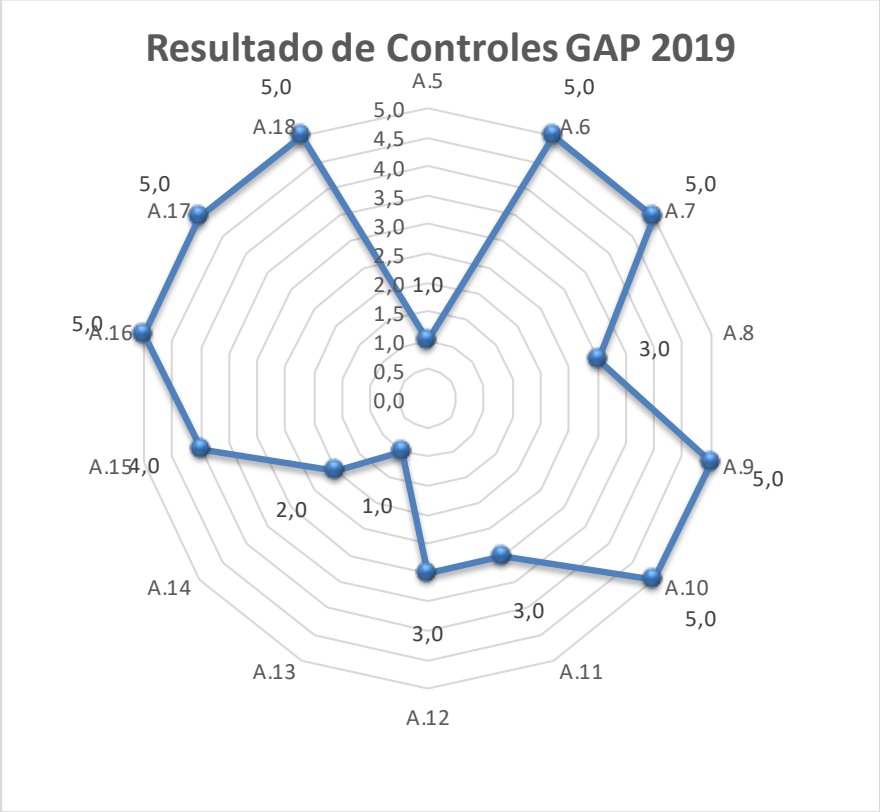
Tabla 3-18. Resultados GAP. Fuente: Elaboración propia.

Sección	Dominio	Valor	Estado	% Cumplimiento
A.5	Políticas de Seguridad	1,0	Inicial	10%
A.6	Organización de la Seguridad de la Información	5,0	Reproducible / intuitivo	50%
A.7	Seguridad de los Recursos Humanos	5,0	Reproducible / intuitivo	50%
A.8	Gestión de Activos	3,0	Inicial	10%
A.9	Control de acceso	5,0	Reproducible / intuitivo	50%
A.10	Criptografía	5,0	Inicial	10%
A.11	Seguridad física y del entorno	3,0	Reproducible / intuitivo	50%

A.12	Seguridad en las operaciones	3,0	Reproducible / intuitivo	50%
A.13	Seguridad de las comunicaciones	1,0	Reproducible / intuitivo	50%
A.14	Adquisición, desarrollo y mantenimiento de sistemas	2,0	Inicial	10%
A.15	Relaciones con los proveedores	4,0	Reproducible / intuitivo	50%
A.16	Gestión de incidentes de seguridad de la información	5,0	Reproducible / intuitivo	50%
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	5,0	Inicial	10%
A.18	Cumplimiento	5,0	Reproducible / intuitivo	50%

Los resultados obtenidos en base a la aplicación del análisis de brecha (GAP) se pueden ver también de forma gráfica en la siguiente telaraña (ver ilustración32 resultado de controles GAP):

Tabla 3-19. Resultado de controles GAP. Fuente: Elaboración propia.



Es de resaltar que el análisis de la telaraña debe ser leídos de abajo hacia arriba, mirando los puntos de interceptación, así como los puntos altos tienen controles aplicados, los puntos bajos es porque tienen controles, pero no están aplicados.

En este caso por ejemplo es factible establecer que los controles que no están siendo aplicados en la entidad del estado, son los siguientes:

- A5 – Políticas de seguridad.
- A8 – Seguridad de los recursos humanos.
- A11–Control de acceso.
- A12 - Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información.
- A13 – Gestión De Los Incidentes De La Seguridad De La Información.
- A14 - Gestión De La Continuidad Del Negocio.

Teniendo en cuenta esto, se debe señalar que, en materia de política de seguridad, se debe tener en cuenta el % de cumplimiento de los controles que tiene la organización, estableciendo que en el caso objeto de estudio, la mayoría de los dominios se encuentran debajo de 50%, lo que significa que apenas están en proceso de ejecución y elaboración de estos controles y algunos de ellos no se encuentra con ningún control aplicado.

Finalmente las metodologías que fueron objeto de estudio, permiten identificar cada uno de los factores, posibilidades, riesgos, amenazas o demás componentes que generan posibles riesgos a las entidades, todo esto teniendo en cuenta que las entidades gubernamentales en Colombia, son entidades que deben verificar que el sistema de Seguridad de la Información en donde se especifican los controles a evaluar según la norma ISO/IEC 27005, delimitando así el alcance de la evaluación final del SGSI, ya que la elección de dichos atributos depende de la prioridad otorgada la alta dirección. [1, 20]

3.2. Fase 2: características de las metodologías para la determinación del riesgo tecnológico

3.2.1. Fase 2-1: Identificar las metodologías objeto de estudio con base al análisis de riesgos

Las metodologías objeto de estudio, fueron seleccionadas porque cada una de ellas tiene unas características específicas que permiten generar un análisis o estudio completo identificando cada uno de los criterios que son comunes o no entre ellas, los cuales están basados en un análisis de riesgo.

- **Aplicación al sector público**: Para realizarla valoración se estudió cada una de las metodologías buscando si aplicaba o no al sector público, en este caso frente a las metodologías FRAP; OCTAVE; Norma Técnica colombiana NTC- ISO/ IEC 27005 NORMA TÉCNICA COLOMBIANA NTC- ISO-31000 no se evidencia esta categoría dentro de los documentos, lo que permite inferir que no tiene una aplicación en un tipo de empresa en específico, sin embargo, la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en

Entidades Públicas en adelante (DAFP) busca unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así, evitar duplicidades o re procesos [9].

Frente a las metodologías de análisis y gestión de riesgos de los sistemas de información MARGERIT, national instituto of estándares and technology y la Guía Para La Implementación Del Principio De Responsabilidad, aunque no determinan si son aplicables estas metodologías para el sector público o privado, si consagran criterios unificados frente al fortalecimiento del enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

- **Quien la genera:** Es el segundo factor que se tiene en cuenta en la valoración, por esta razón lo que se hizo fue buscar en cada una de las metodologías cual era el organismo o la entidad que las creaba, es así como se puede determinar que en el caso de la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT y la FRAP son desarrolladas por organismos de carácter internacional y posteriormente son acogidas por Colombia, a diferencia de la DAFP que es implementada por Departamento Administrativo de la Función Pública.
- **Tamaño de la Empresa:** para el estudio de este atributo, se determinó en cada metodología si estas comprendían el tipo de empresa al que sería aplicada, por esta razón es importante aclarar que la FRAP, DAFP, METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN MARGERIT, ISO-27005 y ISO-31000 [9], aplican para todo tipo de empresa, mientras que la NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST no aplica a las pequeñas empresas, ya que lo que se busca con este tipo de metodología es proteger la información de las entidades administrativas; por otra parte, la metodología

OCTAVE aunque fue diseñada para grandes empresas, puede ser implementada en todas las empresas [7, 8].

- **Inventario de Activos**: El cuarto atributo es el inventario de activos, dentro del que se incluye clasificación y valoración (integridad, confidencialidad, disponibilidad), para que pudiera ser analizado esta característica, se estudió dentro de cada metodología si llevaban estos tres componentes, identificando que en las normas ISO-31000, DAFP, FRAP, NIST, METODOLOGÍA OCTAVE y la guía para la implementación del principio de responsabilidad no se habla de este componente, mientras que en las metodologías norma Técnica NTC/ISO 27005 Y MAGERIT se pueden evidenciar una mayor profundidad dentro de los elementos que integran inventario de activos [1].
- **Clasificación de acuerdo con la integridad:** se evaluó según las diferentes metodologías, en las que se buscó de qué manera se establecían en cada una de ellas, mostrando como similitud una clasificación de tres niveles (alta, media y baja), por esta razón en la FRAP por su parte define este atributo como aquel que protege contra la modificación o destrucción incorrecta de la información, e incluye garantizar el no repudio y la autenticidad de la información; la DAFP afirma que este hace referencia a la propiedad de exactitud y completitud; metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT muestra que si bien es cierto que se muestra que esto hace parte de los errores que se pueden llegar a presentar dentro del proceso, no define este atributo dentro del documento, en la OCTAVE, la define como asegurar que un activo de información permanezca en la condición prevista por el propietario y para los fines previstos por el propietario [8].
- **Clasificación de acuerdo con la disponibilidad:** Este atributo fue analizado conforme a la disponibilidad de la información y si esta es accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los

recursos necesarios para su uso, la FRAP hace referencia a que la disponibilidad debe garantizar el acceso oportuno y confiable y el uso de la información, la DAFP la muestra como una propiedad accesible y utilizable a demanda por una entidad; METODOLOGÍA OCTAVE hace referencia asegurar que el activo de información permanezca accesible para el usuario autorizado, la NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST y la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MARGERIT, la mencionan pero no la define, mientras que la ISO-27005, ISO-31000 y la guía para la implementación del principio de responsabilidad demostrado (accountability).

