# IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001 DE 2013 EN LA CORPORACIÓN NASA KIWE

**ANDREA ESPERANZA TOVAR LEÓN**

**CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA**
**FACULTAD INGENIERÍAS**
**PROGRAMA INGENIERÍA DE SISTEMAS INFORMÁTICOS**
**POPAYÁN, CAUCA**
**2019**

# IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001 DE 2013 EN LA CORPORACIÓN NASA KIWE


**ANDREA ESPERANZA TOVAR LEÓN**

**Trabajo de Grado para optar al título de Ingeniera de Sistemas Informáticos**

**Director**

**Msc. Julio Andrés Mosquera**

**CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA**

**FACULTAD INGENIERÍAS**

**PROGRAMA INGENIERÍA DE SISTEMAS INFORMÁTICOS**

**POPAYÁN, CAUCA**

**2019**

NOTA DE ACEPTACIÓN

El director y los jurados del trabajo de grado: IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001 DE 2013 EN LA CORPORACIÓN NASA KIWE, elaborado por la estudiante Andrea E. Tovar León bajo la modalidad práctica profesional, una vez terminado el documento de informe final y aprobada la sustentación del mismo, autorizan la continuidad del proceso administrativo para optar al título de Profesional en Ingeniería de Sistemas Informáticos de la Corporación Universitaria Autónoma del Cauca.

_____

Director: Julio A. Mosquera Bolaños

_____

Jurado: Juan Pablo Diago Rodríguez

_____

Jurado: Santiago Sánchez Ferreira

Popayán, 19 de julio de 2019

DEDICATORIA

Este trabajo está dedicado primero a Dios por el don de vida y perseverancia para culminarlo, a mis padres por su esfuerzo, confianza y apoyo brindado, el cual fue fuente de inspiración para finalizar mi carrera profesional. A mi hermana que estuvo presente en esta etapa tan importante de mi vida.

# AGRADECIMIENTOS

Agradezco la realización de este proyecto a Dios por haberme dado la oportunidad de lograr los objetivos propuestos y superar con orgullo todos los obstáculos al realizarlo.

Dedicarles a mis padres (Oliva León y Eliecer Tovar), hermana (Marcela Tovar) y César A. Flórez por su apoyo continuo y creer siempre en mis capacidades.

A la Corporación Universitaria Autónoma del Cauca y los docentes, que con su experiencia y dedicación me hicieron crecer tanto en lo profesional como personal.

A la Corporación Nasa Kiwe, la doctora Marcela Zambrano, el ingeniero Alveiro Vásquez y demás funcionarios que de una u otra manera permitieron desde sus labores la ejecución de la práctica profesional.

A los jurados y director de trabajo por sus concejos y asesoría durante esta fase final de mi trabajo de grado.

# CONTENIDO

PÁG.

## LISTA DE ILUSTRACIONES



## LISTA DE TABLAS

# RESUMEN

De acuerdo a las nuevas exigencias sobre la correcta manipulación de los datos, las entidades públicas requieren gestionar adecuadamente la seguridad de la información en cada una de sus dependencias. Sin embargo, el desconocimiento en este campo por parte de los funcionarios ha ocasionado que el desarrollo de buenas prácticas de seguridad no se lleven a cabo según las medidas dirigidas desde la oficina de sistemas en la Corporación Nasa Kiwe de acuerdo al cumplimiento de su misión institucional[1]. La entidad cuenta parcialmente con algunas medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información pero no posee un modelo de seguridad definido, con procedimientos claros, políticas actualizadas y procesos identificados, por lo que es difícil medir el nivel de cumplimiento de los controles de seguridad que tiene implementados, lo que dificulta la identificación y gestión de los riesgos asociados a la seguridad y privacidad de sus activos de información y las amenazas presentes durante su manipulación. Durante el desarrollo de este trabajo se estructuró y diseñó un modelo de gestión de seguridad de la información utilizando como referente las normas ISO/IEC 27001 y 27002:2013 que permitió estructurar una base de procedimientos y políticas obteniendo un documento adaptado a las necesidades de la entidad y a la normativa a la cual está sujeta de tal manera que pueda a futuro ser implementado.

**Palabras clave:** seguridad de información, privacidad, ISO/IEC 27001, modelo de seguridad.

## *ABSTRACT*

According to the new demands on the correct manipulation of data, public entities require to adequately manage the security of information in each of their dependencies. However, the lack of knowledge in this field by officials has caused that the development of good security practices are not carried out according to the measures directed from the systems office in the Nasa Kiwe Corporation according to the fulfillment of its institutional mission [1]. The entity partially has some measures aimed at protecting the confidentiality, integrity and availability of information but does not have a defined security model, with clear procedures, updated policies and identified processes, making it difficult to measure the level of compliance with the security controls that it has implemented, which makes it difficult to identify and manage the risks associated with the security and privacy of its information assets and the threats present during its manipulation. During the development of this work, an information security management model was structured and designed, using the ISO / IEC 27001 and 27002: 2013 standards as a reference, which allowed structuring a base of procedures and policies, obtaining a document adapted to the needs of the entity and the regulations to which it is subject in such a way that it can be implemented in the future.


***Keys words:*** information security, privacy, ISO/IEC 27001, security model.

# INTRODUCCIÓN

Hoy en día el mundo gira entorno a los constantes avances tecnológicos y la era digital, por lo que la información se ha convertido en uno de los activos más valiosos para cualquier organización [2], que administrada de manera responsable e integra se convierte en la base para la toma de decisiones y la óptima ejecución de las operaciones.

El tráfico de información ya sea publica o confidencial es un reto para todas las organizaciones, las cuales tienen el compromiso de dar manejo y protección a la información sensible ante posibles manipulaciones malintencionadas, en este sentido las entidades tanto públicas como privadas deben ser garantes de su confidencialidad, integridad y disponibilidad [3], dando cumplimiento a la normatividad colombiana y según, Ley 1581 donde se establecen las disposiciones que garantizan la protección de los datos personales y la Ley 1712 que regula el derecho de acceso a la información pública, entre otras. .

El robo, manipulación o fuga de información puede conllevar a perdidas económicas, sanciones legales que afecten la imagen y el buen nombre de una organización y su funcionamiento. Adicionalmente, es importante contemplar los requerimientos tecnológicos con los que deben contar las organizaciones y la necesidad de vincular personal capacitado, preparado para realizar un diagnóstico e implementar un plan de seguridad y privacidad que garantice la estabilidad de los recursos tecnológicos con los que se cuenta.

Partiendo de la necesidad de cumplimiento hacia la normatividad vigente en Colombia[4][5], entre otras, las entidades públicas están en la obligación de garantizar la seguridad de la información operacional y de sus usuarios, por lo que se requiere la implementación de un modelo de seguridad y privacidad de la información, que brinde confianza y protección de activos mediante la adaptación

de métricas, estándares y procedimientos que se acojan a las necesidades de cada organización.

En el presente trabajo se desarrolla el diseño y plan de adaptación de un modelo de gestión de seguridad de la información para la Corporación Nasa Kiwe (CNK) con sede principal en Popayán y replicable a sus demás dependencias nacionales. También se da un panorama general de la situación actual de la Corporación, su función, procesos, activos de información y los servicios que se brinda al público; además, una revisión de la documentación vigente que respalda el estado actual de los servicios tecnológicos y procedimientos, entendiendo así el contexto de las tareas a desarrollar mediante un proceso de investigación documental y revisión bibliográfica, teniendo en cuenta el marco de referencia de la norma ISO/IEC 27001:2013.

# CAPÍTULO I: PROBLEMA

## 1.1 ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN EN CNK

Durante las tareas de revisión y valoración de la documentación existente, se pudo evidenciar la situación actual de los procesos que se llevan a cabo en la Corporación. La infraestructura tanto tecnológica como organizacional evidenció algunas vulnerabilidades: desactualización en procedimientos, formatos y manuales establecidos como soporte para la realización de las actividades a desarrollar desde el proceso de gestión de la Informática, bajo uso de dichos formatos y cabe mencionar que se encontraron documentos actualizados, pero no divulgados por lo que expone una descentralización de los activos.

Implementar un modelo o sistema de gestión de seguridad tiene como objeto principal el resguardo de la información y de los activos que soportan el funcionamiento de la organización [6], [7], en el caso de la corporación, existe una gran cantidad de información tanto digital física que nunca se ha clasificado, los activos registrados corresponden a unos pocos procesos dentro de la entidad y se encuentran definidos de manera general en versiones documentales desactualizadas.

Durante gran parte del tiempo de existencia de la Corporación, la oficina de gestión de la informática ha estado a cargo del líder del proceso para el desarrollo de todas las actividades y los múltiples requerimientos tanto de logística como del gobierno. Fue necesario incluir la participación de contratistas y pasantes como apoyo a las labores y responsabilidades relacionadas con este importante proceso de gestión, empezando en el segundo semestre del año 2018 con el levantamiento de activos de información y requerimientos legales, se observó la imperiosa necesidad de establecer un modelo de acuerdo a las políticas de seguridad y privacidad de la información que deben cumplir las entidades públicas.

Por lo anterior, la Corporación estableció un plan de acción vigencia 2016-2018 para la implementación de la estrategia Gobierno en Línea hoy Gobierno Digital, donde se definen proyectos y actividades que se alinean para darle valor a los procedimientos ejecutados en la entidad; sin embargo, durante las tareas de revisión documental realizadas se encontró que cumplido el plazo para su adaptación no se encuentran aún definidos y estandarizados controles de seguridad de la información, algunos están documentados mas no implementados, por ejemplo: la entidad no tiene definidas las actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad; los riesgos son cambiantes y la guía de identificación de riesgos se encuentra desactualizada.

Para entender la problemática se realizó de manera colaborativa un análisis del estado actual de la entidad y la oficina de gestión de la informática donde se detectó el factor económico como un limitante ante el desarrollo de algunas actividades. Es importante aclarar que la entidad a la fecha de ejecución de este trabajo no ha gestionado la vinculación de un experto en seguridad informática como apoyo en las actividades de verificación y validación de cumplimiento de los controles y la correcta ejecución de los procedimientos por parte de los funcionarios, lo que permitiría tener mejores resultados ante una posible auditoria, además, durante el análisis del problema se detectaron falencias en la especificación de software y licencias vigentes.

