MODELO DE GESTIÓN DE TRATAMIENTO DE LA INFORMACIÓN

PROYECTO

DEISY ESTHER CASTRO MÁRQUEZ
JORGE ALBERTO CAMARGO BARBOSA

Códigos

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

MODELO DE GESTIÓN DE TRATAMIENTO DE LA INFORMACIÓN

PROYECTO

DEISY ESTHER CASTRO MÁRQUEZ
JORGE ALBERTO CAMARGO BARBOSA
Códigos

Asesor(es)
Ing. Alejandro Castiblanco Caro

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firmas de los jurados

Bogotá, Junio de 2017.

Agradecimientos

Agradecemos a DIOS y la VIRGEN, a nuestros Padres, Familiares, Compañeros, Amigos y al Cuerpo Docente por su valioso apoyo en este proceso académico como parte del logro de nuestra vida personal, académica y profesional. Dedicado a ustedes.

ÍNDICE

TABLAS

FIGURAS

INTRODUCCIÓN

Toda empresa maneja información como parte fundamental en los procesos de su negocio, que finalmente se transforma en un valor tangible o intangible que puede ser de tipo económico, reputacional o legal, entre otros resultados esperados que pueden contribuir a surgir, mantenerse, ser sostenible y evolutiva de acuerdo a las necesidades actuales del mercado. De igual manera, toda empresa legalmente constituida se enfrenta al cumplimiento de muchos factores internos y externos como parte de la operación de su negocio con el objetivo de lograr su misión, visión, credibilidad de los clientes, y en especial, cumplir los requisitos legales que le aplican en su contexto empresarial, social, económico, político, entre otros. Por tal motivo, este trabajo contempla el estudio del tratamiento adecuado de la información en la organización como factor importante e indispensable para el desarrollo óptimo de las operaciones de su negocio, el cumplimiento de su misión y visión, en especial, en el cumplimiento de los requisitos legales que le aplican a la misma frente a la protección de datos, en especial, personales, datos crediticios y datos corporativos como manera conducente para preservar la integridad, disponibilidad y confidencialidad de la información basada en buenas prácticas establecidas en norma ISO 27001, COBIT, requisitos legales, entre otras que le apliquen.

A continuación de este escrito presentamos este proyecto como parte del desarrollo de una solución óptima que contribuya a la organización en el fortalecimiento y mantenimiento adecuado del tratamiento de la información en sus operaciones, en cumplimiento de su misión, visión y requisitos legales que le apliquen.

1. RESUMEN EJECUTIVO

El desarrollo de este proyecto contempla la definición de un Modelo de Gestión de Tratamiento de la Información a partir de teorías, buenas prácticas como COBIT, ITIL, ISO 27001, ISO 20000, ISO 19011 e ISO 9001 y requisitos legales vigentes sobre esta temática de las empresas contemplados en la Constitución Política de Colombia de 1991. Artículo 15 y 20, Ley 1266 de 2008, Ley 23 de 1982, Ley 527 de 1999, Ley 594 de 2000, Ley 1273 de 2009, Ley 1581 de 2012, Ley 1712 de 2014 y la Circular 042 de la Superintendencia Financiera de Colombia, entre otras.

El Modelo de Gestión de Tratamiento de la Información se encuentra conformado por varios componentes, que parten de tener unas partes interesadas (Clientes, Accionistas, Funcionarios Internos, Terceros Contratistas, Proveedores, Entes de Control), el cual ingresan información personal y corporativa en la organización, e igualmente, esperan el resultado de una salida apropiada del buen tratamiento de la información.

Como complemento a las entradas mencionadas de las partes interesadas, igualmente, se contemplan en el Modelo entradas relacionadas con la legislación, políticas internas y buenas prácticas del tratamiento de la información. Estas entradas pasan al cuerpo central del Modelo de GTI, generando una salidas de este proceso.