- **Vulnerabilidad:** es el quinto atributo, entendido este como una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, en cuanto a las metodologías estudiadas se puede afirmar que la FRAP, menciona los tipos de vulnerabilidad más no los define, al igual que la metodología de análisis y gestión de riesgos de los sistemas de información MARGERIT, OCTAVE; ISO-27005, mientras que la NIST, ISO-31000 y la Guía Para La Implementación Del Principio De Responsabilidad Demostrado (Accountability) no hablan de este atributo.
- **Amenazas**: este es el sexto atributo que fue analizado desde la mirada de las diferentes amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas [17].

Así pues, se resalta que en la FRAPP muestra que la causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o una organización, la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT sabiendo que no todas las amenazas son significativas sobre todos los sistemas; pero con una razonable esperanza de que este catálogo crezca lentamente.

- **Riesgo:** Este busca identificar los medios para facilitar la interacción entre los ciudadanos y la misma de manera efectiva, bajo el apoyo de herramientas tecnológicas, los empleados deben comprometerse por preservar la confidencialidad, integridad y disponibilidad de la información que la entidad produce, recolecta o gestiona, de acuerdo con la regulación aplicable. Es de resaltar que las metodologías que más hacen referencia al tema son: NTC/IEC ISO 27005, ISO 31000, FRAAP, LA DAFP y la Guía para la administración del riesgo y el diseño de controles en entidades públicas.
- **Probabilidad;** fue un elemento estudiado ya que gracias a este se podrán identificar amenazas y usando una fórmula que relacione la probabilidad y el impacto, el equipo luego fijará un nivel de riesgo para cada amenaza y finalmente seleccionará posibles controles para reducir la intensidad del riesgo a un nivel aceptable, por esta razón las normas que más las mencionan son: ISO 27005 [1], FRAPP, LA DAFP y la Guía para la administración del riesgo.
- **Impacto:** El impacto fue abordado dependiendo de los "temas que suelen impactar la ocurrencia de los riesgos". En este paso puede encontrarse un símil con las dimensiones presentadas por Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT con los elementos presentados por FRAAP [9](sin embargo, las que más lo mencionan son la NTC/IEC ISO 27005 [1] y la FRAPP) se utilizan para llevar a cabo un análisis de riesgos mediante esta metodología o al menos con los pasos que describe la misma puede requerir de mucho tiempo y personal [18].

- **Controles:** estos son los últimos atributos evaluados, frente a la FRAPP: muestra que existen dos tipos de controles, el preventivo entendido este como los controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos y el correctivo se afirma como controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido.

Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes en las demás metodologías, no se hace referencia a este concepto [13]

Para poder entender cómo se desarrolló esta tabla, es necesario primero conocer que la lectura debe hacerse bajo la aplicación de dos (Si/no) caracteres que equivalen a si "aplica/ no aplica", lo que significa que en la metodología que se analiza, se menciona o no, el atributo estudiado [13].

A manera de resumen, el siguiente cuadro consolida los elementos anteriormente estudiados.

Tabla 3-20. Metodología por atributo evaluado. Fuente: elaboración propia.

METODOLOGÍAS	ATRIBUTOS																		
	Aplica Sector - Gobierno pública o privada		Quien la Genera de orden local o internacional		Tamaño – Empresa			Inventarios – Activos				Vulnerabilidades	Amenazas	Riesgo		Controles		
	Si	No	Local	Internacional	Grande	Mediana	Pequeña	Clasificación	Valoración					Probabilidad	Impacto	Clasificación	Diseño	Evaluación
									I	C	D							

FRAP		NO	NO	SI	SI	SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI
DAFP	SI		SI		SI	SI	SI	NO	SI	SI	SI	NO	NO	SI	SI	NO	NO	NO
METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN MARGERIT	SI		NO	SI	SI	SI	SI	SI	SI	SI	si	SI	SI	SI	SI	NO	NO	NO
NIST	SI		NO	SI	SI	SI	NO	NO	NO	NO	NO	SI	SI	SI	SI	SI	NO	NO
OCTAVE		NO	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI	SI	NO	NO	NO	NO	NO
ISO-27005		NO	NO	SI	SI	SI	SI	SI	NO	NO	NO	SI	SI	SI	SI	NO	NO	NO
ISO-31000		NO	NO	SI	SI	SI	SI	NO	NO	NO	NO	NO	NO	SI	SI	SI	NO	NO

Guía para la implementación del principio de responsabilidad demostrado (accountability)	SI		SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

El desarrollo de esta tabla permite consolidar de una manera más concreta, los atributos estudiados conforme a las metodologías de gestión de riesgos que fueron consultadas, extractando de esta manera cuales son los que establecen en mejor medida la manera en cómo debe de ejecutarse el atributo.

3.2.2. Fase 2-2: revisión de las metodologías de análisis de riesgo con base a los criterios inventario de activos, vulnerabilidades, amenazas, controles y riesgos

La revisión de los atributos evaluados se realizó a través del método de selección cualitativo y cuantitativo a través de un análisis de las diferentes metodologías, permitiendo así resaltar aquellos que mostraron en mayor detalle los procedimientos que se deben tener en cuenta para el desarrollo del mismo.

Partiendo de lo anterior se obtuvo la revisión de los diferentes atributos de las metodologías estudiadas las cuales fueron consolidadas en tablas y evaluadas por cada uno de los atributos:

3.3. Inventario de activos

En la siguiente tabla, es posible evidenciar la revisión de las metodologías de análisis de riesgo, mostrando que la que cumple con los criterios de valoración (obteniendo un nivel alto) es la metodología Magerit.

Tabla 3-21. Revisión de la metodología de riesgo conforme a los activos. Fuente: Elaboración propia.

	INVENTARIO DE ACTIVOS				VALORACIÓN		
		VALORACIÓN			CARACTERÍSTICAS EN		
METODOLOGÍA	CLASIFICACIÓN	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	%	NIVEL	ESTADO
Magerit	]La clasificación estableciendo que es la primera etapa por la que pasa la valoración de los activos de acuerdo a su importancia	Explica a que hace referencia y trabajaba conforme si está o no disponible	Muestra los diferentes tipos y como deben ser estos definidos	Plantea estrategias para la integridad de los activos	50%	ALTA	ELEGIBLE

NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018	Esta norma solo define la clasificación estableciendo que es la primera etapa por la que pasa la valoración de los activos de acuerdo a su importancia	Establece que la disponibilidad es una restricción que no permite que el proceso del SGSI sea efectivo	La metodología no trabaja conforme al atributo	Dependen del software o hardware	29%	BAJA	NO ELEGIBLE
NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 31000	La metodología no trabaja conforme al atributo	La metodología no trabaja conforme al atributo	La metodología no trabaja conforme al atributo	La metodología no trabaja conforme al atributo	15%	BAJA	NO ELEGIBLE

NIST RIST MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEM AND ORGANIZATION	La metodología no trabaja conforme al atributo	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	La metodología trabaja con factores contextuales en el que se incluye el nivel de sensibilidad de la PII, incluidos elementos específicos o en conjunto; los tipos de organizaciones que utilizan o interactúan con el sistema y las percepciones de	15%	BAJA	NO ELEGIBLE

				las personas sobre las organizaciones con respecto a la privacidad			
Octave	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	parte de una información ADN del activo. Son los requisitos de protección y sostenibilidad del activo	La metodología no trabaja conforme al atributo	Los requisitos de seguridad (confidencialidad, integridad y disponibilidad) son parte de una información ADN del activo	20%	BAJA	NO ELEGIBLE

Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas (DAFP)	Es el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	20%	BAJA	NO ELEGIBLE

	organización para funcionar en el entorno digital.						
Guía para la implementación del principio de responsabilidad demostrada (Accountability)	Se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital	Propiedad de ser accesible y utilizable a demanda por unas entidades se definen de acuerdo con el modelo de seguridad y privacidad de la información	Se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	30%	BAJA	NO ELEGIBLE

Metodología FRAAP	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	La metodología no trabaja conforme al atributo	La metodología no trabaja conforme al atributo	La metodología no trabaja conforme al atributo	10%	BAJA	NO ELEGIBLE

El resultado que arroja la anterior tabla se centra en que las ocho metodologías de riesgo que fueron objeto de análisis, si bien hablan o desarrollan los activos y su valoración, no todos detallan los procedimientos que se deben llevar a cabo para la correcta elaboración del inventario de activos, por esto es de resalar que la metodología seleccionada fue la magerit por cuanto identifica, establece y desarrolla actividades que permiten la consolidación de un inventario de activos completa, sin embargo las otras metodologías no cumplen con la valoración porque no tienen encuentra o desarrollan a profundidad elementos importantes para la consolidación del

inventario, por esto la menos valorada es la metodología FRAAP y la que alcanza una mejor posición es la NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018 [1].