El proceso de gestión de la informática y la conectividad tiene por objetivo proveer y administrar los recursos tecnológicos, es considerado como uno de los procesos fundamentales para garantizar la integridad, confidencialidad y disponibilidad de la información de la entidad [8]. Este proceso desarrolla actividades propias de seguridad informática, pero la falta de supervisión de un experto, de preferencia externo a la entidad podría generar un riesgo debido a la falta de separación de funciones dentro de la ejecución y supervisión de tareas. Para reducir este impacto ante posibles vulnerabilidades la oficina de gestión de la informática

realiza anualmente capacitaciones a los funcionarios con el objetivo de aminorar fallas humanas, más sin embargo, dichas capacitaciones son orientadas al uso de aplicativos y no se realizan de manera periódica como instrumento de información y prevención ante posibles amenazas informáticas, para la implementación de buenas prácticas de seguridad o como medio de divulgación de políticas de obligatorio cumplimiento.

### 1.1.1 DIAGNOSTICO SITUACIÓN PROBLEMA

A partir del análisis del estado de la seguridad con la que cuenta actualmente la Corporación y las posibles vulnerabilidades o situaciones que afecten la integridad, confidencialidad y disponibilidad de la información, la situación problema se ve representada en la Ilustración 1:

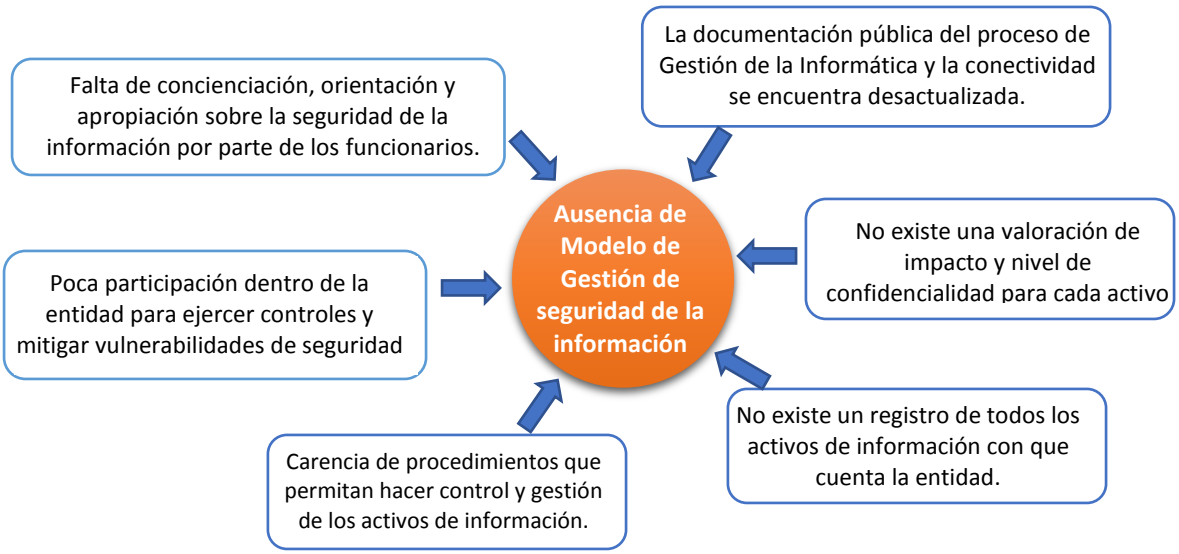


Ilustración 1. Situación problema. Fuente propia

## 1.2 PLANTEAMIENTO DEL PROBLEMA

Actualmente la información representa uno de los activos más valiosos, por lo que cada día más organizaciones apoyan sus procesos con el uso de tecnologías de la información y las comunicaciones [2][9], considerando principalmente los beneficios que trae la adaptación de recursos físicos para la gestión dejando de lado y rezagados los mecanismos de control, implementación y seguimiento de la seguridad de la información, en muchos casos la utilización de sistemas de seguridad no son suficientes cuando estos no se mantienen actualizados o se encuentran de manera parcial[10][11]. Las fallas y vulnerabilidades dentro de ellos son tan comunes como el surgimiento de nuevas tecnologías, por lo que cada día hay miles de personas y organizaciones dedicadas a aprovechar las falencias a través de la red[12][13].

Es común escuchar sobre ataques, secuestro de información, fallas en los sistemas o colapso en los servicios de los cuales ni los grandes tecnológicos como Google, HBO (*Home Box Office*, canal de televisión), PS(*PlayStation*) o las agencias de seguridad gubernamentales se han salvado[14][15][16]. Por ejemplo, recientemente en Estados Unidos la Agencia Nacional de Seguridad (*NSA*) reportó una falla que comprometió la seguridad de la información de sus ciudadanos, colocando en riesgo su privacidad, debido a "numerosos casos de incumplimiento de las normas y a las regulaciones diseñadas para proteger las redes informáticas, los sistemas y la información" [17].

Bajo el interés de gestionar y prevenir estos tipos de riesgos sobre la información han surgido y evolucionado estándares internacionales que brindan lineamientos para optimizar los procesos de seguridad[18][19][20], en Colombia por ejemplo el gobierno Nacional a través del ministerio de las Tecnologías y las Telecomunicaciones establece el Modelo de Seguridad de la Información basado en la ISO/IEC 27001, el cual debe ser implementado por las entidades

gubernamentales [21][22] ya que no hacerlo podría estar en riesgo los activos de información y la continuidad en la prestación del servicio.

Acogiéndose a esto, la Corporación busca adoptar lineamientos de buenas prácticas en seguridad de la información [23] que le permitan mejorar los procesos, detectar oportunamente y a tiempo de brechas de seguridad, fortalecer su organización interna y estar a nivel de otras grandes entidades públicas o privadas a nivel mundial.

## 1.3 JUSTIFICACIÓN

La necesidad de minimizar el impacto que afecte la información y mejorar el manejo de los activos de información de la entidad requiere la toma de decisiones y acciones preventivas que garanticen a la Corporación resultados favorables ante posibles auditorías externas, la no interrupción en la continuidad de sus labores, evitar demandas, perdidas económicas o afectación a la imagen corporativa; todo esto a través del establecimiento de un modelo de gestión de seguridad de la información que oriente los esfuerzos hacia una mejora continua de los procesos internos y el manejo adecuado de la información [24].

La ley 1712 de Transparencia y del Derecho de Acceso a la Información Pública Nacional, busca garantizar a la ciudadanía acceso a información veraz relacionada con la gestión de una entidad gubernamental, y de esta manera ser parte activa en la rendición de cuentas [25][26]. Debido a que la Corporación captura información tanto física como electrónica durante la prestación de sus servicios o en la interacción de usuarios con la página web de la entidad, se hace responsable del manejo, manipulación y protección de los datos personales de los usuarios de acuerdo a la Ley 1581 de 2012, Decreto 1377 de 2013 y en ejecución de políticas internas de protección de datos personales. Estas políticas deben ser adoptadas como fundamento del correcto cumplimiento de su misión, con alcance a

funcionarios y usuarios en general sin importar el tipo de vinculación, ya que su incumplimiento derivaría en sanciones [27].

Se evidenció la necesidad de adoptar un modelo que permita orientar los esfuerzos hacia la implementación controles de seguridad y buenas prácticas para contrarrestar acciones de violación de accesos, manipulación indebida o pérdida de información que pongan en riesgo los datos personales de los usuarios y la integridad de los activos[28] de la Corporación Nasa Kiwe. Además, este trabajo permite a ingenieros de sistemas en formación aplicar conocimientos y contribuir con una mejora en el desarrollo de las actividades propias de una entidad, esto fortalece y complementa el conocimiento con el desarrollo de habilidades requeridas al enfrentarse a un entorno de aplicación real, bajo condiciones de trabajo en equipo, participación continua y resolución de eventos inesperados.

## 1.4 OBJETIVOS

### 1.4.1 OBJETIVO GENERAL

Implementar un Modelo de Seguridad y Privacidad de la Información, basado en la norma internacional ISO/IEC 27001 de 2013 acorde al Sistema de Gestión de Seguridad de la Información de la Corporación Nasa Kiwe y normatividad vigente para la protección de activos.

### 1.4.2 OBJETIVOS ESPECÍFICOS

1. Establecer la línea base que soporta la seguridad de la información en la Corporación Nasa Kiwe.
2. Proponer estrategias de adaptabilidad de la norma ISO/IEC 27001 en la Corporación Nasa Kiwe según los requerimientos y servicios tecnológicos presentes.
3. Validar el modelo de gestión de seguridad de la información propuesto para la Corporación Nasa Kiwe.

## 1.5 ALCANCE Y LIMITACIONES

### 1.5.1 ALCANCE

Debido a las condiciones actuales y el estado de la documentación existente el alcance de este trabajo está orientado a cubrir la planificación y diseño de un modelo de gestión de seguridad de la información para la Corporación Nasa Kiwe con el propósito de resguardar la privacidad, confidencialidad e integridad de los activos de información. En este trabajo se considera el proceso de gestión de la informática y la conectividad de la entidad y algunos procesos específicos que se involucran directamente, este alcance está ligado a las decisiones de la alta dirección; como guía para el desarrollo del trabajo se tendrá como base la norma internacional ISO/IEC 27001 y su Anexo A (27002).

### 1.5.2 LIMITACIONES

- El trabajo llevará a cabo la planificación y algunos apartes de las fases previas a la implementación del modelo de Gestión de Seguridad de la Información, no incluye fases de implementación, revisión, mantenimiento y mejora de dicho modelo.
- Depende de la disponibilidad de la alta dirección para la aprobación de los documentos. El poco tiempo definido para realizar el trabajo implica considerar este como un limitante.
- Documentación faltante: el proceso de identificación y clasificación de activos de información no se ha realizado hasta el momento en la entidad, por lo que no considera ya que estará a cargo de un ente externo.