El cuerpo central del Modelo de Gestión de Tratamiento de la Información es concebido fundamentalmente de la aplicación de la gestión del tratamiento de la información soportado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), a nivel estratégico, táctico y operativo como parte de un proceso de mejora continua que apoyará a la organización en el cumplimiento de su misión, visión, objetivos y metas estratégicas, mostrándose como una empresa firme, segura y confiable en el tratamiento de su información a nivel corporativo y frente a sus partes interesadas. Igualmente, en este contexto del Modelo conforme a la operación del Ciclo PHVA,

en su fase del Planear, se establecen los diferentes planes relacionados con el diagnóstico, identificación de información clasificada, análisis de riesgos y de auditorías internas relacionadas con el tratamiento de la información. Estos planes se harán efectivos en la fase del Hacer en el cual se realizará el diagnóstico, se identificará la información clasificada, se analizarán y evaluarán los riesgos, y se realizarán las auditorías planeadas. Posteriormente, al ejecutar estas actividades se tomarán todos los resultados y se validarán en la etapa del Verificar, en la cual se validará el resultado del análisis diagnóstico, se validará la información clasificada, se validará la eficiencia de los controles como parte del análisis de riesgos, e igualmente, se validarán los hallazgos identificados de la auditoría interna realizada en la etapa del hacer. Posteriormente, una vez verificado los resultados de la etapa del verificar se procede establecer los planes de acción o de mejora pertinentes relacionados con el análisis diagnóstico, clasificación de la información, controles de riesgos y auditoría respectivamente.

Finalmente, Como resultado del proceso realizado en el Modelo de Gestión de Tratamiento de la Información se espera obtener como resultados o salidas, la satisfacción de las partes interesadas respecto a la información segura en cuanto a integridad, disponibilidad y confidencialidad, el cual genera confianza en los mismos, e igualmente, el cumplimiento de requisitos legales o regulatorios y cumplimiento de políticas internas de la organización.

Es importante rescatar de este modelo que todo está soportado en la cultura organizacional en tratamiento de la información que se va generando a través del tiempo como parte de la experiencia que va dejando el recorrido de los ciclos PHVA del Modelo como parte de la madurez en este proceso.

Este Modelo es una propuesta que se propone a la organización como apoyo fundamental en un adecuado tratamiento de la información, el cual le va a permitir fortalecer no solo el cumplimiento de los requisitos legales vigentes en la materia, si no generar una cultura organizacional en el tratamiento de la información en todos

sus procesos, áreas y recurso humano, mostrándose como empresa sólida en el manejo de sus operaciones con un tratamiento de información confiable y eficiente de cara a sus partes interesadas, especialmente en sus clientes.

2. JUSTIFICACIÓN

En las empresas aún hoy en día es normal encontrar que no se tenga un control adecuado para el manejo de la información, y que este no se encuentre direccionado en las áreas y en sus operaciones como parte del cumplimiento de su misión y visión empresarial. En otras palabras, en muchas empresas aún no perciben la información como un activo de vital importancia en el funcionamiento de la misma, pues realmente las empresas sin información difícilmente existirán. Toda empresa se compone de información que se crea, se procesa, se transforma, se genera, se conserva, se almacena o custodia, dentro de otras características que hacen parte de ese gran proceso que debe existir para que se puedan realizar actividades en la misma, que puedan conllevar al cumplimiento de sus objetivos o metas establecidas. De esta manera, toda organización requiere de un adecuado tratamiento de la información, de no hacerlo al estar expuesta a amenazas podría conllevar a la organización a pérdidas económicas, pérdidas de imagen corporativa, incumplimientos contractuales y sanciones legales de la organización.

Como parte de esta problemática se requiere fortalecer el tratamiento adecuado de la información en las organizaciones con el fin de blindarlas y protegerlas de amenazas que puedan afectar los intereses de su negocio. Por tal motivo, a través de este estudio se propone diseñar un modelo de gestión de tratamiento de la información como herramienta para la organización en razón de cumplir su misión, visión y requisitos legales relacionados con la protección de datos en las organizaciones.

3. MARCO TEÓRICO Y REFERENTES

3.1 BUENAS PRÁCTICAS DE TRATAMIENTO DE LA INFORMACIÓN

De acuerdo a las buenas prácticas identificadas para implementarlas en el desarrollo del tratamiento de la información de este proyecto se encuentran las relacionadas a continuación:

- Cobit 5: Marco de referencia que permite alinear el Gobierno con las Tecnologías de la Información aplicando acciones para llegar al nivel de madurez deseado para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- ITIL: Estándar utilizado para administrar los servicios tecnológicos y salvaguardar la protección de la información.