3.4. Vulnerabilidades

El otro atributo analizado es vulnerabilidades, en este caso también se realizó un recuento de Las diferentes metodologías, sin embargo, se logra demostrar gracias a la siguiente tabla que la metodología que es elegible es la NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018 [1], concretamente el Anexo D

Tabla 3-22. Revisión de la metodología de riesgo conforme a vulnerabilidades. Fuente: Elaboración propia.

METODOLOGÍA	VULNERABILIDADES	VALORACIÓN		
		CARACTERÍSTICAS EN %	NIVEL	ESTADO
NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018	Son una lista de amenazas dentro de los activos y controles por esto deben ser reconocidas e identificadas para identificar el control a implementar, esto según el Anexo D ya que se consigna en este anexo los diferentes tipos de vulnerabilidades y las posibles amenazas	50%	Alta	Elegible
NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 31000	La metodología no trabaja conforme al atributo	0%	Nula	No elegible

NIST RIST MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEM AND ORGANIZATION	Acciones, dispositivos, procedimientos, técnicas u otras medidas que reducen la vulnerabilidad de un sistema	25%	Baja	No elegible
Octave	La identificación de vulnerabilidades en realidad da como resultado una pérdida de impulso y no proporciona información adicional que no se puede obtener mediante la identificación de escenarios.	5%	Baja	No elegible
Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas (DAFP)	La metodología no trabaja conforme al atributo	5%	Baja	No elegible
Guía para la implementación del principio de responsabilidad demostrada (Accountability)	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	5%	Baja	No elegible
Magerit	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	5%	Baja	No elegible

Metodología FRAAP	como un proceso que involucra un análisis de un sistema, aplicación, plataforma, proceso de negocio o segmento de operación de negocio a la vez. Al convocar un equipo de expertos interno, el FRAAP se basará en la propia gente de la organización para completar el proceso de evaluación de riesgos	25%	Baja	No elegible

La Metodología elegible en este caso es la NORMA TÉCNICA COLOMBIANA NTS/IEC 27005:2018 [1], por cuanto detalla cómo deben ser tratadas las vulnerabilidades como elemento indispensable de la gestión de riesgo, porque son elementos que se deben tener bajo constante control y actualización, las menos valoradas son la magerit, la accountability y la DAFF; la nula es la NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 3100.

3.5. Amenazas

En cuanto a las amenazas, tras la revisión de las metodologías de análisis de riesgo, fue posible concluir que la que se puede considerar elegible por cuanto cuenta con la mayor valoración es la Magerit quien trabaja bajo los anexos anexo 4a, 5a, 6, 7, 8, 9ª dentro de los cuales se hace posible consignar un catálogo de amenazas, sin embargo, también se utilizó la metodología FRAAP concretamente con el anexo 10 pues esta permite la categorización de amenazas muchas más pequeña.

Tabla 3-23. Revisión de la metodología de riesgo conforme a las amenazas. Fuente: Elaboración propia.

METODOLOGÍA	AMENAZAS	VALORACIÓN

		CARACTERÍSTICAS EN %	NIVEL	ESTADO
Magerit	Permite la identificación de un catálogo de amenazas que permite categorizar y ayudar a identificar los tipos que se puedan presentar, esto se realiza a través de diferentes anexos tales como anexo 4a, 5a, 6, 7, 8, 9ª	50%	ALTA	ELEGIBLE
Fraap	Permite la identificación de aquellas amenazas más pequeñas, esta metodología a través de sus formatos permite ser más preciso en la detección de la amenaza se trabajará conforme al anexo 10	40%	ALTA	ELEGIBLE

NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018	Establece que estas pueden ser de origen natural o humano por esto ninguna amenaza puede ser pasada por alto	30%	Baja	No elegible
NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 31000	La metodología no trabaja conforme al atributo	10%	Baja	No elegible
NIST RIST MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEM AND ORGANIZATION	incluyen fallas de equipos, interrupciones ambientales, errores humanos o de máquinas y ataques intencionados que a menudo son sofisticados, disciplinados, bien organizados y bien financiados	20%	Baja	No elegible
Octave	La metodología no trabaja conforme al atributo	10%	Baja	No elegible
Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de	Una vez se hayan registrado todas las amenazas para el primer atributo, el facilitador mostrará el segundo atributo para revisión con ejemplos de amenazas	25%	Baja	No elegible

Controles en Entidades Públicas (DAFP)	y dará al equipo entre tres a cinco minutos para escribir sus ideas			
Guía para la implementación del principio de responsabilidad demostrada (Accountability)	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	25%	Baja	No elegible

En este caso, las metodologías elegibles son dos, ya que una de ellas que es la FRAAP establece los lineamientos que se deben seguir [7], mientras que la MAGERIT trae un catálogo de amenazas que permiten definidas e identificadas.

3.6. Controles

A través de los formatos que facilito la metodología FRAAP [7] se realizaron la identificación de controles, lo que permitió aportar al programa de concientización dando así un punto de partida a la fase 4 en donde se da a conocer la metodóloga propia.

Tabla 3-24. Revisión de la metodología de riesgo conforme a los controles. Fuente: Elaboración propia.

METODOLOGÍA	CONTROLES			VALORACIÓN CARACTERÍSTICAS EN %	NIVEL	ESTADO
	CLASIFICACIÓN	DISEÑO	EVALUACIÓN			
Metodología FRAAP	Esta se realiza a través de una lista de posibles controles preventivos entendidos como aquellos que están diseñados para evitar un evento no deseado en el momento en el que ocurre; los controles defectivos se diseñan para identificar un evento o	Esto se realiza a través de identificar cada uno de los controles tiene una periodicidad específica, bajo un criterio de periodicidad para la realización del control, son este tipo de procesos los que se deben diseñar	Siguiendo las variables a considerar en la evaluación del diseño del control revisadas. Este tipo de procesos se define como fuerte, moderado o débil ; De igual forma, se menciona en esta dimensión que, para llevar a cabo el ejercicio de	50%	Alta	ELEGIBLE

	resultado que es previsto después de que se haya producido		planeación, la entidad debe documentar dicho ejercicio en donde se describa la parte conceptual u orientación estratégica; y la parte operativa en la que se señale de forma precisa los objetivos, las metas y resultados a lograr, las trayectorias de implantación o cursos de acción a seguir, cronogramas, responsables,			

			indicadores para monitorear y evaluar su cumplimiento y los riesgos que pueden afectar tal cumplimiento y los controles para su mitigación			
Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas (DAFP)	La metodología no especifica la manera o la forma en cómo se trabaja	solamente hace definición del atributo	La metodología no especifica la manera o la forma en cómo se trabaja	0%	Nulo	NO ELEGIBLE

NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 31000	la metodología no trabaja conforme al atributo	la metodología no trabaja conforme al atributo	Es el proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo para la determinación del mismo, su magnitud o ambos son aceptables	15%	BAJO	NO ELEGIBLE
NIST RIST MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEM AND ORGANIZATION	Se trabaja en Las pruebas, evaluaciones y validaciones consideran productos en configuraciones específicas y de forma aislada	Los pasos de RTF y las tareas asociadas se pueden aplicar a nuevos sistemas de desarrollo y sistemas existentes en las fases apropiadas del SDLC. Para los	la metodología no trabaja conforme al atributo	25%		NO ELEGIBLE

		sistemas nuevos y existentes, las organizaciones se aseguran de que se hayan completado las tareas designadas para prepararse para la ejecución del RTF				
Octave	la metodología no trabaja conforme al atributo	la metodología no trabaja conforme al atributo	la metodología no trabaja conforme al atributo	0%	Nulo	NO ELEGIBLE
Guía para la implementación del principio de responsabilidad demostrada (Accountability)	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	Debe tener definido el responsable de llevar a cabo la actividad de control, después Debe tener una periodicidad definida para su	la metodología no trabaja conforme al atributo	29%	Bajo	NO ELEGIBLE

		ejecución., además indicar cuál es el propósito del control, establecer el cómo se realiza la actividad de control,				
MARGERIT	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	la metodología no trabaja conforme al atributo	la metodología no trabaja conforme al atributo	5%	Bajo	NO ELEGIBLE

En este caso la metodología seleccionada es la FRAPP ya que esta plantea los diferentes controles que se pueden dar y al mismo tiempo fija los lineamientos que se deben de seguir con el objetivo de poder establecer los controles específicos que deben ser implementados

3.7. Riesgos

Para la identificación del riesgo, se realizó la revisión de las diferentes metodologías, estableciendo que la que cumple con los requisitos es la DAFP implementaron dos fichas que permitieron la detección de los riesgos por cada uno de los activos, todo esto bajo el formato AG. Mapa de riesgos y A4.4.