## 1.6 RESULTADOS ESPERADOS

### 1.6.1 PRODUCTOS ESPERADOS

Conforme a la elaboración de herramientas documentales, formatos y procedimientos necesarios para el cumplimiento de este trabajo se listan los entregables que lo soportan:

- Modelo de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001.
- Procedimiento de contacto con las autoridades.
- Procedimiento de Gestión de usuarios y contraseñas de acceso.
- Formato para la solicitud y aprobación de cambios.
- Guía para la Gestión y clasificación de incidentes.
- Formato de reporte, valoración y gestión de eventos e incidentes de seguridad.
- Formato de acceso a servicios informáticos
- Políticas de Seguridad de la Información.

## 1.7 IMPACTO

Actualmente la Corporación Nasa Kiwe brinda acompañamiento a las comunidades afectadas no solo como una responsabilidad gubernamental sino como generadores de cambio en la calidad de vida de quienes en su momento enfrentaron la desintegración familiar, la pérdida de su territorio, enseres y su sustento. Las labores están orientadas a la implementación de proyectos productivos para el auto sostenimiento y el desarrollo de obras (vías, vivienda, espacios de acceso a TI) para las comunidades afectadas. Por medio de lineamientos de seguridad y estrategias que blinden sus activos de información y servicios, la Corporación Nasa Kiwe busca garantizar cumplimiento de su misión, y que le permita [29]:

- Identificarse como una entidad pública que cumple satisfactoriamente el desarrollo de sus actividades[30], acogiendo y garantizando la seguridad, confidencialidad, integridad y disponibilidad de la información de sus usuarios y los activos propios de la Corporación.
- Agregarle valor a la información en la Corporación.
- Incrementar los niveles de confianza en los servidores públicos.
- Generar hábitos de buenas prácticas de seguridad dentro de los funcionarios y colaboradores en la Corporación a partir de políticas y lineamientos adoptados.
- Dar cumplimiento a requerimientos legales.
- Disminuir el impacto de riesgos, mediante acciones preventivas.
- Establecer barreras de seguridad contra posibles fugas de información, intrusos o ataques.
- Mejorar su seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información.

En caso de no avanzar hacia el objetivo propuesto en este trabajo, la Corporación Nasa Kiwe podría verse afectada durante el desarrollo de sus actividades, ya sea con pérdidas en infraestructura tecnológica y/o de fuga de información confidencial. El Decreto Nacional 2145 establece la obligatoriedad en el ejercicio de autocontrol y documentación de procesos en entidades públicas [31], por lo que adicionalmente acarrearía sanciones disciplinarias o económicas.

# CAPÍTULO II: MARCO TEÓRICO O REFERENTES CONCEPTUALES

## 2.1 MARCO TEÓRICO

La Corporación Nasa Kiwe brinda acompañamiento a comunidades en el departamento del Cauca y el Huila por lo que se requiere del manejo adecuado de la información tanto dentro de la entidad y como con los demás colaboradores que participan en pro del cumplimiento de la misión institucional[1].

Con la evolución tecnológica es indispensable un aumento de esfuerzos para garantizar la seguridad de la información ante posibles amenazas, por lo que contar con un modelo de gestión de seguridad de información permite gestionar adecuadamente los recursos y orientarlos hacia el cumplimiento de objetivos conforme a la ley y con base a estándares mundiales de seguridad. En Colombia por ejemplo, el modelo propuesto por el ministerio de las Tecnologías y las Telecomunicaciones debe ser implementado por las entidades gubernamentales [21] ya que no hacerlo podría estar en riesgo los activos de información y la continuidad en la prestación del servicio. Es por esto que la Corporación busca adoptar lineamientos de buenas prácticas en seguridad de la información [23] que le permitan mejorar los procesos, detectar oportunamente y a tiempo las brechas de seguridad, fortalecer su organización interna y estar a nivel de otras grandes entidades públicas o privadas a nivel mundial.

### 2.1.1 REFERENTES TEÓRICOS

A continuación, se presentan algunos de los referentes teóricos utilizados como fundamento para el establecimiento del modelo de gestión de seguridad de la información para Nasa Kiwe, ver Tabla 1.

| | |
|---|---|
| **Título** | Modelo de Seguridad |
| **Descripción** | "El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información" [7]. |
| **Ubicación** | Entidades públicas en Colombia |

| | |
|---|---|
| **Título** | Implementación de Seguridad de la Información en una MIPYME. |
| **Descripción** | "El contexto del cibercrimen aborda todo tipo de esferas; en ese sentido firmas de auditoría y el Centro Cibernético Policial argumenta que el 46 % de los crímenes informáticos se dan por la carencia de elementos de seguridad" [32]. |
| **Ubicación** | Colombia |

| | |
|---|---|
| **Título** | Política de Seguridad y Privacidad de la Información |
| **Descripción** | "Política de Seguridad de la Información en la Gobernación, materializa la gestión responsable de información que proyecta garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos y metas trazadas en la |

| | |
|---|---|
| | administración pública”[33]. |
| **Ubicación** | Gobernación Nariño, Colombia |

| | |
|---|---|
| **Título** | Política de Seguridad de la Información |
| **Descripción** | “El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas.”[34] |
| **Ubicación** | Colombia |

| | |
|---|---|
| **Título** | Inventario de activos de Información |
| **Descripción** | “Garantizar la seguridad de la información en la entidad, mediante la definición, implementación, seguimiento y mejoramiento de elementos (herramientas, controles, procedimientos, etc.) que permitan proteger la información frente a la posible materialización de riesgos.” [30]. |
| **Ubicación** | Colombia |

Tabla 1. Referentes teóricos para la aplicación de un modelo de seguridad de la información

### 2.1.2 SEGURIDAD DE LA INFORMACIÓN

Se entiende por seguridad de la información como el conjunto de medidas preventivas y reactivas que permiten protegerla y resguardarla [28], involucra un proceso de mejora continua y su principal objetivo es hacer frente a los riesgos que puedan vulnerar la confidencialidad, la integridad y la disponibilidad de la información o los sistemas, de tal manera que mediante las políticas, estrategias,

controles y técnicas de seguridad sea posible analizar, prevenir y encontrar soluciones rápidas que contrarresten los efectos adversos sobre la información [35].

El concepto de seguridad de información involucra la adopción de medidas de seguridad tanto físicas como lógicas para asegurar uno de los activos más valiosos para toda organización, la información. Se entiende como la preservación de las características fundamentales como se evidencia en la Tabla 2 [36]:

| Criterio | Definición |
|---|---|
| **Disponibilidad** | Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. |
| **Confidencialidad** | Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma. |
| **Integridad** | Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento, que la información no sea modificada sin la debida autorización. |
| **Autenticidad** | Busca asegurar la validez de la información en tiempo, forma y distribución. Garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. |
| **No repudio** | Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió. |
| **Legalidad** | Cumplimiento de leyes, normas, reglamentaciones. |

Tabla 2. Aspectos fundamentales Seguridad de la Información. Fuente: MinTIC

### 2.1.3 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Es un enfoque sistemático que permite administrar y proteger la información de una organización sin importar el formato de esta. Incluye personas y sistemas de

TI(Tecnologías de la Información) mediante la aplicación de un proceso de gestión de riesgos de tal manera que se pueda contrarrestar cualquier amenaza y garantizar el desarrollo normal de las actividades[37].

Por tener características adaptables, la gestión de seguridad brinda lineamientos ajustables según la necesidad, no se rige al total u obligatorio cumplimiento de las políticas y lineamientos de la norma [7][38]; aplicar labores de gestión de seguridad puede ayudar a mantener seguros los activos de información de cualquier tipo de organización independiente de su tamaño o naturaleza.

Aplicar correctamente un modelo de gestión de seguridad de la información implica la participación de toda la organización para el desarrollo de las fases, la identificación de las necesidades y dar cumplimiento a los controles que se determinen para asegurar los activos [37][39]. Además, el compromiso con el sistema de gestión permite tener un acceso adecuado de los recursos y evitar comprometer el funcionamiento de la organización.

### 2.1.4 NORMAS ISO/IEC 27000

La familia de normas ISO/IEC 27000, es publicada por la Organización Internacional de Normalización (*International Organization for Standardization - ISO*) y la Comisión Electrotécnica Internacional (*International Electrotechnical Commission - IEC*), ayuda a las organizaciones a mantener seguros los activos de información mediante la implementación de prácticas de gestión de la seguridad de la información.

El uso de esta familia de estándares ayudará a una organización a administrar la seguridad de activos tales como información financiera, propiedad intelectual, detalles de empleados o información confiada por terceros [40] permite:

- Asegurar sus activos críticos.
- Administrar los riesgos de forma mucho más efectiva.

- Mejorar y mantener la confianza de los usuarios.
- Demostrar conformidad con las mejores prácticas internacionales.
- Evitar daños de imagen, pérdida de ganancias o posibles multas regulatorias.
- Desarrollar su postura de seguridad de la información junto con los desarrollos tecnológicos.