- ISO 27001: Norma utilizada para gestionar la Seguridad de la Información.

- ISO 20000: Norma utilizada para Gestionar los servicios de Tecnologías de la Información.

- ISO 19011: Norma que definen pautas para llevar a cabo auditorías de los Sistemas de Gestión.

- ISO 9001: Norma utilizada para aplicar acciones que permitan medir el nivel de madurez en un Sistema de Gestión de Calidad.

3.2 REQUISITOS LEGALES DE TRATAMIENTO DE LA INFORMACIÓN

El marco legal identificado para el tratamiento de la información en las organizaciones a nivel interno y externo se fundamenta en lo siguiente:

- Constitución Política de Colombia de 1991. Artículo 15 y 20.

- Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 23 de 1982. Ley de Derechos de Autor.

- Ley 44 de 1993. Modificación y adición de la Ley 23 de 1982. Ley de Derechos de Autor.

- Ley 527 de 1999. Ley de acceso y uso de los mensajes de datos, del correo electrónico y firmas digitales.

- Ley 594 de 2000. Ley general de archivos.

- Ley 1273 de 2009. Ley de Protección de la Información y de los Datos.

- Ley 1520 de 2012, por la cual se establece la responsabilidad por infracciones al derecho de autor y los derechos conexos en Internet.

- Ley 1581 de 2012. Ley de Protección de los datos personales.

- Ley 1712 de 2014. Ley de Transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- Circular 042 de la Superintendencia Financiera de Colombia. Capítulo décimo segundo: requerimientos mínimos de seguridad y calidad para la realización de operaciones.

4. METODOLOGÍA

En el desarrollo de la Gestión de Tratamiento de la Información para la organización se ha contemplado una metodología de tipo investigativa mediante la identificación, estudio, análisis y generación de conocimiento a partir de teorías, buenas prácticas y requisitos legales vigentes en tratamiento de la información, complementada con estudio evaluativo inicialmente, en la cual conlleva a la identificación de aquellos elementos que dispone o le hacen falta a la empresa para lograr establecer un modelo que le permita gestionar adecuadamente el tratamiento de la información en cumplimiento de su misión, visión, objetivos y metas estratégicas. De esta manera, a continuación se describe la metodología utilizada para llevar a cabo este proyecto:

1. Identificación de teorías y buenas prácticas del tratamiento de la información.
2. Identificación de requisitos legales vigentes en tratamiento de la información.
3. Desarrollo y elaboración de herramienta diagnóstica que permita identificar el estado actual de cumplimiento de la organización del tratamiento de la información.
4. Definición de elementos de tratamiento de la información necesarios para el modelo de gestión.
5. Definición del Modelo de Gestión de Tratamiento de la Información.

5. RESULTADOS Y DISCUSIÓN

ENTREGABLE 1 Objetivo 1 de Proyecto

5.1 DEFINICIÓN DE LA HERRAMIENTA DIAGNÓSTICA DE CUMPLIMIENTO DE TRATAMIENTO DE LA INFORMACIÓN

5.1.1 Herramienta Diagnóstica de Cumplimiento de Tratamiento de la información

Para realizar el estudio diagnóstico sobre el tratamiento de la información en la organización fue necesario diseñar una herramienta que permita conocer el estado actual de cumplimiento de la misma frente a la temática presentada en este proyecto (Ver Anexo 1).

ENTREGABLE 2 Objetivo 2 de Proyecto

5.2 ELEMENTOS DE GESTIÓN DE TRATAMIENTO DE LA INFORMACIÓN

5.2.1 Política de Tratamiento de la Información

La organización gestiona el tratamiento de la información en cumplimiento de su misión, visión, objetivos y metas estratégicas como parte de la satisfacción de sus partes interesadas, asegurando su calidad, seguridad y eficiencia en el control de los riesgos de la misma en todos sus procesos fomentando una cultura organizacional con base al compromiso por parte de todo su personal a nivel estratégico, táctico y operativo, e implementado las medidas necesarias en todos sus activos de información, el cual la hacen una organización confiable, estable y sostenible.