Tabla 3-25. Revisión de la metodología de riesgo conforme a los riesgos. Fuente: Elaboración propia.

METODOLOGÍA	RIESGO		VALORACIÓN		ESTADO
			CARACTERÍSTICAS EN %	NIVEL	
	PROBABILIDAD	IMPACTO			
NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 27005:2018	La probabilidad hace referencia a la combinación de las consecuencias que se presentarían después de la ocurrencia	La norma plantea que para desarrollar los criterios de impacto se recomienda especificarlos en términos de grado o de los costos para la organización, causados por un evento de seguridad	20%	Bajo	No elegible

NORMA TÉCNICA COLOMBIANA NTS/IEC ISO 31000	Se pueden determinar modelando los resultados de un evento o grupo de eventos a través de la extrapolación a partir de estudios experimentales o datos disponibles	Identificando las tareas que se van a impactarse expresan en tangibles e intangibles	29%	Bajo	No elegible
NIST RIST MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEM AND ORGANIZATION	la metodología no trabaja conforme al atributo	Se realiza una priorización de sistemas organizacionales con el mismo nivel de impacto.	10%	Bajo	No elegible
Octave	La metodología no especifica la manera o la forma en cómo se trabaja, solamente hace definición del atributo	toda la información relevante sobre un riesgo específico para un activo de información se captura en una hoja de trabajo de riesgo de activos de información	10%	Bajo	No elegible

Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas (DAFP)	A través del formato AG. Mapa de riesgos (Ver anexo H) Para que una fuente de información pueda proporcionar datos de inteligencia sobre la probabilidad de que una amenaza se materialice sobre un cierto tipo de activos	La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo y A4.4. Estado de riesgo	50%	Alto	Elegible
Guía para la implementación del principio de responsabilidad demostrada (Accountability)	se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo	la metodología no trabaja conforme al atributo	15%	Baja	No elegible

Magerit	Proporciona un análisis cuantitativo simple del riesgo al introducir el concepto de puntuación de riesgo relativo. Una puntuación de riesgo relativo es un valor derivado de una consideración de una descripción de la probabilidad de riesgo combinada con una priorización del impacto organizacional del riesgo en términos de los criterios de medición de riesgos de la organización. La puntuación se puede utilizar para comparar importancia relativa de los riesgos individuales.	toda la información relevante sobre un riesgo específico para un activo de información se captura en una hoja de trabajo de riesgo de activos de información	29%	Baja	No elegible

Metodología FRAAP	Para iniciar en el proceso de asignación de nivel de riesgo, se usará un ejemplo de umbrales de probabilidad e impacto con una escala simplificada. (El apéndice N de "Information Security Risk Analysis	los responsables de una unidad o dependencia encuentran una afectación en esta, tienden a establecer un nivel de impacto "Alto", pero este nivel se presenta para amenazas que afectan a toda la organización.	29%	Baja	No elegible

Gracias a las tablas anteriores, se debe resaltar que el resultado final es mostrado en la siguiente tabla, permitiendo de esta manera establecer los atributos que se utilizan en la metodología propia, así:

Tabla 3-26. Metodologías elegibles. Fuente: elaboración propia.

Nombre de metodología	Atributos	ESTADO	% DE CUMPLIMIENTO
Magerit	Inventario de activos	Elegible	50%
ISO 27005	Vulnerabilidades	Elegible	50%
Magerit	Amenazas	Elegible	50%
DAFP	Riesgo	Elegible	40%
FRAPP	Controles	Elegible	50%

Gracias a la identificación de los atributos frente a las metodologías analizadas se hizo posible extractar las que mayor manejo le dan a cada uno de los atributos.

3.8. Fase 3. Creación de la metodología propia de análisis de riesgo para una entidad del sector público

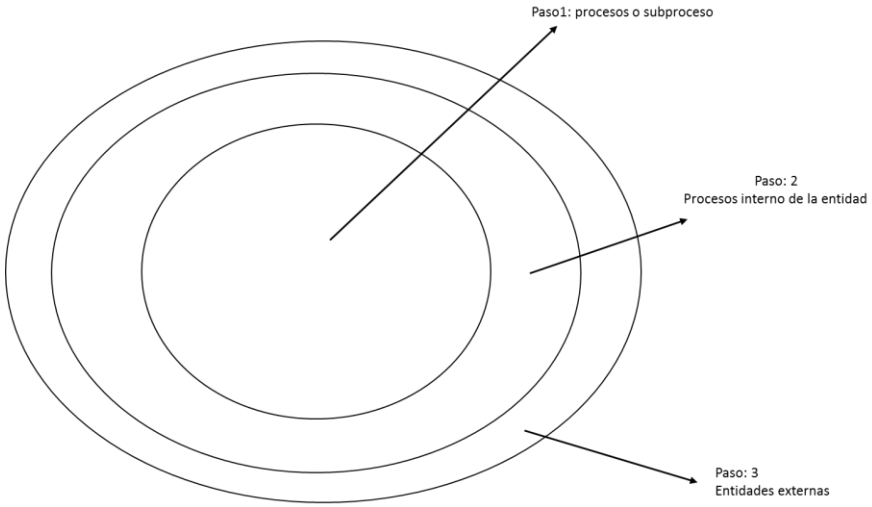
Una vez identificado y detallado los procedimientos metodológicos anteriores se obtuvo como resultado la creación de la metodología propia de análisis de riesgo el cual está conformada por 7 pasos para su ejecución en una entidad del estado quedando de la siguiente manera:

1. Alcance:
2. Inventario de activos
3. Identificación de vulnerabilidades
4. Identificación de amenazas
5. Identificación de riesgo
6. Identificación de controles
7. Manejo de incidentes

Por otra parte, se relaciona a continuación los diferentes formatos a utilizar por cada uno de los atributos que integran la metodología construida.

- **Alcance:** es de anotar que el alcance no trabaja con un formato si no que comprende el nivel que se puede implementar un SGSI, una vez se identifique el mismo se realiza la caracterización de los procesos utilizando el método de las elipses como aparece en la siguiente imagen.

Figura 3-1. Método de elipse. Fuente: Elaboración propia.



- **Inventario de activo:** para trabajar la identificación de inventario se utilizará el siguiente formato:

[info] Activos esenciales: información

Tabla 3-27. [Info] Activos esenciales: información. Fuente: Elaboración propia.

[Info] Información	
Código:	Nombre:
Descripción:	
Propietario:	
Responsable:	
Tipo:	

Valoración de la información, típicamente en las siguientes dimensiones de seguridad:

[I] integridad

[C] confidencialidad

[A] autenticidad de los datos

[T] trazabilidad de los datos, quién ha modificado qué

Tabla 3-28. Activos esenciales - Valoración. Fuente: Modificado de **[9]**.

Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A]		
[T]		

Las dependencias normalmente identifican servicios y personas que manejan esta información:

Tabla 3-29. Dependencias de activos inferiores. Fuente: Modificado de **[9]**.

Dependencias de activos inferiores (hijos)	
activo:	grado:
Dependencias de activos inferiores (hijos)	
¿por qué?:	

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

- **Identificación de vulnerabilidades:** El reporte de vulnerabilidades se realizará conforme al siguiente formato:

Tabla 3-30. Método para la valoración de las vulnerabilidades NTC - ISO/IEC 27005. [19].

METODO PARA LA VALORACION DE LAS VULNERABILIDADES NTC - ISO/IEC 27005		
Tipos	**Vulnerabilidades**	**Amenazas**
Hadware		
Software		
Red		
Personal		
Lugar		
Organización		

- **Identificación de amenazas:** el reporte de amenaza se realizará conforme al siguiente formato:

Tabla 3-31. Identificación de amenazas. [9].

Código [ ] Descripción:	
Tipos de activos:	Dimensiones:
Descripción:	

- **Identificación del riesgo:** la identificación del riesgo se realizará con relación al siguiente formato:

Tabla 3-32. Identificación de Riesgo. Fuente: Elaboración propia.

MATRIZ DE VALORACION DEL RIESGO (DAFF)						
Riesgo	**Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Zona de riesgo**

Extremo	
Alto	
Moderado	
Bajo	

- **Identificación de controles:** el reporte de identificación de controles se realizará con relación al siguiente formato:

Tabla 3-33. Identificación de controles. Fuente: Elaboración propia.

IDENTIFICACION DE CONTROLES (FRAAP)		
Atributo	**Amenaza**	**Controles existentes**
Integridad		
Confidencialidad		
Disponibilidad		

- **Manejo de incidentes:** el reporte de incidentes de seguridad se realiza con base al siguiente formato:

Reporte de incidente de seguridad de la información

GTC-ISO/IEC 27035

Tabla 3-34. Manejo de incidentes Fuente: [20].