La ISO agrupa un extenso número de normas dentro de la familia ISO 27000 [40][41][42][43] como se muestra en la Tabla 3 las cuales pueden ser adoptadas según el requerimiento de seguridad:

**Familia Norma 27000**

| Norma | Definición |
|---|---|
| ISO 27001 | Es la norma principal de toda la serie ya que incluye todos los requisitos con los cuales se puede auditar y certificar el Sistema de Gestión de Seguridad de la Información en las organizaciones. En el Anexo A (norma ISO 27002) se enumeran los objetivos de control y los análisis que desarrolla la norma ISO 27001. |
| ISO 27002 Anexo A | Manual de buenas prácticas, describe los objetivos de control y las evaluaciones recomendables en cuanto a la seguridad de la información. No es certificable. En ella se puede encontrar 39 objetivos de control y 133 controles agrupados en 11 dominios diferentes. La norma ISO 27001 incluye este anexo que resume todos los controles, las organizaciones pueden elegir no aplicarlos. |
| ISO 27003 | Es un manual para implementar un Sistema de Gestión de Seguridad de la Información, además, brinda una descripción clara hasta su implementación y todos los requerimientos de las fases. |
| ISO 27004 | En este estándar se especifican las técnicas de medida y las métricas que son aplicables a un Sistema de Gestión de Seguridad de la Información y los controles relacionados. Las métricas se utilizan para la medición de los controles implementados de |

| | |
|---|---|
| | acuerdo al Anexo A. |
| ISO 27005 | Norma de apoyo a conceptos generales que vienen especificados en la ISO 27001, diseñada para ayudar a aplicar la seguridad de la información basada en un enfoque de gestión de riesgos. Se puede aplicar a todo tipo de organizaciones e implica conocer todos los conceptos, modelos, procesos y términos descritos en la norma ISO 27001 e ISO 27002. |
| **ISO 27006** | Este estándar especifica todos los requisitos de la ISO 27001 para lograr la acreditación de las entidades de auditoría y certificación de Sistema de Gestión de Seguridad de la Información. |
| ISO 27007 | Es un manual de auditoría de un Sistema de Gestión de Seguridad de la Información. Ha sido creado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). |
| ISO 27011 | Es una guía de gestión de seguridad de la información específica para telecomunicaciones. |

Tabla 3. Normas 27000. Fuente: Propia

### 2.1.5 BASES LEGALES

El diseño de un modelo de gestión de Seguridad de la Información en la entidad y sus derivados (políticas, formatos, procedimientos y procesos) deben estar de acuerdo con las buenas prácticas de seguridad establecidas según el estándar y la normatividad tanto en Colombia como en el exterior, para poder establecer reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información. A

continuación, se presentan los principales instrumentos normativos aplicables [44][45]:

- “LEY 1712 DE 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones”.
- “Ley Estatutaria 1581 de 2012: Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales”.
- “Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones”.
- “Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones”.
- “Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos”.
- “Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.
- “Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- “Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.
- “Ley 1150 DE 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos”.
- “Ley 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos”.
- “Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa”.
- “LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República”.

Decreto 1377 de 2013, Resolución No.040 de 2016, Resolución No.021 de 2010, Resolución No.022 de 2010, además, Políticas de seguridad y protección de la Corporación Nasa Kiwe [18] [19].

# CAPÍTULO III: METODOLOGÍA

En este capítulo se describe la metodología que permite dar cumplimiento a los objetivos específicos, los cuales a su vez permiten alcanzar el objetivo general.

Debido a que este trabajo parte de la modalidad de grado Pasantía, las tareas propias presenciales llevadas a cabo en la Corporación implican labores investigativas, observaciones, evaluaciones según el criterio del autor, reuniones periódicas y entrevistas con el personal involucrado. Conocer el estado del proceso de gestión de la informática y la conectividad es una labor iterativa, por lo que aquí se utilizará un método de investigación de campo apoyado de un marco de trabajo que permite la inclusión de cambios durante las fases.

Se tiene en cuenta el marco de trabajo SCRUM para el desarrollo de la práctica, a pesar de que no corresponde a un proyecto de software se puede adaptar para el desarrollo de actividades de tal manera que se cuente con revisiones periódicas después de la terminación de cada dominio del documento, lo que se podría denominar según Scrum como Sprint [48] con el propósito de evaluar el estado del documento del modelo y detectar posibles mejoras. Se establecen cuatro fases, cada una ofrece un grupo de actividades ligadas entre sí, de tal manera que el desarrollo de la práctica es iterativo, en cualquier momento y cuando así se requiera se puede retornar a una fase anterior [48][49] dependiendo de las necesidades que surjan durante la elaboración de documentación o en el respaldo de fundamentos legales. A continuación, se listan las fases y sus respectivas actividades, necesarias para abordar la situación problema ya definida, y de manera dinámica se representa en la Ilustración 2.

- **Fase I. Identificación de necesidades y composición institucional.**

1.1 Identificar el entorno y las herramientas de trabajo.
1.2 Realizar inducción e identificar tareas y procesos de desarrollo
1.3 Identificar funciones.
1.4 Estimar alcance de la práctica profesional de acuerdo a las necesidades.

- **Fase II. Identificación de normatividad y valoración de la documentación existente**

2.1 Identificar prioridades en la elaboración de la documentación.
2.2 Identificar políticas internas y normatividad vigente en Colombia.
2.3 Validar y agrupar la documentación que involucra al proceso de gestión de la informática y la conectividad con el cumplimiento de la Políticas de seguridad y privacidad.
2.4 Revisar la documentación existente (políticas, manuales, reportes, procesos, guías, formatos, instrumentos de documentación, etc.).
2.5 Validar aplicación de políticas externas en los procesos de la Corporación.

- **Fase III. Documentación del (MSPI) de acuerdo a los dominios establecidos en la norma ISO/IEC 27001.**

3.1 Estudiar y profundizar en la normatividad colombiana base de las Políticas de seguridad y privacidad de información.
3.2 Tareas de investigación (recopilación de información, consulta portales oficiales, depuración de información, consolidación de documentación de soporte) según la necesidad de cada dominio.
3.3 Redactar sistemáticamente dominios, políticas, lineamientos, procedimientos y sugerencias que sirvan de base para la implementación del modelo.

- **Fase IV. Adaptación**

4.1 Validación del documento generado
4.2 Socializar el documento con el proceso de gestión de la informática y la conectividad y la secretaría General.
4.3 Aprobación del documento por parte de la Secretaria General.
4.4 Adaptar documentación actual de la Corporación conforme al modelo generado y aprobado.
4.5 Divulgar cambios para posterior adopción dentro de Nasa Kiwe.

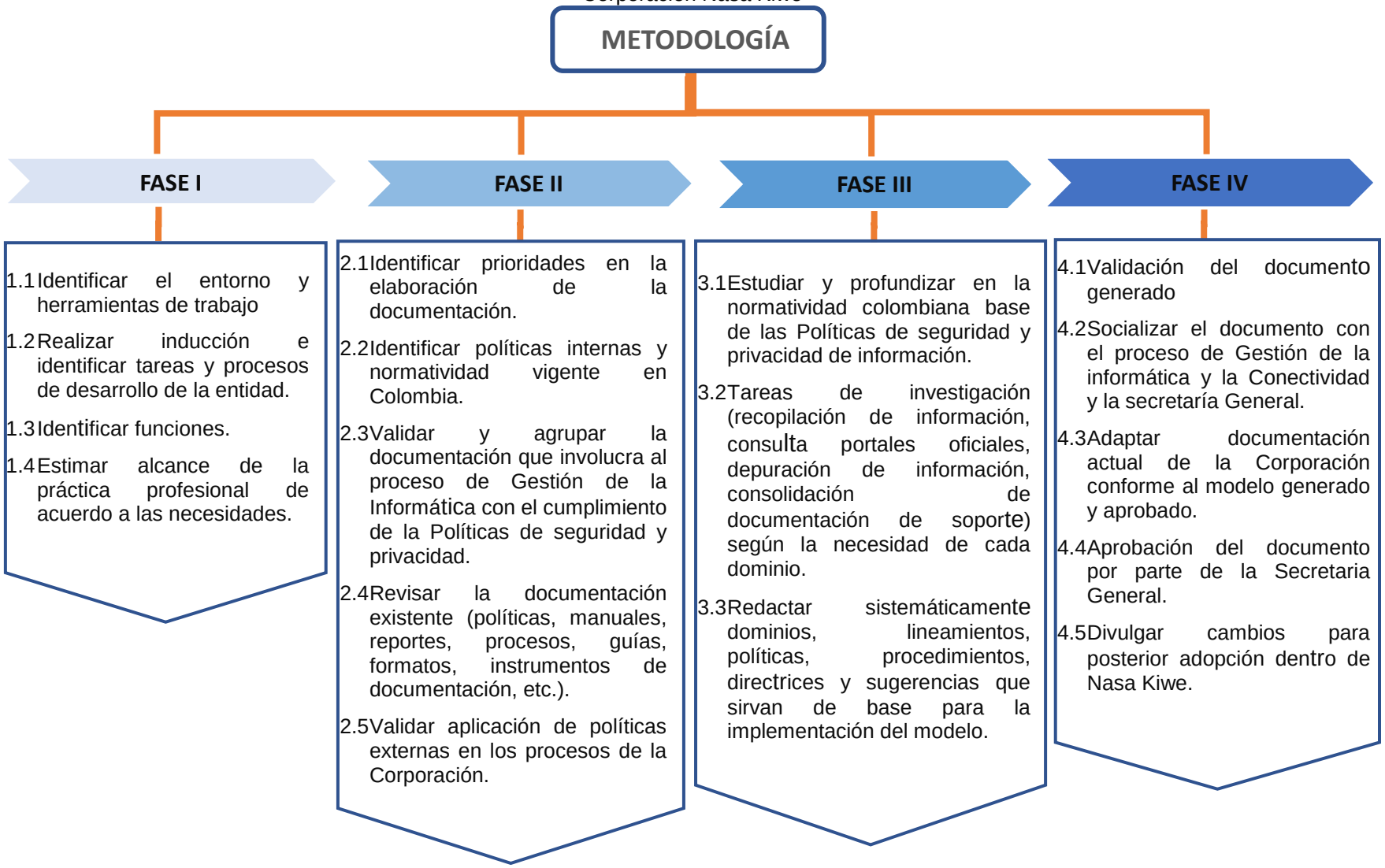


Ilustración 2. Fases metodológicas. Fuente: Propia

# CAPÍTULO IV: DESARROLLO DEL PROYECTO

## 4.1 FASE I. IDENTIFICACIÓN DE NECESIDADES Y COMPOSICIÓN INSTITUCIONAL

Para dar inicio al desarrollo de la práctica de tal manera que se cumplan los objetivos, fue necesario un reconocimiento institucional e identificar los procesos involucrados. Para el desarrollo de estas actividades se contó activamente con el líder del proceso de Gestión Informática y Conectividad y la secretaria General de la Corporación Nasa Kiwe ya que a manera de consenso se identificaron las funciones a desempeñar respecto al alcance estimado para la práctica profesional; durante esta fase se establecieron reuniones mensuales para la identificación de nuevas necesidades, y semanales según la necesidad, de tal manera que hubiese comunicación constante y retroalimentación hacia los instrumentos generados. Como función principal se definió la elaboración de la documentación requerida para el plan de gestión de la entidad de acuerdo a la implementación de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), adicionalmente, las demás funciones se determinaron variables según la necesidad dentro del proceso de gestión de la informática y la conectividad y/o otros requerimientos en la entidad.