5.2.1.1 Recolección de la Información

En la organización se recolectará la información conforme a los canales establecidos y a los responsables o encargados autorizados.

5.2.1.2 Definición de los Canales de la Información

En la organización se identificarán y establecerán los canales autorizados para recolectar la información. De esta manera, se considerarán canales internos y externos:

Canales Externos

- Puntos de atención (Sucursales).
- Canales telefónicos.
- Páginas web de la empresa.

Canales Internos

- Áreas de la organización.
- Intranet.

5.2.1.3 *Identificación de la Información*

En la organización se identificará toda la información que hace parte de la misma, y que se maneja en todos sus procesos. Así se identificará la siguiente información:

- Información relacionada con datos personales.
- Información corporativa y organizacional (misión, visión, procesos, etc).
- Información financiera.

- Información tecnológica (relacionada con el hardware y software).
- Información jurídica, legal y normativa.
- Información contable.
- Información de riesgos.
- Información de recursos humanos.

5.2.1.4 Definición de la Finalidad del Tratamiento de la Información

Para cada tipo de información en la organización se establecerá la finalidad para la cual se utiliza y/o se le da el tratamiento a la misma.

5.2.1.5 Autorización del Tratamiento de la Información

Toda información en la organización deberá partir de una autorización previa de su titular (en el caso de datos personales), o en su defecto de los propietarios de la misma en la organización.

5.2.1.6 Definición y Clasificación de las Bases de Datos

En la organización se definirá y clasificarán todas las bases de datos. De esta manera, se establecerá la siguiente información:

- Nombre de la base de datos.
- Tipo de información que contiene la base de datos.
- Descripción de la finalidad de la base de datos.
- Clasificación de la información.
- Fecha de establecimiento de la base de datos.
- Cantidad de registros de la base de datos.
- Medio de almacenamiento de la base de datos.
- Tiempo de retención de la información de la base de datos.

- Legislación y normativa que ampara la base de datos.

5.2.1.7 Registros de las Bases de Datos

Toda base de datos de la organización deberá disponer de registros de la misma a nivel interno. Igualmente, a nivel externo se registrarán en los diferentes entes de control que lo requieran de acuerdo a la legislación vigente.

5.2.1.8 Definición, Clasificación y Control de Acceso de Responsables y Encargados del Tratamiento de la Información

Toda la información en la organización deberá tener definidos unos responsables o encargados del tratamiento de la misma. De esta manera, se definirá, se clasificará y se establecerán los controles de acceso permitidas al personal autorizado. Conforme a lo anterior, se definirán los permisos de escritura, lectura, eliminación o supresión de la misma.

5.2.2 Objetivos del Modelo de Gestión de Tratamiento de la Información

5.2.2.1 Objetivo General

Llevar un control de tratamiento de la información en todo su ciclo de vida durante todas operaciones de la organización, en razón de cumplir su misión, visión y requisitos legales vigentes establecidos.

5.2.2.2 Objetivos Específicos

- Proporcionar información íntegra durante todo su ciclo de vida en la organización.

- Asegurar la confidencialidad y disponibilidad de la información de las investigaciones de tal manera que sea accedida por las partes interesadas y el personal autorizado que se encuentre disponible oportunamente.

- Cumplir requisitos legales con el fin de evitar pérdidas económicas, pérdidas de imagen y sanciones a la empresa.

5.2.3 Alcance del Modelo de Gestión de Tratamiento de la Información

El Modelo de Gestión de Tratamiento de la Información aplica a todo el contexto de la organización. Considerando lo anterior se describe detalladamente su aplicación:

- Aplica a todos los activos de información.
- Aplica a toda la información de la la organización, cualquiera sea su clasificación y representación de la misma (física, electrónica, verbal y cognitiva).
- Aplica a todos los contenedores de la información.
- Aplica a todo el recurso humano que hace parte de la organización.
- Aplica a toda la legislación y normatividad aplicable a la organización.
- Aplica a la misión y a la visión de la organización.
- Aplica a todos los procesos de la organización.
- Aplica a toda la información en todos sus niveles (estratégico, táctico u operativo).
- Aplica a todas las áreas y sedes de la empresa cualquiera sea su ubicación.
- Aplica a todo tercero encargado de tratamiento de la información.