1. Fecha del incidente	Página 1 de 2
2. Número del incidente	3. (Si es aplicable) Números de identificación de eventos y/o incidentes relacionados

4. DETALLES DEL MIEMBRO DEL PUNTO DE CONTACTO (PC)		
4.1 Nombre	4.2 Dirección	
4.3 Organización	4.4 Departamento	
4.5 Teléfono	4.6 Correo electrónico	
5. DETALLES DEL MIEMBRO DE ISIRT		
5.1 Nombre	5.2 Dirección	
5.3 Organización	5.4 Departamento	
5.5 Teléfono	5.6 Correo electrónico	
6. DESCRIPCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
6.1 Descripción adicional del incidente:		
7. DETALLES DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
7.1 Fecha y hora en la que ocurrió el incidente		
7.2 Fecha y hora en la que se descubrió el incidente		
7.3 Fecha y hora en la que se reportó el incidente		
7.4 Identificación/detalles de contacto de la persona que hace el reporte		
7.5 ¿Ya finalizó el incidente? *(Marque la respuesta adecuada).*	SÍ	NO
7.6 En caso afirmativo, especifique cuánto duró el incidente en días/horas/minutos		

Tabla 3-35. Manejo de incidentes. Fuente: Fuente: [21].

Página 2 de 2		
8. CONCLUSIÓN		
Mayor ___ Menor ___		
9. INDIVIDUOS INTERNOS/ENTIDADES NOTIFICADAS		
	Líder/funcionario responsable de seguridad de la información __	Líder del ISIRT __
	Gerente del sitio __ (indique qué sitio)	Líder de sistemas de información __
	Originador del reporte __	Líder del originador del reporte/
Otros		

Especifique:		
10. INDIVIDUOS EXTERNOS/ENTIDADES NOTIFICADAS		
	Policía	Otros
Especifique:		
11. FIRMAS		
ORIGINADOR	Revisor	Revisor
Firma digital	Firma digital	Firma digital
Nombre	Nombre	Nombre
Rol	Rol	Rol
Fecha	Fecha	Fecha

3.9. Fase 4: Caso de estudio

3.9.1. Fase 4-1: Socialización de la metodología de gestión de riesgo

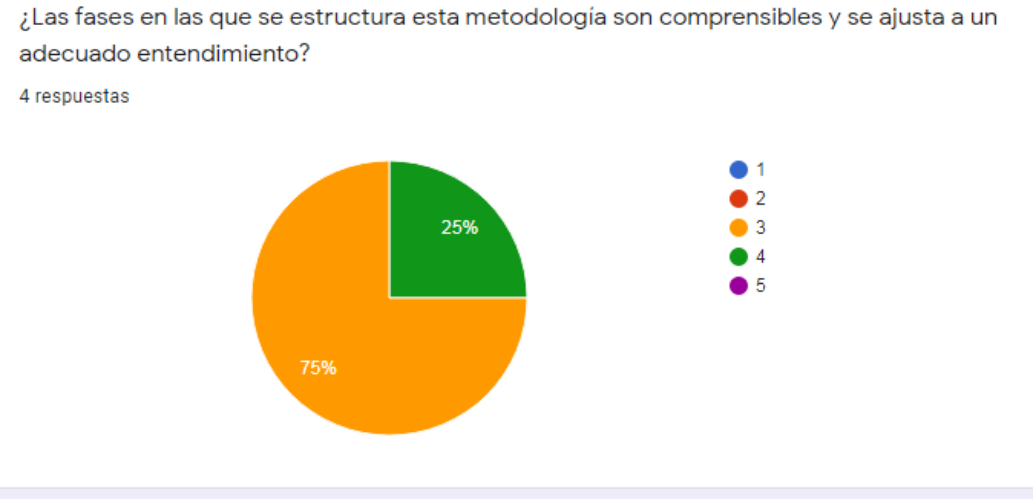
En el marco de la socialización de la metodología creada se obtuvieron los siguientes resultados:

- Los encargados del área TIC de la entidad del estado conocieron el proceso metodológico para aplicar la metodología en su entidad.
- Los encargados de are TIC conocieron los diferentes formatos y la manera como se deben diligenciar.
- Los encargados del ares TIC conocieron como se realiza un análisis de riesgo conforme a la metodología creada.
- Los encargados del área TIC cocieron la importancia de contar con SGSI en su entidad para mitigar los riesgos.

3.9.2. Fase 4-2: Diseño de satisfacción con base en el funcionamiento de la metodología

Una vez aplicada la encuesta de satisfacción a los diferentes funcionarios que elaboran en el área TIC de la entidad del estado se obtuvieron los diferentes resultados conforme a las preguntas consignadas en el formulario:

Figura 3-2. Pregunta 1. Fuente: Elaboración propia.

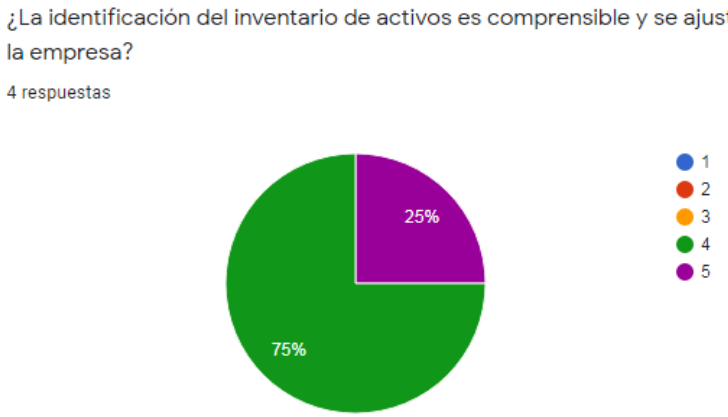


El 75% manifiesta que las fases que está estructurada la metodología es aceptable mientras que el 25% considera que tiene una estructura buena.

Figura 3-3. Pregunta 2. Fuente: Elaboración propia.

El cien por ciento de los encuestados dio una valoración de cuatro a esta respuesta, concluyendo de esta manera que las elipses que se consagran dentro de esta metodología se consideran propia para identificar el alcance del SGSI.

Figura 3-4. Pregunta 3. Fuente: Elaboración propia.



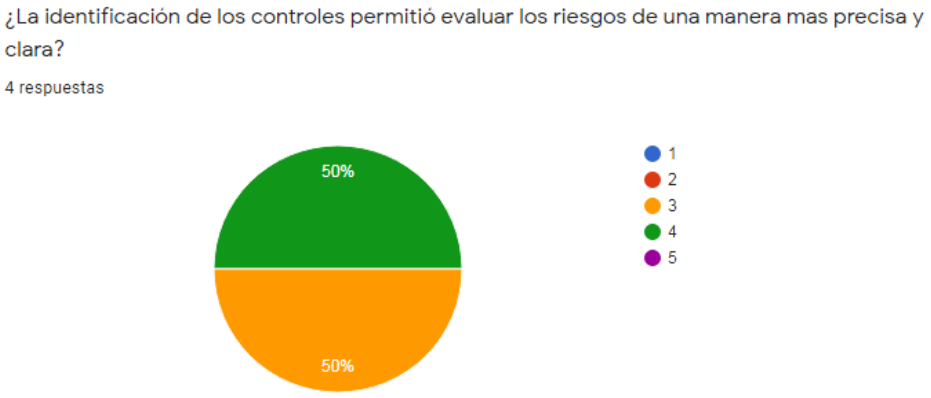
Gracias a esta respuesta es factible concluir que el 75% de los encuestados califican de manera satisfactoria la metodología con relación al inventario de activos, por cuanto

afirman que este apartado permite la identificación y se ajusta a las necesidades de la empresa.

Figura 3-5. Pregunta 4. Fuente: Elaboración propia.

el 75% de los encuestados manifiestan que las identificaciones de amenazas a través de los códigos son comprensibles y de fácil manejo mientras que el 25% manifiesta que tiene una excelente manera de identificar las amenazas.

Figura 3-6. Pregunta 5. Fuente: Elaboración propia.



Esta respuesta se encontró dividida, obteniendo niveles de calificación 3 y 4, lo que permite identificar que es aceptable la manera cómo evalúa los controles la metodología.

Figura 3-7. Pregunta 6. Fuente: Elaboración propia.

En este caso fue dividida la respuesta, el 75% de los encuestados calificaron en el nivel de medición 3, mientras que el 25% afirma que esta etapa permite la consolidación de los riesgos de manera completa

3.9.3. Fase 4-3: Aplicación de la metodología propuesta

Una vez creada la metodología de análisis de riesgo para una entidad del estado se puso en marcha su aplicación por parte de un funcionario de la misma, es de aclarar que los procesos realizados desde el inventario de activo hasta el manejo de incidente, él lo desarrolló conforme a un activo realizando los procesos de la estructura de la metodología obteniendo los siguientes resultados:

3.9.3.1. Alcance

Basados en el mapa de procesos de la organización el funcionario de la entidad pública pudo identificar las diferentes áreas que conforman la entidad, hasta llegar al área objeto de estudio, que para este caso fue la dependencia de las TIC, donde aplico el método de la siguiente forma:

Paso 1: Como resultado de este paso el funcionario identificó los servicios que hacen parte de los procesos y subprocesos del área de TIC para poderlo ubicar en la elipse más interna.