### 4.1.1 LA ENTIDAD

La **Corporación Nasa Kiwe** es una entidad pública, fundada para atender una tragedia socioambiental en 1994 en el departamento del Cauca. Desde entonces la entidad ha contado con recursos públicos para la realización de proyectos y la atención de las personas afectadas [1].

### 4.1.2 MISIÓN

“La Corporación Nasa Kiwe es la institución creada por el estado colombiano para ejecutar en coordinación con distintos organismos públicos y privados las actividades tendientes a recuperar y rehabilitar social, económica y culturalmente la población asentada en la zona de Tierradentro y áreas aledañas, afectadas por desastres de origen natural” [50].

### 4.1.3 VISIÓN

“Ser una entidad reconocida por haber logrado que las comunidades atendidas avancen significativamente hacia su auto sostenimiento y aprendan a administrar los riesgos naturales de su condición geográfica, económica, social y cultural, mediante la implementación de los planes de rehabilitación y reconstrucción de la cuenca del Río Páez y Zonas Aledañas de la Corporación Nasa Kiwe” [50].

**Actividades Misionales que realiza**

La Corporación cuenta con campos de acción específicos, mediante proyectos o actividades ejecutadas directamente o mediante convenios interinstitucionales realiza acciones de reconstrucción, protección y recuperación de la biodiversidad e integridad de los ecosistemas, desarrollo sostenible, adquisición y recuperación de tierras de las comunidades afectadas [51].

### 4.1.4 ESTRUCTURA ORGANIZACIONAL

Se presenta la estructura definida en la Corporación Nasa Kiwe, la jerarquía y relación entre las áreas en la Ilustración 3.

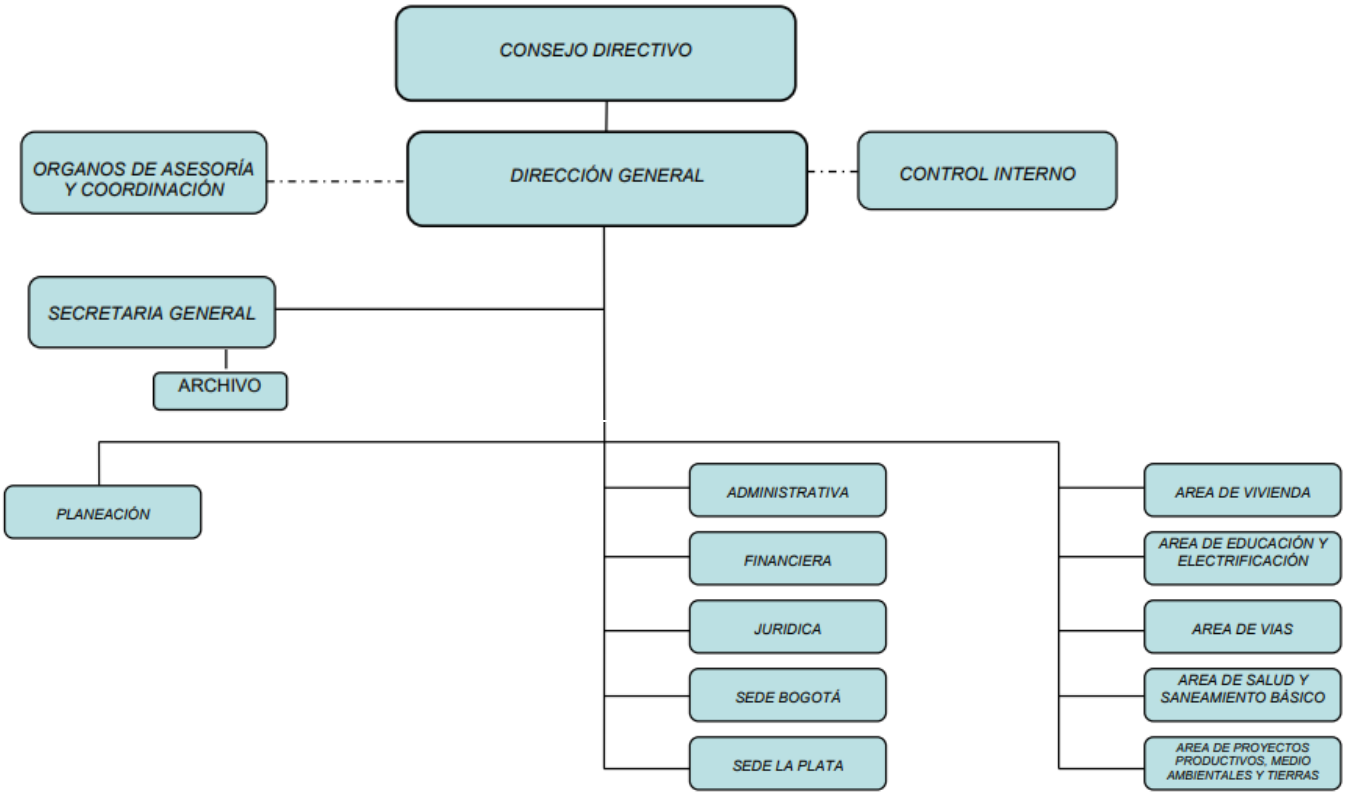


Ilustración 3. Estructura Organizacional Corporación Nasa Kiwe. Fuente: www.nasakiwe.gov.co

### 4.1.5 MAPA DE PROCESOS

En la estructura organizacional no se relaciona la oficina de gestión de la informática, pero éste por ser transversal hace parte fundamental del desarrollo de todas las actividades de la entidad, como se muestra en la Ilustración 4, entre los procesos de la entidad se resalta el de gestión de la informática y la conectividad.

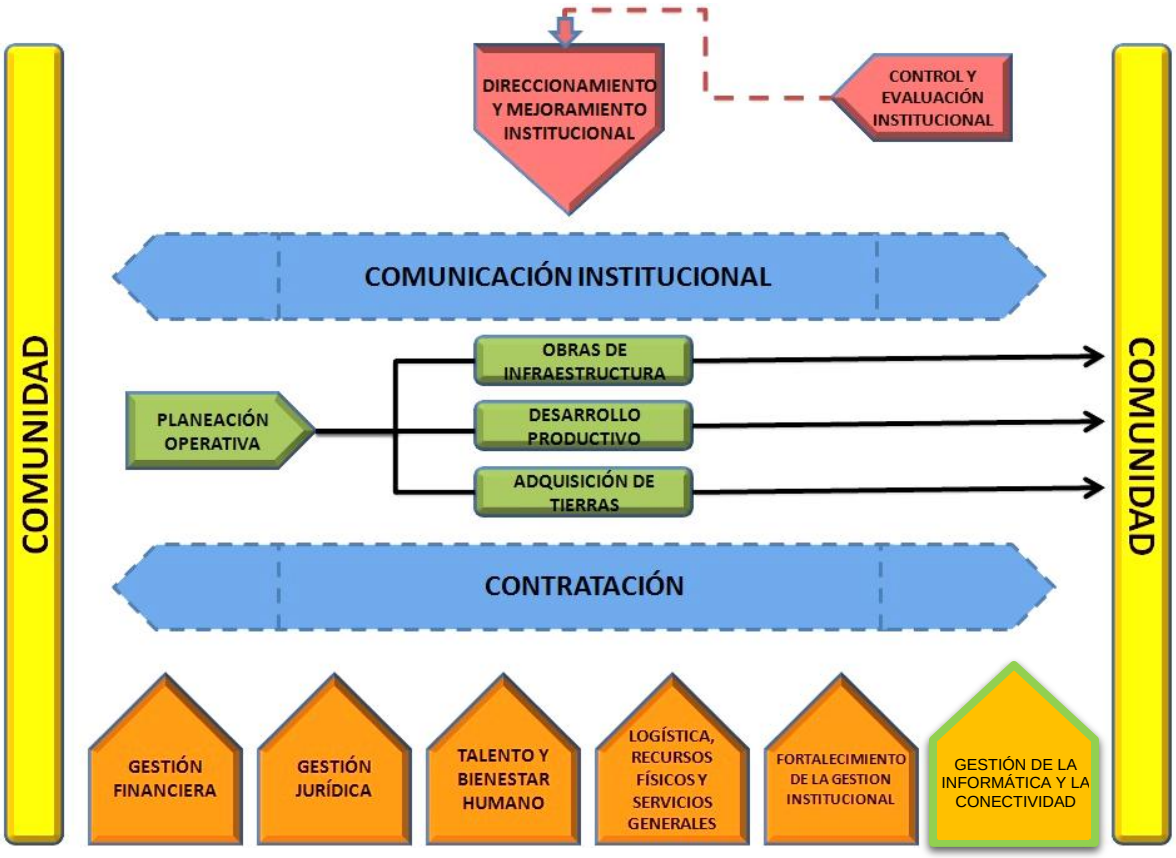


Ilustración 4. Mapa de procesos Corporación Nasa Kiwe. Fuente: www.nasakiwe.gov.co

### 4.1.6 PROCESO DE GESTIÓN DE LA INFORMÁTICA Y LA CONECTIVIDAD

El principal objetivo es brindar apoyo técnico de manera oportuna y eficaz a la infraestructura tecnológica e informática de la Corporación Nasa Kiwe y contribuir para que todos los procesos de la Corporación puedan desarrollar sus actividades. El proceso inicia con la identificación de los recursos y requerimientos tanto a nivel de software como a nivel de hardware incluyendo las solicitudes de servicios y termina con la entrega e instalación de equipos, aplicativos y prestación de servicios solicitados. Además, se encarga del reporte de la información a los portales estatales desde el proceso de recepción de la información hasta el registro de ésta en la plataforma estatal. Por ser una entidad pública debe realizar reporte de información a las diferentes entidades estatales.

Es uno de los procesos fundamentales para el tratamiento de toda la información de la Corporación ya que interviene en la protección de la integridad, disponibilidad y confidencialidad de la información manejada a través de los recursos tecnológicos que se cuentan[8]. La seguridad de la información recae en las acciones que se realicen desde el proceso, de ahí la necesidad de incluir buenas prácticas de seguridad y privacidad de la información.