5.2.4 Organización y Estructura del Tratamiento de la Información

Como parte de la Gestión de Tratamiento de la Información en la Organización se organiza y se estructura de acuerdo a su estructura organizacional y funciones en la organización. De acuerdo a lo anterior, se propone la siguiente organización y estructura para gestionar el tratamiento de la información:

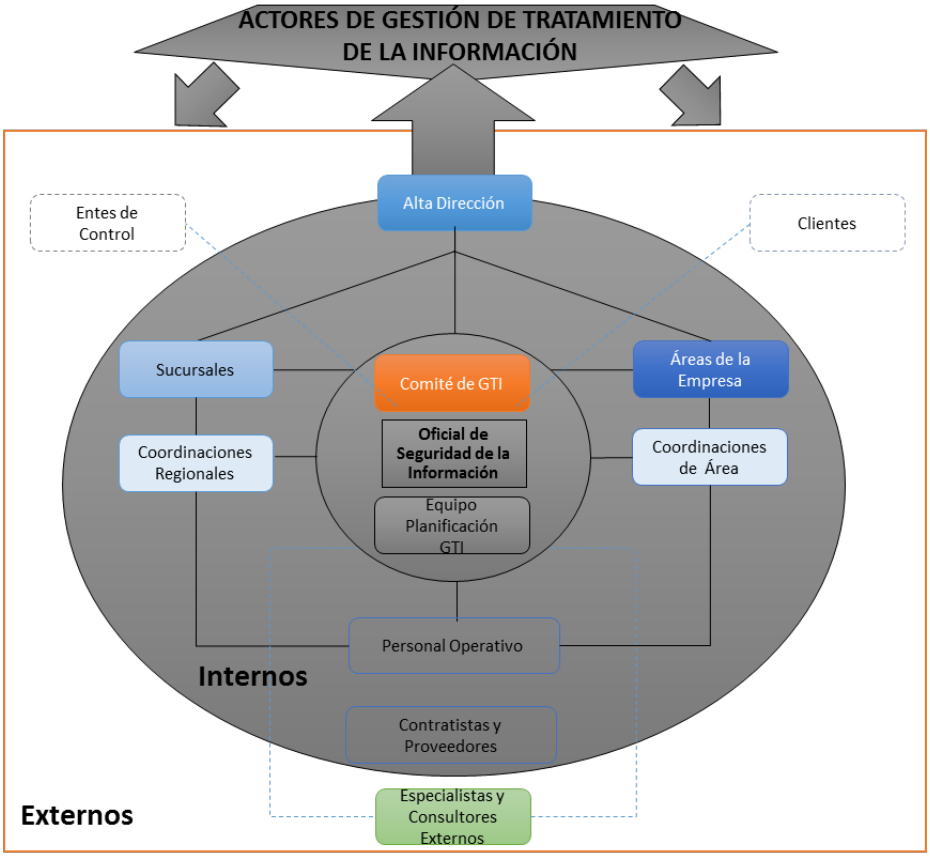

Figura 1. Actores de Gestión de Tratamiento de la Información.

5.2.4.1 *Esquema de estructura del comité de gestión de seguridad de la información*

Considerando las buenas prácticas de seguridad de la información y la estructura organizacional, el comité de gestión de tratamiento de la información se conformará de la siguiente manera:

- Gerente General.
- Oficial de Seguridad de la Información.
- Jefe de Control Interno.
- Jefe Jurídico.
- Jefe de Planeación.
- Director de Gestión de la Información.
- Representante de Tecnologías de la Información.
- Representante de Recursos Humanos.
- Representante de Servicios Administrativos.

5.2.5 Gestión de Riesgos de la Información

5.2.5.1 Compromiso de la Dirección General con la Gestión de Riesgo de Seguridad de la Información

La Alta Dirección de la organización debe asumir el compromiso con la gestión de riesgo en toda la organización como parte fundamental en el desarrollo y optimización de los activos de información en cumplimiento de la misión y visión organizacional. De acuerdo a lo anterior, define una metodología de gestión de riesgos de seguridad de la información que debe ser implementada en toda la organización.