Servicio de administración de base de datos

- Base de datos video admón.
- Base de datos SQL versión 11
- Sistema operativo del servidor

Servicio de internet corporativo

- Media comer-internet
- Router media comer
- App wikili

Paso 2. El resultado que obtuvo el funcionario en la elipse intermedia fue los procesos interno propio de la entidad los cuales se interactúa constantemente, este lo realizó a través de las diferentes dependencias cuyos activos son administrados por el área TIC siendo los siguientes:

Sede Principal la Confianza

- Oficina Tic

Sede Principal Salud

- Oficina Tic sede tercer piso

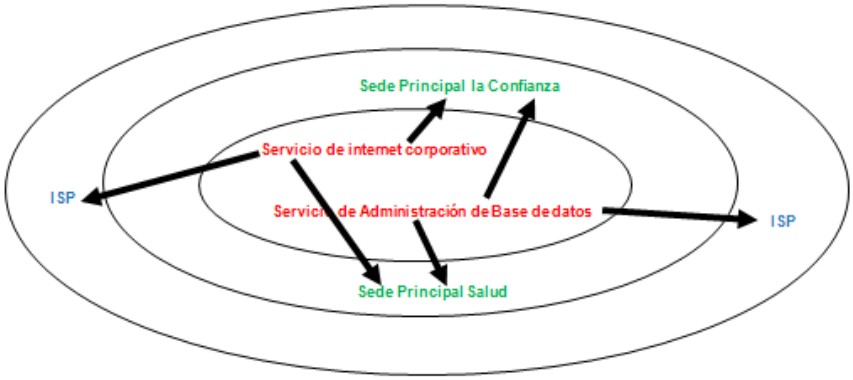
Paso 3. El funcionario de la entidad del estado aplico este paso consiguiendo la elipse más externa cuyo resultado fue el siguiente:

- ISP Proveedor de Servicios de Internet

El funcionario de la entidad del estado después de conseguir estos resultados genero las elipses de procesos y servicio como se muestra a continuación:

Tabla 3-36 Elipses gestión de riesgo

Figura 3-8. proceso de las elipses. Fuente: elaboración propia.



3.10. Inventario de activos

el resultado obtenido conforme a este atributo por parte del funcionario de la entidad del estado es que realizo la descripción de un activo tipo software.

3.10.1. [SW] Aplicaciones (software)

Tabla 3-37 SW Aplicaciones (software).

[SW] Aplicaciones (software)	
código: 001	nombre: WINBOX
descripción: software para revisar el estado de las mikrotic	
responsable: Yosimar Palacios Romaña	
Tipo: Servidor de terminales	

Las dependencias normalmente identifican personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.

Tabla 3-38. Dependencias de activos inferiores (hijos).

Dependencias de activos inferiores (hijos)	
activo: Administrador	grado: 1
¿por qué?:	

Tabla 3-39. Inventario de activos. Fuente: elaboración propia.

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

3.11. Identificación de Vulnerabilidad

Con relación a la vulnerabilidad el funcionario le realizó una valoración al activo que identifico en el proceso anterior donde pudo encontrar que dicho activo de software tiene una vulnerabilidad que puede ser explotada más a delante si no se toman medidas urgentes.

Tabla 3-40. Método para la valoración de las vulnerabilidades NTC - ISO / 1BC 27005. [6]

METODO PARA LA VALORACION DE LAS VULNERABILIDADES NTC - ISO/IEC 27005		
Tipos	**Vulnerabilidades**	**Amenazas**
Hadware	No aplica para este activo	No aplica para este activo
Software	Configuracion incorrecta de parametrsos	Error en el Uso
Red	No aplica para este activo	No aplica para este activo
Personal	No aplica para este activo	No aplica para este activo
Lugar	No aplica para este activo	No aplica para este activo
Organización	No aplica para este activo	No aplica para este activo

3.12. Identificación de amenaza

El funcionario de la entidad del estado luego de realizar el proceso diligenciamiento de la amenaza conforme al activo obtiene el siguiente resultado donde se deja entrever que la amenaza afectada la disponibilidad del activo.

Tabla 3-41. Reporte de amenaza. Fuente: elaboración propia.

Código [1.5] Descripción: Avería de origen físico o lógico

Tipos de activos: Software	Dimensiones: **1.** [D]disponibilidad
Descripción: Problemas de configuración de los equipos que están bajo la administración de este software donde se quedan sin prestar el servicio a la demás dependencia que necesitan del internet.	

3.13. Identificación del Riesgo

Con forme al riego el funcionario de la entidad del estado realiza el proceso de diligenciamiento del formato obteniendo el siguiente resultado donde deja en evidencia que el activo presenta un riesgo extremo lo cual indica que se debe tomar medidas urgentes ante que se puede materializar esta amenaza.

Tabla 3-42. Matriz de valoración de riesgo. Fuente: Elaboración propia.

MATRIZ DE VALORACION DEL RIESGO (DAFF)						
Riesgo	**Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Zona de riesgo**
Perdida de la disponibilidad	Software Winbox	Averia de origen físico o lógico	Configuaracion incorecta de parametros	4-Probable	4-Mayor	Extrema

Extremo	
Alto	
Moderado	
Bajo	

3.14. Identificación de Control

Una vez diligenciado este formato por parte del funcionario de la entidad del estado se obtiene como resultado que el activo contiene una amenaza y para esto no han aplicado medidas de control

Tabla 3-43. Identificación de controles (FRAAP). Fuente: Elaboración propia.

IDENTIFICACION DE CONTROLES (FRAAP)		
Atributo	**Amenaza**	**Controles existentes**
Integridad	No aplica	No aplica
Confidencialidad	No aplica	No aplica
Disponibilidad	Avería de origen físico o lógico	El activo de software no tiene ningun control aplicado para su seguridad y funcionalidad del mismo

3.15. Manejo de incidentes

Frente al manejo de incidentes el funcionario de la entidad del estado simula un caso de incidente donde consigna toda la información a la que solicita el formato, una vez realiza todo el diligenciamiento obtiene como resultado que la información se relaciona de una manera que le permite tener reportes de incidentes que hallan sucedido en la entidad para sí tomar medidas que le permita mitigar estos eventos a futuro

Reporte de incidente de seguridad de la información

GTC-ISO/IEC 27035

Tabla 3-44. Reporte de incidentes. Fuente: Elaboración propia.

1. Fecha del incidente: 5/12/2020	Página 1 de 2
2. Número del incidente: 01	3. (Si es aplicable) Números de identificación de eventos y/o incidentes relacionados: para este caso no es aplicable
4. DETALLES DEL MIEMBRO DEL PUNTO DE CONTACTO (PC)	
4.1 Nombre: yosimar palacios romaña	**4.2 Dirección:** cra 20 nro 30-15 B/ margarita
4.3 Organización: Área Tic	4.4 Departamento: Chocó
4.5 Teléfono: 67465806	**4.6 Correo electrónico:** yisimarpalcios@hotmail.com
5. DETALLES DEL MIEMBRO DE ISIRT	
5.1 Nombre: Harlen Ibarguen	**5.2 Dirección:** cra 20 nro 13-20
5.3 Organización: Área Tic	5.4 Departamento: Chocó
5.5 Teléfono	5.6 Correo electrónico
6. DESCRIPCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
6.1 Descripción adicional del incidente: **Qué ocurrió:** El servidor de bases de datos de contabilidad dejo de funcionar Cómo ocurrió: se abrió una aplicación que no era compatible con el sistema Por qué ocurrió: se descargó una aplicación no autorizada	

Consideraciones iniciales sobre componentes/activos afectados: el software financiero del área de contabilidad Cualquier vulnerabilidad identificada: no existe control de acceso		
7. DETALLES DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
7.1 Fecha y hora en la que ocurrió el incidente: 5/12/2020 hora 10:00am		
7.2 Fecha y hora en la que se descubrió el incidente: 5/12/2020 hora 10:10am		
7.3 Fecha y hora en la que se reportó el incidente: 5/12/2020 hora: 11:00am		
7.4 Identificación/detalles de contacto de la persona que hace el reporte: C.C. 12.050.354 Cel 3158305040		
7.5 ¿Ya finalizó el incidente? *(Marque la respuesta adecuada).*	SÍ X	NO
7.6 En caso afirmativo, especifique cuánto duró el incidente en días/horas/ minutos: 2 minutos		

Tabla 3-45. Reportes de incidente - 2. Fuente elaboración propia.

Página 2 de 2
8. CONCLUSIÓN
Se debe tener mecanismos de protección para la infraestructura de red de la organización con el objetivo de minimizar los riesgos que pueden afectar a los activos con los que se cuenta y generan procesos productiva para la misma Mayor _X__ Menor ___
9. INDIVIDUOS INTERNOS/ENTIDADES NOTIFICADAS

Ninguna por el momento	Líder: Yosimar palacios romaña	Líder del ISIRT: Harlen Ibarguen
	Gerente del sitio __	Líder de sistemas de información __
	Originador del reporte: yosimar palacios romaña	Líder del originador del reporte: contabilidad
Otros Ninguno		
Especifique: Ninguno		
10. INDIVIDUOS EXTERNOS/ENTIDADES NOTIFICADAS		
Ninguna	Policía	Otros
Especifique:		

11. FIRMAS: Yosimar Palacios Romaña		
ORIGINADOR	Revisor	Revisor
Firma digital	Firma digital	Firma digital
Nombre	Nombre	Nombre
Rol	Rol	Rol
Fecha	Fecha	Fecha

Una vez aplicada la metodología de análisis de riesgo por parte de un funcionario de la entidad del estado se obtuvo como resultado la identificación del riesgo que ocasiona no contar con un SGSI que le permita mitigar oportunamente los problemas de seguridad en los activos.