## 4.2 FASE II. IDENTIFICACIÓN DE NORMATIVIDAD Y VALORACIÓN DE LA DOCUMENTACIÓN EXISTENTE

Esta fase contiene las actividades necesarias para identificar las prioridades en Seguridad y Privacidad dentro de la entidad, haciendo un análisis de aplicabilidad del modelo propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el estándar internacional ISO 27001. El desarrollo de las actividades de la Fase I, II y III permitió generar una propuesta de adaptación de la norma al modelo de gestión de seguridad de la entidad y dar cumplimiento a los Objetivos específicos 1 y 2 de este trabajo. Las actividades se abarcaron según el requerimiento, por ser definidas como de uso iterativo fueron indispensables para determinar la viabilidad de controles y métricas contenidos en el Anexo A(ISO 27002) de la norma.

### 4.2.1 IDENTIFICAR PRIORIDADES EN LA ELABORACIÓN DE DOCUMENTACIÓN:

Debido a que la entidad no cuenta con un consolidado para los criterios de seguridad de la información, las funciones parten de la recolección de documentación existente que permita dar inicio a la estrategia Gobierno Digital y a la elaboración del modelo según los dominios asignados del Anexo A.

### 4.2.2 IDENTIFICAR POLÍTICAS INTERNAS Y NORMATIVIDAD EN COLOMBIA:

La protección y seguridad de la información que soporta los procesos de la entidad e identificar los usuarios que intervienen con los servicios debe cumplir con ciertas políticas. Se identificó el documento

manejado por la entidad donde establecen las responsabilidades que tiene con el tratamiento de los datos personales de sus usuarios definida como; “Políticas de Seguridad – Políticas de Protección de Datos Personales”, además políticas definidas desde el proceso de gestión de la informática y la conectividad de la entidad. Adicionalmente la normatividad ya definida en el apartado 2.1.5 Bases Legales.

Durante la identificación de las políticas internas de la entidad para la seguridad de la información se evidenció la desactualización y la inclusión parcial de las políticas vigentes que sugiere la norma. Sin embargo, no se definen mecanismos para la medición del nivel de cumplimiento ya que la evaluación se realiza durante sesiones de trabajo directo con el líder del proceso.

**4.2.3 VALIDAR Y AGRUPAR LA DOCUMENTACIÓN QUE INVOLUCRA AL PROCESO DE GESTIÓN INFORMÁTICA Y CONECTIVIDAD CON EL CUMPLIMIENTO DE LA POLÍTICAS DE SEGURIDAD Y PRIVACIDAD**: Se agrupa el mayor número de información relacionada con la seguridad y privacidad de la información dentro del proceso de gestión de la informática y lo relacionado con otros mecanismos (si aplica). La documentación de fuentes externas tomada como base para la elaboración de la nueva documentación del modelo fue agrupada según el criterio de vigencia (año). Dentro de los lineamientos de la entidad se establece el respaldo periódico de los activos por lo que se realizó una preselección de la documentación dividida de la siguiente manera: una parte como “apoyo y base para la redacción” la cual no requería ser ingresada al repositorio, y otra parte que incluía los nuevos documentos generados a diario los cuales debían ser incluidos en las copias de respaldo.

**4.2.4 REVISAR LA DOCUMENTACIÓN EXISTENTE (políticas, manuales, reportes, procesos, guías, formatos, instrumentos de documentación, etc.):** Se revisó la documentación que permitió identificar el estado actual del

proceso de gestión de la informática y la conectividad, ya que gran parte de ésta se encontraba desactualizada o inexistente.

**4.2.5 VALIDAR APLICACIÓN DE POLÍTICAS EXTERNAS EN LOS PROCESOS DE LA CORPORACIÓN:** La norma contempla establecer ciertas políticas y lineamientos para el aseguramiento de la información, algunas eran adaptables, otras de lo contrario no se encontró aplicabilidad a la entidad por el momento, ya sea por el tamaño o naturaleza de la entidad o porque aún no se contempla una certificación en la norma. De acuerdo a otro tipo de reglamentación legal solo se tuvo en cuenta normatividad vigente en Colombia como, por ejemplo, trato de datos personales, derechos de autor, transparencia, derecho a la información, etc.

## 4.3 FASE III. DOCUMENTACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE ACUERDO AL ANEXO A DE LA NORMA ISO/IEC 27001:2013

**4.3.1 ESTUDIAR Y PROFUNDIZAR EN LA NORMATIVIDAD COLOMBIANA BASE DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN:** Se profundizó en la interpretación de la normatividad identificada para apoyar las tareas de manejo de software y derechos de autor dentro de la entidad, las políticas de ciberseguridad y ciberdefensa permitieron documentar controles sobre seguridad y buenas prácticas, además, tener presente las responsabilidades que tiene toda persona natural o jurídica sobre la protección de la información y los datos en tránsito fue importante para entender la posible clasificación y los niveles de confidencialidad existentes de los activos dentro del proceso de gestión de la informática.

**4.3.2 TAREAS DE INVESTIGACIÓN (RECOPILACIÓN DE INFORMACIÓN, CONSULTA PORTALES OFICIALES, DEPURACIÓN DE INFORMACIÓN,**

**CONSOLIDACIÓN DE DOCUMENTACIÓN DE SOPORTE) SEGÚN LA NECESIDAD PARA LA ELABORACIÓN DE CADA DOMINIO:** Esta actividad no se limita a la Fase III, se relaciona con los apartados *2.3* y *2.4* de la Fase II. Estas tareas de investigación se desarrollaron durante las fases que implican recolección de información y como base para la construcción de cada dominio del Anexo A.

**4.3.3 REDACTAR SISTEMÁTICAMENTE DOMINIOS, LINEAMIENTOS, DIRECTRICES, POLÍTICAS, PROCEDIMIENTOS Y SUGERENCIAS QUE SIRVAN DE BASE PARA LA PUESTA EN MARCHA, SUPERVISIÓN, MEJORA Y CONTROL DE LA IMPLEMENTACIÓN DEL MODELO:** Inicialmente la construcción del modelo empezó por la asignación de los dominios a elaborar de acuerdo al conocimiento del líder del proceso, posteriormente a criterio propio y según la relación se documentaron los demás, donde se propuso la metodología para abordar la documentación, incluyendo procedimientos, formatos o políticas correspondientes si se requerían.

Los dominios abordados de la norma son: Aspectos organizativos de la Seguridad de la Información, Seguridad ligada a los recursos humanos, Gestión de activos, Cifrado, Seguridad física y ambiental, Seguridad en la operativa, Seguridad en las telecomunicaciones, Relaciones con proveedores y Gestión de incidentes en la seguridad de la información, contenidos en el ANEXO 1 del presente trabajo, los formatos, procedimientos, guías y políticas derivadas de los dominios fueron generados en documentos independientes, ver Anexos (2,3,4,5,6,7,8).

## 4.4 FASE IV. ADAPTACIÓN

Una vez creado el documento acorde a la normatividad aplicada a los procesos de la Corporación, se realizó de manera conjunta la socialización de toda la documentación, donde se llevó a cabo:

**4.4.1 VALIDACIÓN DE LOS DOCUMENTOS GENERADOS:** Para llegar a la documentación final se incluyó revisiones periódicas para los avances y sesiones de trabajo completas destinadas para la revisión de los documentos finales como se presenta a continuación en la Tabla 4:

| CRONOGRAMA DE REUNIONES | | | | | |
|---|---|---|---|---|---|
| Día | Mes | Hora | Lugar | Asistentes | Observaciones |
| 1 | Agosto | 8:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Inicio pasantía |
| 6 | Agosto | 10:00 a.m. | Oficina Secretaría General | Dra. Zambrano Ing. Vásquez, Est. Tovar | Distribución de actividades/tiempo |
| 24 | Agosto | 9:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Revisión de avances |
| 24 | Septiembre | 3:00 p m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Revisión de avances |
| 26 | Septiembre | 9:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Dra. Zambrano Ing. Vásquez, Est. Tovar | Revisión de avances |
| 25 | Octubre | 10:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Revisión de avances |
| 2 | Noviembre | 9:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Dra. Zambrano Ing. Vásquez, Est. Tovar | Revisión de avances |
| 23 | Noviembre | 10:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Revisión de avances |
| 3 | Diciembre | 9:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Dra. Zambrano, Ing. Vásquez, Est. Tovar | Revisión de avances |
| 19 | Diciembre | 9:00 a.m. 3:00 p.m. | Oficina Gestión de la Informática y la Conectividad | Dra. Zambrano, Ing. Vásquez, Est. Tovar, colaboradores | Socialización de documentación |
| 20 | Diciembre | 9:00 a.m. 3:00 p.m. | Oficina Gestión de la Informática y la Conectividad | Dra. Zambrano, Ing. Vásquez, Est. Tovar, colaboradores | Socialización de documentación |
| 26 | Diciembre | 10:00 a.m. | Oficina Gestión de la Informática y la Conectividad | Ing. Vásquez, Est. Tovar | Revisión de cambios |

Tabla 4. Cronograma de reuniones. Fuente: Propia

**4.4.2 SOCIALIZAR EL DOCUMENTO CON LÍDER DEL PROCESO DE GESTIÓN DE LA INFORMÁTICA Y LA CONECTIVIDAD, Y DEMÁS INTERESADOS:** La socialización se llevó a cabo con la Secretaria General (representante de la alta dirección) de la Corporación y todos los colaboradores (funcionario y contratistas) del proceso de gestión de la informática y la conectividad, durante las sesiones se realizaron los ajustes sugeridos a medida que se abordaban los dominios, de tal manera que al finalizar se tuviera un documento depurado y ajustado a las necesidades de la Corporación sin tener que hacer uso de reuniones extras**.**

**4.4.3 ADAPTAR DOCUMENTACIÓN ACTUAL DE LA CORPORACIÓN CONFORME AL MODELO GENERADO Y APROBADO:** La documentación que respalda la planificación y diseño del modelo se generó como primera versión para todos los anexos, excepto el ANEXO 2; al revisar la documentación existente vinculada al proceso de gestión informática y el proceso de Fortalecimiento [16] [17] en la Corporación Nasa Kiwe a través de la red interna y el portal web se evidenció la necesidad de actualizar algunas políticas de acuerdo con las nuevas necesidades. Fue el único documento existente que oficialmente de modificó.