5.2.5.2 *Estrategias de la Gestión de Riesgos de Seguridad de la Información*

La Alta Dirección de la organización como parte del éxito de la gestión de riesgos de seguridad de la información debe establecer las siguientes estrategias:

- **A corto plazo**

  - Establecimiento de la metodología de gestión de riesgo de seguridad de la información.
  - Levantamiento de los activos de información.
  - Clasificación de los activos de información e identificación de los más críticos para la operación del negocio.

- **A mediano plazo**

  - Evaluación de los riesgos identificados (comenzando por los más críticos).
  - Definir y mantener actualizado el mapa de riesgos de seguridad la información de la organización.
  - Implementación de controles que mitiguen los riesgos y apoyen el cumplimiento de la misión y visión de la organización.
  - Implementación y seguimiento a planes de tratamiento.
  - Definición de indicadores de gestión de riesgos con el fin de medir la eficiencia en este proceso.
  - Capacitar al personal en la gestión de riesgos.

- **A largo plazo**

  - Fomentar la cultura organizacional en la gestión de riesgos de seguridad de la información.
  - Actualizar la matriz mapa de riesgos.

5.2.5.3 Objetivo de la Gestión de Riesgos

Gestionar los riesgos de seguridad de la información que se presenten en las operaciones de la organización.

5.2.5.4 Alcance de la Gestión de Riesgos

La gestión de riesgos en la organización aplica todos los activos de información, en especial a los más críticos. Igualmente, aplica a todos los propietarios o responsables de los activos de información.

5.2.5.5 Organización de la Gestión de Riesgos

Previamente a la definición de la metodología de gestión de riesgos se definirá el comité de gestión de riesgos.

5.2.5.6 Comité de Gestión de Riesgos

Inicialmente se propone crear el Comité de Gestión de riesgos como ente encargado de evaluar, tomar decisiones e implementar estrategias y controles o medidas que permitan mitigar los riesgos en la organización.

5.2.5.7 Definición de los Indicadores de la Gestión de Riesgos

Para la gestión de riesgos de la organización se definen los siguientes indicadores:

- Número de riesgos materializados por mes.
- Número de riesgos tratados por mes.
- Número de riesgos aceptados.
- Número de riesgos mitigados.

5.2.5.8 Plan de Auditoría de Gestión de Riesgo

Se define un plan de auditoría que permita monitorear y llevar un control de la gestión de riesgos en la organización.

5.2.5.9 Plan de Mejora Continua de Gestión de Riesgo

Se define un plan de mejora continua, como producto de la implementación del plan de auditoría previamente, con el fin de realizar acciones preventivas, correctivas y de mejoras al proceso de gestión de riesgo de la organización.

5.2.5.10 Metodología de Análisis de Riesgos de Seguridad de la Información

Como parte del Modelo de Gestión de Tratamiento de la Información se define la metodología de análisis de riesgos de seguridad de la información, como un proceso iterativo conformado por una serie de pasos ejecutados secuencialmente que permiten una mejora continua para la toma de decisiones para la organización, en el cual se minimicen pérdidas y se maximicen oportunidades. De acuerdo a lo anterior, para esta metodología se tomará como referencia modelo de gestión de riesgos de la Norma ISO 27005, como base para el diseño de la metodología adaptada a su organización:

La metodología de análisis de riesgos de seguridad de la información se propone como parte operativa con el fin de valorar cualitativamente y cuantitativamente el nivel de riesgo que presentan los activos de información. De esta manera, esta metodología hace parte del procedimiento de valoración, evaluación y tratamiento de riesgos de seguridad de la información para la organización.

Pasos de la Metodología de Gestión de Riesgos

La metodología de análisis de riesgos contempla las siguientes actividades:

i. Establecer el contexto de riesgos.
ii. Identificar los activos de información.
iii. Valorizar los activos de información.
iv. Identificar los riesgos, amenazas y vulnerabilidades.
v. Analizar los riesgos.
vi. Evaluar los riesgos.
vii. Tratar los riesgos.
viii. Monitorear y revisar todo el proceso de gestión de riesgo.
ix. Comunicar y consultar los resultados de cada una de las fases del proceso de gestión de riesgo.
x. Documentación.

i. Contexto del riesgo

Se determinará el contexto del riesgo a nivel estratégico, organizacional y de gestión del mismo con el fin de tomar decisiones sobre la implementación de medidas que permitan mitigarlos y llevarlos a un nivel mínimo aceptable. De esta manera, especialmente se identificarán los procesos que se van evaluar, iniciando por los más críticos.