4. Capítulo IV - Conclusiones y Recomendaciones

- Este trabajo investigativo contiene un diseño de un sistema de gestión de seguridad de la información con base en la gestión de riesgos y el manejo de incidentes, ajustado a las necesidades de una empresa del sector público de la ciudad de Quibdó, el cual se inició con una análisis del estado del arte de los diseños de sistemas de gestión de seguridad de la información, analizando la manera como la es empresas del sector público han abordado el diseño e implementación del mismo al interior de sus organizaciones, dicha información sirvió de gran utilidad para el cumplimiento de los objetivos propuestos. Igualmente se pudo identificar en cada uno de los trabajos revisados su alcance con relación al sistema de gestión de seguridad de la información (SGSI).
- Teniendo en cuenta las consideraciones anteriores, en la investigación se desarrolló una metodología compuesta por cuatro fases, orientadas al cumplimento de los cuatros objetivos de la misma, iniciando con el diagnostico empresarial, continuando con la identificación de las diferentes metodologías para la determinación del riesgo tecnológico, luego con la metodología de control de riesgo de la información que facilite la clasificación, control y manejo de incidentes y por último se hizo el estudio de caso.
- **El diagnóstico empresarial**, se de desarrollo en una entidad del sector público de la ciudad de Quibdó, dicho procedimiento permitió identificar la manejar como se ejercen procedimientos de seguridad informática, igualmente se identificaron los activos de información existentes en el área TIC de la empresa, y al mismo tiempo valorar los tipos de controles que tienen aplicados a los activos de la misma**. Identificación de las diferentes metodologías para la determinación del riesgo**

tecnológico, estas fueron identificadas mediante la selección de 8 metodologías de análisis de riesgo, siendo estas las más utilizadas en este sentido, igualmente se hicieron valoraciones considerando unos atributos para identificar su pertinencia conforme a los seleccionados, posteriormente se hizo una valoración para determinar de qué metodología saldría los atributos para conformar la creación de la metodología propuesta en la tercera fase, seguidamente con los atributos seleccionados se crea **la metodología de control de riesgo de la información que facilite la clasificación, control y manejo de incidentes,** mediante 7 pasos (Alcance, Inventario de activos, Identificación de vulnerabilidades, Identificación de amenazas, Identificación de riesgo, Identificación de controles y Manejo de incidentes), logrando identificar los formatos a utilizar por cada uno de los atributos que conforman la metodología creada, luego de haber creado la metodología se puso a prueba la misma a través de un **Estudio de casos,** logrando socializarla a los funcionarios del are TIC de la empresa del sector público, igualmente se identificó el nivel de satisfacción utilizando una encuesta y por último se logró que un funcionario la aplicar en la empresa, obteniendo como resultado un sistema de gestión de seguridad de la información (SGSI) que oportunamente mitigue los problemas de seguridad en los activos de información.

- Teniendo en cuenta que el diseño del sistema de gestión de seguridad de la información con base en la gestión de riesgos y el manejo de incidentes, ajustado a las necesidades de una empresa del sector público de la ciudad de Quibdó, es flexible, para trabajo futuro se pueden tener en cuenta más metodologías de análisis de riesgo a estudiar que posibiliten mayores alternativas de selección de los atributos, teniendo en cuenta las particularidades y necesidades de cada organización. Igualmente se recomienda desarrollar una herramienta de software que tenga como línea base la metodología creada en este trabajo.

5. Bibliografía

[1] N.-I. ICONTEC, «TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS,» Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237 Bogotá, D.C., 2006. [En línea]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

[2] MINTIC, «Ministerio de Tecnologías de la Información y las Comunicaciones,» 10 06 2018. [En línea]. Available: https://www.mintic.gov.co/portal/604/w3-article-14081.html.

[3] Significados.com, «Marco teórico,» Significados.com, 20 Enero 2021. [En línea]. Available: https://www.significados.com/marco-teorico/. [Último acceso: 16 Febrero 2021].

[4] F. Coelho, «www.significados.com,» 6 6 2019. [En línea]. Available: https://www.significados.com/metodologia/.

[5] Superintendencia de Industria y Comercio, «Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability),» SIC, 2014. [En línea]. Available: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf. [Último acceso: 16 Febrero 2021].

[6] NORMA TÉCNICA COLOMBIANA NTC- ISO/ IEC 27001, «NORMA TÉCNICA COLOMBIANA NTC- ISO/ IEC 27001,» Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI, 01 08 2018. [En línea].

Available: http://www.iso27000.es/certificacion.html#seccion4. [Último acceso: 16 02 2021].

[7] S. Adirha, «THE FACILITATED RISK ANALYSIS AND ASSESSMENT (FRAAP),» BINUS University, 26 Julio 2018. [En línea]. Available: https://student-activity.binus.ac.id/isgbinus/2018/07/the-facilitated-risk-analysis-and-assessment-fraap/#:~:text=The%20Facilitated%20Risk%20Analysis%20and%20Assessment%20(FRAAP)%20was%20developed%20as,operations%20are%20considered%20and%20documented.&tex. [Último acceso: 16 02 2021].

[8] M. Hurtado, «GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT,» Universidad Piloto de Colombia, 2018. [En línea]. Available: http://polux.unipiloto.edu.co:8080/00004420.pdf. [Último acceso: 16 02 2021].

[9] 0. MAGERIT versión3, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.,» Ministerio de Hacienda y Administraciones Públicas. NIPO: 630-12-171-8, Octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 16 02 2021].

[10] NTC-ISO31000, «La norma en Gestión de Riesgos ISO 31000 y sus beneficios,» 26 08 2016. [En línea]. Available: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf. [Último acceso: 16 02 2021].

[11] N. -. N. I. O. S. A. TECHNOLOGY, «NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST. Special Publication 800-37,» NIST Releases Version 1.1 of its Popular Cybersecurity Framework. GAITHERSBURG, Md, 15 8 2018. [En línea].

Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Último acceso: 16 02 2021].

[12] A. Ibrahim, C. Valli, A. I McAteer y J. Chaudhry, «A security review of local government using NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,» Springer Science, 16, 2018.

[13] F. Guardia, «Diseño de un sistema de gestión de seguridad de la información ajustada a las necesidades de la corporación medica Clínica Vida de Quibdó,» Medellín, Colombia, 2017.

[14] J. E. Eterovic y G. A. Pagliari, «Metodología de Análisis de Riesgos Informáticos,» Técnica Administrativa. ISSN 1666-1680 Vol.10. Buenos Aires, Argentina, 03 01 2011. [En línea]. Available: http://www.cyta.com.ar/ta1001/v10n1a3.htm. [Último acceso: 16 02 2021].

[15] S. ,. A. GUZMAN, «DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO,» medellín, 2015.

[16] B. Béatrix y A. L. Mesquida, «Integrating Risk Management in IT settings from ISO,» *elsevier,* p. 26, 2016.

[17] Incibe, 20 03 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[18] F. Guardia, «repositorio UPB,» 20 03 2017. [En línea]. Available: https://repository.upb.edu.co/handle/20.500.11912/3567?locale-attribute=en.

[19] NIT-ISO/IEC27005, «Norma tecnica NIT-ISO/IEC27005 colombiana,» bogota, 2009.

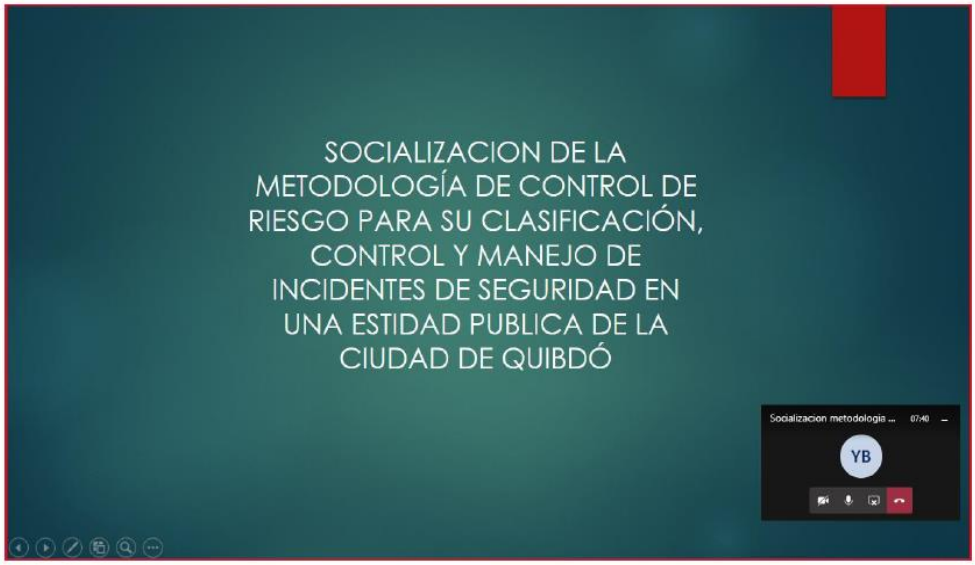
[20] ISO27000, «ISO 27000.es,» 1 9 2018. [En línea]. Available: http://www.iso27000.es/sgsi.html.