**4.4.4 APROBACIÓN DEL DOCUMENTO POR PARTE DE LA SECRETARIA GENERAL:** Al finalizar la actividad de socialización y ya con los documentos terminados la Secretaria General procedió a dar como aprobado el trabajo realizado durante la práctica profesional. La publicación e implementación del modelo y las herramientas generadas pasan a consideración del comité y la Dirección de la entidad.

**4.4.5 DIVULGAR CAMBIOS PARA POSTERIOR ADOPCIÓN DENTRO DE NASA KIWE:** La divulgación a nivel institucional del trabajo realizado quedó

por fuera del tiempo de la práctica profesional debido a la extensión de la documentación y la limitación del tiempo. La propuesta será presentada a la Dirección por parte de la Secretaria General y en caso de capacitación será por parte del líder del proceso de gestión de la informática y la conectividad; por cuestiones financieras de la entidad no se logró la consolidación un contrato de continuidad laboral para la implementación del modelo.

Aunque se logró validar el modelo, no se logró su total implementación debido a que al iniciar con el proyecto la entidad no contaba con sus activos de información identificados, muchos de los procedimientos no estaban documentados la información del proceso de gestión de la informática y la conectividad no se encontraba centralizada ni existía un registro de la información vigente lo que necesitó la inversión de más tiempo del estimado. Cabe resaltar que el modelo de gestión de seguridad generado quedó adaptado a las necesidades de la corporación y de acuerdo a los requisitos de la norma para su eventual implementación como se sugiere en la "*Ruta para generar impacto"* de este trabajo. Todos los lineamientos que se deben tener en cuenta y los aspectos organizativos para ejecutar el modelo y sus derivados se encuentran contenidos en el ANEXO 1.

# CAPÍTULO V: RESULTADOS

## 5.1 RESULTADOS

- Los primeros resultados obtenidos se ven reflejados en el Capítulo I, Estado de la Seguridad de la Información y Diagnóstico de la situación problema, los cuales junto a la realización de las fases I y II permitieron establecer la línea base para el desarrollo de este trabajo.
- Se establecieron criterios de clasificación y medición de los impactos de riesgo sobre los activos de información de la Corporación, el documento generado fue clasificado como información reservada por lo que no se presenta como un anexo en este trabajo, pero de manera general es encuentra especificado en ANEXO 3. Es muy importante ya que la Corporación Nasa Kiwe no contaba con esta herramienta documentada.
- La entidad no disponía de una hoja de vida completa de sus equipos de cómputo, durante el desarrollo de este trabajo se estableció un modelo de formato y se realizó un inventario total de equipos con sus respectivas licencias de software y documentación legal que lo respaldan. Adicionalmente, se realizó la primera jornada de identificación y depuración de software no licenciado en estaciones de trabajo.
- Los resultados obtenidos que dan cumplimiento a la Fase III se ven reflejados en los Anexos: Anexo 1. Modelo de Seguridad y Privacidad de la Información, Anexo 2. Procedimiento de contacto con autoridades, Anexo 3. Procedimiento de Gestión de usuarios y contraseñas de acceso, Anexo 4. Formato solicitud y aprobación de cambios, Anexo 5. Guía para la Gestión y Clasificación de incidentes, Anexo 6. Formato de reporte, valoración y gestión de eventos e incidentes, Anexo 7. Formato de acceso a servicios informáticos, Anexo 8. Políticas de Seguridad CNK que hacen parte de los entregables del presente trabajo, los cuales en su totalidad se encuentran listos para su implementación.

- La entidad no contaba con un documento completo basado en la norma ISO 27001, que incluyera los diferentes criterios que garantizan la seguridad de la información, por lo que el ANEXO 1 generado en este trabajo representa una guía completa con lineamientos que derivan en nuevos procedimientos y formatos nuevos con los que la entidad no contaba.
- Las actividades desarrolladas durante la Fase IV permitió obtener la aprobación del modelo, siendo así validada y aprobada la propuesta ante la Secretaria General de la Corporación Nasa Kiwe, sin embargo, la implementación no se llevó a cabo de acuerdo a las observaciones en los numerales *1.1, 1.5 y Fase 4 (actividad 4.4.5*) del presente documento.

Sin embargo, se evidencia que falta mucho para tener un proceso consolidado de manejo y seguridad de la información dentro de la entidad ya que no se cuenta con un experto certificado en Seguridad informática que avale, ejecute y haga seguimiento a los controles y procedimientos generados. Adicionalmente, por factores externos a la ejecución de este trabajo y a las condiciones financieras, organizativas, de tiempo y demás de la entidad, no fue posible la puesta en marcha del modelo, pero se crea una *ruta de implementación*, la cual se apoya en el uso de todos los anexos generados en este trabajo acorde a la norma 27001, 27002 y que permitirá su ejecución a futuro.

***Ruta de implementación para generar el impacto esperado***

- Validar y adoptar los lineamientos y procedimientos propuestos en los ANEXOS 1, 2, 3, 4, 5, 6, 7 y 8 de este trabajo.

- Implementar del procedimiento de identificación y clasificación de activos de información, el cual se encuentra en proceso de elaboración por parte de un ente externo y así dirigir los esfuerzos a la gestión de riesgos identificando, evitando o mitigando las pérdidas e impactos desafortunados sobre el desarrollo de las actividades dentro de la entidad.

- Priorizar la medición del impacto sobre todos los activos de información, por lo que desde la dirección se debe garantizar la disposición de propietarios y custodios de los activos.

- Poner en marcha procedimientos para dar respuesta a incidentes de seguridad mediante el uso de los ANEXOS 3, 4 y 7.

- Formular Plan de tratamiento de riesgos para ser gestionados adecuadamente utilizando el ANEXO 1 y 3 de este trabajo para brindar la atención adecuada y evitar su materialización.

- Implementar del plan de tratamiento de riesgos (controles) y definir instrumento de medición de eficacia de controles según criterio del experto en seguridad informática.

- El uso adecuado y completo del modelo y todos sus derivados permitiría mejorar los procesos en la entidad, identificar oportunamente vulnerabilidades, cumplir con requisitos de administración pública, agilizar las tareas a desarrollar desde la oficina de gestión de la informática y ejercer control en el cumplimiento de las políticas de seguridad. Del acatamiento del modelo depende evitar impactos negativos para la entidad de tipo financiero, legal, reputación o afectación de la imagen corporativa.

- Para que el modelo tenga el impacto esperado requiere la inclusión de los funcionarios en la ejecución de los procedimientos dirigidos a fomentar buenas prácticas de seguridad de la información dentro de la entidad y con terceros, este empoderamiento del factor humano es el compromiso más grande para el éxito en la implementación del modelo mediante la distribución de roles y responsabilidades (ANEXO 1), apartado 6.1 Organización interna), este anexo da la guía y lineamientos para la implementación del modelo teniendo encuentra los diferentes aspectos.

- Implementar el plan de entrenamiento, capacitación y sensibilización dentro de la entidad.

- Una vez establecida la fase de implementación es necesario de la mano del experto contar con las fases de Seguimiento y revisión, Mantenimiento y mejora, con sus respectivas actividades, roles y responsabilidades.

# CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

## 6.1 CONCLUSIONES

- Este trabajo es fundamental para dar comienzo y cumplimiento a la implementación de un modelo de Gestión de Seguridad de la Información planteado para las entidades públicas dentro de la estrategia Gobierno Digital
- La norma ISO 27001 e ISO 27002, ayudan a orientar los esfuerzos hacia la realización de actividades y controles claves para minimizar los riesgos sobre la información y los sistemas informáticos dentro de una organización.
- Los lineamientos dados en la ISO 27002 brindan una guía de adaptación de la norma a cualquier tipo de organización ya que no son de obligatorio cumplimiento cuando no se busca una certificación.
- No contar con un inventario de activos representa un riesgo para la seguridad de toda la información de la entidad. La aplicación de controles y políticas se ve limitado cuando se realizan actividades de gestión de riesgo sobre activos no clasificados.
- Mediante el diseño de un modelo de gestión de seguridad de la información es posible identificar puntos débiles que puedan comprometer los intereses de una entidad y establecer mecanismos de mejora continua.

  Llevar a cabo un modelo de seguridad exitoso requiere de una participación activa por parte de todos los usuarios y la elaboración de un plan de capacitación en buenas prácticas de seguridad informática que fomente la integridad, disponibilidad y confidencialidad de los activos de información.

## 6.2 RECOMENDACIONES

- Partiendo de los controles ya identificados y de los procedimientos elaborados que no se encontraban disponibles o actualizados, la Corporación requiere de su implementación para dar cumplimiento a la

norma y la reglamentación colombiana. Desafortunadamente el proceso de gestión de la informática y la conectividad no cuenta con el personal suficiente para mantener la independencia de los roles al momento de ejecutar el modelo, por lo que se sugiere involucrar activamente la Dirección general para garantizar ya sea el apoyo permanente o la disponibilidad de personal de apoyo.

- En la ejecución de cualquier proyecto es vital el factor humano, para adoptar buenas prácticas de seguridad e implementar los procedimientos que involucran información sensible de la Corporación es necesario que la entidad brinde campañas de sensibilización y concienciación respecto a la seguridad de la información y los riesgos que podrían presentarse en caso de que esta se vea afectada. Además, este tipo de capacitaciones podrían generar un nivel mayor de propiedad y responsabilidad por parte de los funcionarios y usuarios hacia la entidad.

- Se requiere establecer un plan anual de capacitación, sensibilización y formación en buenas prácticas de seguridad de la información para los usuarios (funcionarios, contratistas y demás interesados).

- La entidad tiene disponibles procedimientos y formatos para hacer un correcto tránsito de los activos dentro de la entidad, pero no están siendo aplicados en su totalidad, por lo que se recomienda mayor divulgación y control sobre estos.