Esta metodología de análisis de riesgo, se desarrolla considerando el contexto de la organización, enfocada en su misión, visión, funciones, su estructura organizacional, normatividad legal y el modelo de procesos de la compañía. De esta manera, a continuación se describe la manera de establecer el contexto como base fundamental en la para gestionar los riesgos ajustada a la organización:

- Identificar y entender todo el contexto del negocio de la organización. Partiendo de su misión, visión, procesos, leyes aplicables, normatividad, estructura organizacional, funciones, objetivos, planes estratégicos, servicios que presta la empresa, entre otros factores que hagan parte de la misma.

- Identificar las partes interesadas del negocio de la organización a nivel interno y externo, incluyendo los entes de control de la misma.

Análisis del Contexto del Riesgo para la Organización

Una vez estudiada la organización, su misión, visión, su propósito principal, sus objetivos estratégicos, su estructura organizacional, mapa de procesos requerimientos legales, servicios prestados, sus partes interesadas, entre otros factores que la componen, se logra concebir a la organización como parte fundamental en el cual el tratamiento adecuado de la información que recolecta, genera, procesa, almacena, transfiere para emitir resultados que puedan aportar grandes beneficios a la sociedad. Razón por la cual hace a la empresa una importante institución en el cual a través de un adecuado tratamiento de la información en sus procesos y en el desarrollo de sus funciones le permite mantener un buen nombre a nivel corporativo (reputación), cumplir la legislación (requisitos legales), confiabilidad en sus clientes, entre otros factores asociados, especialmente, en lo que respecta a la calidad de la misma haciéndola efectiva, eficaz, confiable y segura, preservando su integridad, disponibilidad y confidencialidad. De esta manera, el contexto del riesgo para la organización fundamentalmente estará asociado al logro del cumplimiento de su misión, visión, objetivos y metas estratégicas definidas.

ii. Identificación de activos de información

En la organización inicialmente para aplicar el análisis de riesgos se identificarán todos los activos de información, sus propietarios, contenedores y custodios. De esta manera, la identificación de los activos se realizará de la siguiente manera:

- Se identifican los propietarios de cada activo.
- Se identifican los contenedores de los activos.
- Se identifican los custodios de los activos
- Se levantará el inventario de todos los activos de información que hacen parte de las operaciones de la organización.
- Se asociarán los activos que hacen parte de cada proceso.
- Se valoran los activos.
- De acuerdo a la valoración obtenida se identifican los activos más críticos de cada proceso.

Tipos de activos de información

Los activos de información de la organización se considerarán en los siguientes tipos:

Propietarios de los activos de información

En la organización serán considerados propietarios de los activos de información todo aquel funcionario como delegado o responsable de la información que maneja en su proceso. De acuerdo a lo anterior, son propietarios de los activos de información para la organización los siguientes:

- El presidente, gerente o jefe de la empresa.
- Jefes de área.
- Líderes de proceso.
- Otros que considere la empresa.

Inventario Propietarios de Activos de Información

Como parte importante para el apoyo en la identificación de los propietarios de activos de información, se recomienda definir un inventario de los activos de información con cada uno de sus propietarios. De esta manera, a continuación se propone un modelo de inventario de activos de información para la organización con su respectivo propietario de información.

ACTIVO DE INFORMACIÓN	PROPIETARIO DE LA INFORMACION
Activo 1	Propietario 1
Activo 2	
…	

Tabla1. Propuesta Propietarios de Activos de Información.

Contenedores de información

Los contenedores de la información para la organización se presentarán en los siguientes tipos:

- Contenedores de software

  En la organización los contenedores de software son todas aquellas aplicaciones, desarrollos, bases de datos, archivos electrónicos u programas electrónicos que hacen parte de la creación, procesamiento u almacenamiento de activos de información.