[21] ISO, «ISO,» 26 10 2018. [En línea]. Available: https://www.iso.org/iso-31000-risk-management.html.

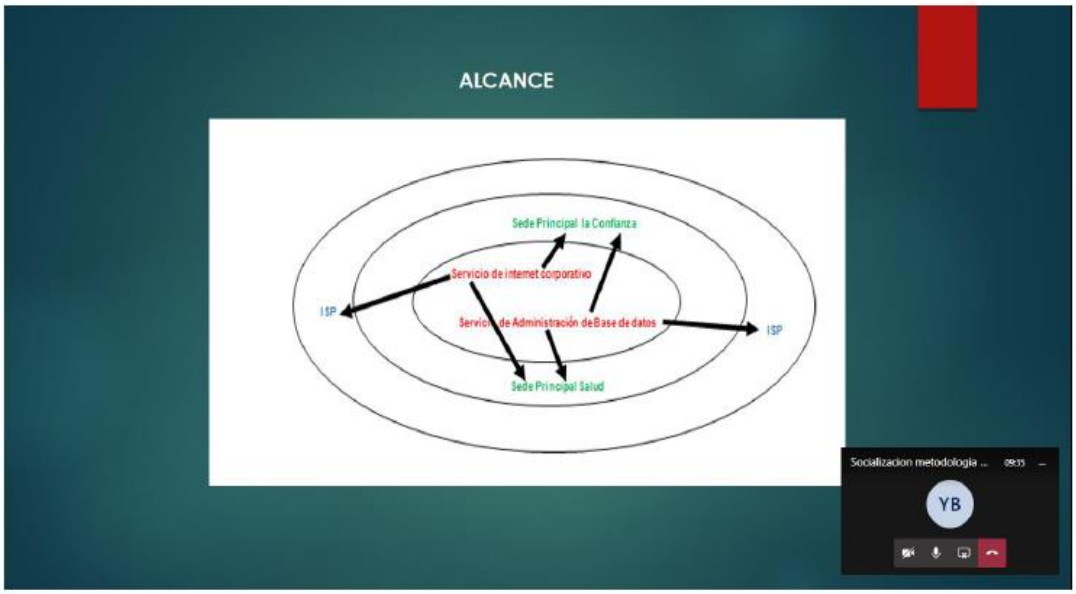
6. Anexos

A. Anexo A: Socialización de la metodología propia

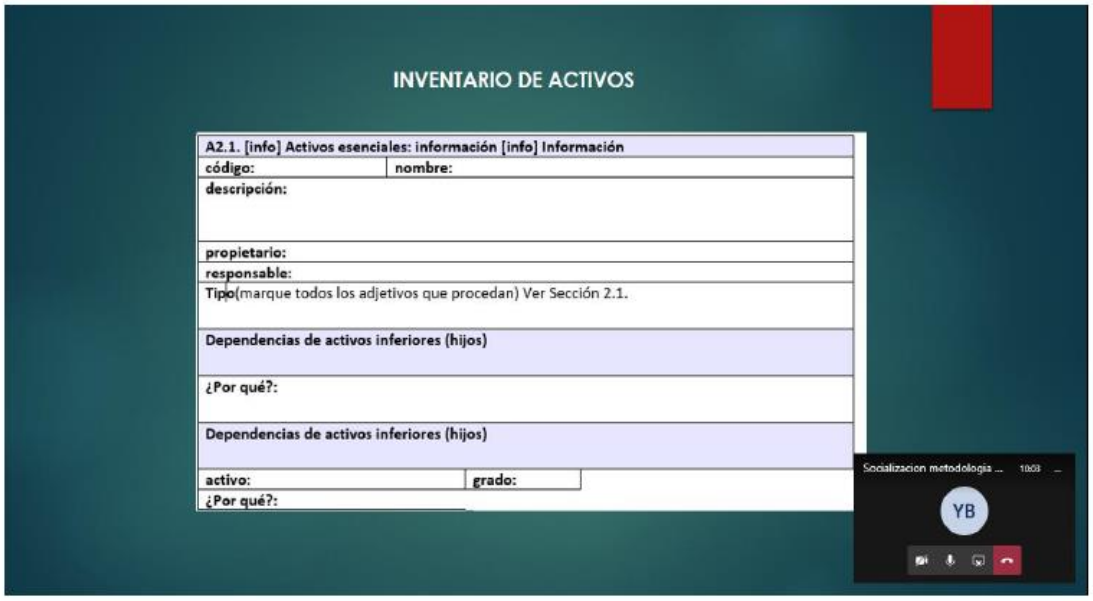
Las siguientes imágenes son la evidencia de los diferentes formatos socializados a las diferentes personas que conforman el área Tic de la entidad del sector público el cual se le socializo la metodología.



B. Anexo 1 Socialización elipses

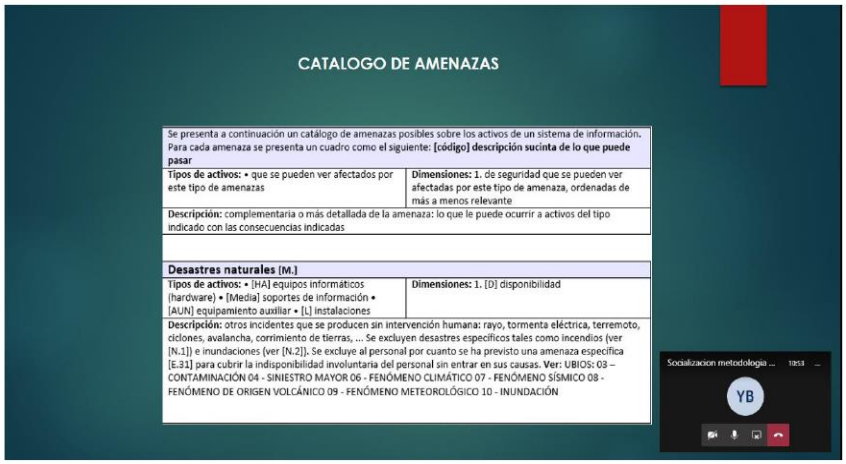


C.Anexo 2 Socialización inventario de activos

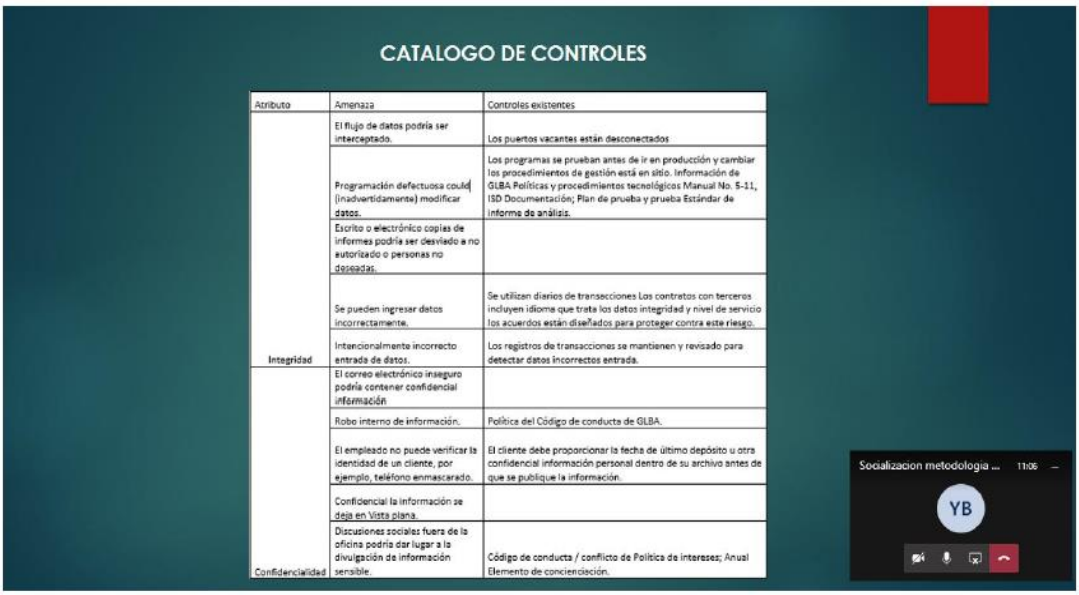


D. Anexo 3 Socialización de vulnerabilidades

E. Anexo 4 Socialización catálogo de amenazas



F. Anexo 5 Socialización de catálogo de controles



G. Anexo 6 Socialización de catálogo de riesgos