- No está demás recalcar como se manifiesta en el dominio “Aspectos organizativos de la seguridad de la información”, sección “Organización Interna”, ANEXO 1 de este trabajo, es fundamental el compromiso por parte de los involucrados y la asignación de responsabilidad, ya sea desde el proceso de gestión de la informática y la conectividad, la Dirección o los

comités de seguridad que se decidan conformar, ya que al no tener el respaldo continuo el modelo podría fracasar.

- Se requiere hacer un inventario de activos para cada proceso y designar custodios para su actualización.

- Se evidencia la necesidad de unificar de la información del Almacén respecto a las licencias de software activas y los equipos en función para garantizar la continuidad de soporte y garantía por parte de los proveedores.

- El procedimiento y guía para la gestión de incidentes de seguridad es uno de los más extensos e importantes para garantizar la continuidad de las operaciones en la Corporación, se recomienda incluir y aprobar la herramienta de reporte, valoración y gestión de los eventos e incidencias de seguridad de la información.

- Las sugerencias, lineamientos, políticas y procedimientos definidos en este trabajo dependen del nivel de compromiso de la entidad y sus interesados, por lo que se sugiere establecer criterios de medición para evaluar su nivel de cumplimiento.

# BIBLIOGRAFÍA

[1] Corporación Nasa Kiwe, “Historia.” [Online]. Available: http://www.nasakiwe.gov.co/la-corporacion/historia/.

[2] AGESIC, “Vivimos en una nueva era: la era digital,” 2017. [Online]. Available: https://www.agesic.gub.uy/innovaportal/v/5793/31/agesic/vivimos-en-una-nueva-era:-la-era-digital.html?padre=5792&idPadre=5792. [Accessed: 30-Aug-2018].

[3] Symantec, “TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE,” 2014.

[4] “Ley estatuaria 1581,” 2012.

[5] C. de la República, “Ley 1712 de transparencia y del derecho a la información pública nacional,” *6 Marzo 2014*, p. 14, 2014.

[6] ETITC, “Modelo de Seguridad de la Información (MSPI) y Sistema de Seguridad y Privacidad de la Información (SGSI).” [Online]. Available: http://www.itc.edu.co/es/nosotros/seguridad-informacion.

[7] MinTIC, “Modelo de Seguridad,” 2017. [Online]. Available: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

[8] Corporación Nasa Kiwe, “Caracterización Gestión Informática y Conectividad - Corporación Nasa Kiwe Nacional,” 2018. [Online]. Available: http://www.nasakiwe.gov.co/download/caracterizacion-gestion-informatica-y-conectividad/.

[9] I. M. A. Rodriguez and C. G. Gómez, “La información como recurso estratégico en las empresas de base tecnológica/Information as a strategic resource intechnology-based companies,” *Rev. Gen. Inf. y Doc.*, vol. 25, no. 2, pp. 265–285, 2015.

[10] J. Burgos Salazar and P. G. Campos, “Modelo Para Seguridad de la Información en TIC,” Concepción, 2009, pp. 234–253.

[11] Y. Zambrano Cedeño, “Plan informático para mejorar la gestión de seguridad de informacon del Gad Municipal Tosagua,” Universidad Regional Autónoma de los Andes, 2017.

[12] D. Santiago, G. J. Carlos, R. Gomes, A. Vergara Torres, I. Maria, and I.

Serrano, “Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala.”

[13] D. Felipe González *et al.*, “El riesgo y la falta de políticas de seguridad informática una amenaza en empresas certificadas,” Bogotá, 2014.

[14] M. Erice, “Ciberataque masivo,” 2017. [Online]. Available: https://www.abc.es/tecnologia/redes/abci-twitter-spotify-netflix-y-otras-webs-quedan-inutilizadas-ciberataque-masivo-201610211941_noticia.html.

[15] S. La rotta, “¿Por qué elsecuestro de datos se volvió un tema de todos los días?,” *Tecnología*, 2017. [Online]. Available: https://www.elespectador.com/tecnologia/por-que-el-secuestro-de-datos-se-volvio-un-tema-de-todos-los-dias-articulo-700279.

[16] BBC Mundo, “Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo,” *News*, 2017. [Online]. Available: https://www.bbc.com/mundo/noticias-internacional-40422053.

[17] iProfesional, “Detectan fallas en la protección de información ciudadana de EE.UU.,” *Tecnología*, 2018. [Online]. Available: https://www.iprofesional.com/tecnologia/272190-estados-unidos-seguridad-tecnologí-a-Detectan-fallas-en-la-proteccion-de-informacion-ciudadana-de-EEUU.

[18] D. C. Franco and C. D. Guerrero, “Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002,” in *Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*, 2013, p. 10.

[19] J. S. Borbón Sanabria, “Normas, estándares y buenas prácticas,” *Seguridad*, vol. 11, p. 5.

[20] G. Pallas, “Metodología de Implantacion de un SGSI en un grupo empresarial jerárquico,” Universidad de la Republica, 2010.

[21] MinTIC, “Manual para la implementación de la política de Gobierno Digital,” 2018.

[22] MinTIC, “Política de Gobierno Digital.” [Online]. Available: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html.

[23] J. Lucila Guerrero and L. Gómez Flórez, “Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional,” *ELSEVIER*, pp. 87–95, 2012.

[24] Corporación Nasa Kiwe, “Objetivos y Funciones,” 2017. [Online]. Available: http://www.nasakiwe.gov.co/la-corporacion/objetivos/.

[25] C. A. Muñoz Peña, “Ley de Transparencia y del Derecho de Acceso a la Información Pública,” Bogotá, 2015.

[26] República de Colombia, “Rendición de cuentas, un derecho de la ciudadanía - Función Pública.” [Online]. Available: http://www.funcionpublica.gov.co/preguntas-frecuentes/-/asset_publisher/sqxafjubsrEu/content/rendicion-de-cuentas-un-derecho-de-la-ciudadania/28585938.

[27] Caldas, “Política de Seguridad y Privacidad de la Información,” 2018.

[28] Universidad Veracruzana, “Seguridad de la información.” [Online]. Available: https://www.uv.mx/celulaode/seguridad-info/tema1.html.

[29] M. A. Mendoza, “Beneficios de la aplicación efectiva de políticas de seguridad,” 2014. [Online]. Available: https://www.welivesecurity.com/la-es/2014/07/25/beneficios-aplicacion-efectiva-politicas-de-seguridad/.

[30] Alcaldía Mayor de Bogotá, “Inventario de activos,” Bogotá, 2015.

[31] Presidencia de la República, *Gestor Normativo*. 2015.

[32] MinTIC, “Guía para la Implementación de Seguridad de la Información en,” Bogotá, 2016.

[33] New Technologie, “Política de Seguridad y Privacidad de la Información de la Gobernación de Nariño,” 2014. [Online]. Available: http://xn--nario-rta.gov.co/inicio/index.php/gobernacion/gestion-administrativa/planes-programas-y-politicas/502-politica-de-seguridad-y-privacidad-de-la-informacion.

[34] Universidad Distrital Francisco José de Caldas, “Política de Seguridad de la Información.”

[35] OBS BusinessSchool, “Seguridad de la información, un conocimiento imprescindible.” [Online]. Available: https://www.obs-edu.com/es/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible.

[36] MinTIC, “Lineamientos para la implementación del modelo de seguridad de la información 2.0,” Colombia, 2011.

[37] NormasISO, “ISO 27001 - Seguridad de la información.” [Online]. Available: https://www.normas-iso.com/iso-27001/.

[38] J. Burgos Salazar and P. Campos, “Modelo Para Seguridad de la Información en TIC,” Concepción.

[39] ISO 27000.ES, “Gestión de Seguridad de la Información,” 2012. [Online]. Available: http://www.iso27000.es/iso27000.html.

[40] ISOTools, “Norma ISO/IEC 27000,” *Calidad y Excelencia*, 2018. [Online]. Available: https://www.isotools.org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada/.

[41] ISOTools, “La familia de normas ISO 27000,” *Calidad y Excelencia*, 2015.

[Online]. Available: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/.

[42] NOTICEBORED, “Norma de certificación ISO/IEC 27001.” [Online]. Available: http://www.iso27001security.com/html/27001.html.

[43] ISO 27000.ES, “ISO/IEC 27002:2013.,” 2013.

[44] Invima, “POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN,” 2017.

[45] SGC, “Manual de Normas y Políticas de Seguridad Informática,” 2014.

[46] Corporación Nasa Kiwe, “Políticas de Seguridad - Políticas de Protección de Datos Personales.” [Online]. Available: http://www.nasakiwe.gov.co/politicas-de-seguridad-politicas-de-proteccion-de-datos-personales/.

[47] Presidencia de la República, “Transparencia y acceso a información pública,” 2017. [Online]. Available: http://es.presidencia.gov.co/AtencionCiudadana/transparencia-y-acceso-a-informacion-publica.

[48] S. I. Mariño and P. L. Alfonzo, “Implementación de SCRUM en el diseño del proyecto del Trabajo Final de Aplicación,” *Sci. Tech.*, vol. 19, no. 4, pp. 413–418, 2014.

[49] J. Torres, E. Arzuza, and O. Becerra, “Aplicación de la metodología Scrum para la optimización de procesos,” 2012.

[50] Corporación Nasa Kiwe, “Misión - Visión - Corporación Nasa Kiwe Nacional.” [Online]. Available: http://www.nasakiwe.gov.co/la-corporacion/mision-vision/.

[51] Corporación Nasa Kiwe, “Principios Orientadores.” [Online]. Available: http://www.nasakiwe.gov.co/la-corporacion/principios-orientadores/.

# ANEXOS

**ANEXO 1. Modelo de seguridad y privacidad de la información CNK.**

**ANEXO 2. Políticas de seguridad CNK.**

**ANEXO 3. Guía para la gestión y clasificación de incidentes.**

**ANEXO 4. Procedimiento de contacto con autoridades.**

**ANEXO 5. Procedimiento de gestión de usuarios y contraseñas de acceso.**

**ANEXO 6. Formato solicitud y aprobación de cambios.**

**ANEXO 7. Formato de reporte, valoración y gestión de eventos e incidentes.**

**ANEXO 8. Formato de acceso a servicios informáticos.**