- Contenedores de hardware

  Los contenedores de hardware en la organización son los equipos o dispositivos en el cual se maneja o almacena cualquier tipo de información de la empresa.

- Contenedores físicos

  Los contenedores físicos en la organización se clasificarán en dos tipos:

  - Contenedores físicos electrónicos. Estos hará referencia a todo contenedor que almacene información a través de medios electrónicos como: usb, cd, dvd, discos duros externos, memorias sd, y cualquier tipo de medio de almacenamiento externo.

- Contenedores físicos impresos. Estos hacen referencia a todo contenedor representado especialmente en papel o cualquier medio impreso.

Custodio de la información

Los custodios de la información son aquellos usuarios autorizados para el uso de la misma. De esta manera, manera los custodios de la información en la organización son todos los funcionarios, contratistas o proveedores, visitantes y usuarios en general que tienen acceso autorizado a determinada información.

iii. Valoración de activos de información

Una vez identificados los activos de información que hacen parte de los procesos de la organización, se evaluarán los mismos, de tal manera que se le dará un nivel de clasificación de acuerdo al nivel de importancia en las operaciones de la organización. Cumpliendo con lo anterior, se establecen los siguientes criterios de valoración para los activos:

Valor	Clasificación	Valoración Cualitativa	Valoración Cuantitativa
1	Bajo	El activo proporciona una funcionalidad básica para la operación de la organización y en caso de existir afectación o pérdida del mismo podría generar una leve pérdida económica, reputacional o legal; y no afecta la continuidad del negocio.	El activo representa un valor menos del 0,5% del capital o patrimonio de la empresa.

2	Medio	El activo es importante para la operación de la organización y en caso de llegar a existir pérdida del mismo podría generar una moderada afectación económica, reputacional y legal; y puede llegar a afectar la continuidad del negocio.	El activo representa un valor entre el 0,5% y 2% del capital o patrimonio de la empresa.
3	Alto	El activo es muy importante para la operación de la organización y en caso de llegar a existir afectación o pérdida del mismo generaría alta pérdida económica, reputacional y legal; y puede llegar a afectar la continuidad del negocio.	El activo representa un valor entre el 3% y el 7% del capital o patrimonio de la empresa.
4	Crítico	El activo es de vital importancia para las operaciones de la organización y en caso de llegar a existir afectación o pérdida del mismo generaría extremas pérdidas económicas, reputacional y legal; y	El activo representa un valor mayor al 7% del capital o patrimonio de la empresa.

		afectaría la continuidad del negocio.	

Tabla 2. Valoración de Activos.

De acuerdo a los criterios establecidos, se define a continuación la clasificación del activo de acuerdo a su nivel de importancia considerando la siguiente ecuación:

CA = X

Ecuación de valoración de clasificación del activo.

CA: Clasificación del Activo.

X: Valor de clasificación del activo de acuerdo a los criterios establecidos.

iv. Identificación de Riesgos, Amenazas y Vulnerabilidades

Posteriormente, a la identificación de los activos de información se procede a identificar los riesgos, amenazas y vulnerabilidades que pueden generar un impacto en los mismos. En este caso se identificarán riesgo, vulnerabilidades y amenazas asociadas de diferentes eventos que se puedan presentar a nivel:

- Eventos naturales.
- Eventos físicos.
- Eventos informáticos.
- Eventos de Recurso Humano.

v. Análisis de Riesgos

Una vez identificadas las amenazas se procederá a realizar el análisis de los riesgos. Para esto, se evaluará la probabilidad de ocurrencia y el impacto

que pueden tener las mismas sobre los activos de información que hacen parte de las operaciones.

Criterios de Impactos

Como parte de la metodología para la organización se seleccionaron impactos relacionados con su contexto organizativo. De esta manera, a continuación se consideran los criterios de impacto:

Tipos de Impacto

Dentro de los criterios se establecen los diferentes tipos de impacto:

Tipo de Impacto	Descripción
Confidencialidad	Afectación en la seguridad de la información por acceso no autorizado.
Integridad	Afectación de la calidad de la información en las operaciones.
Disponibilidad	Afectación de las operaciones o en la continuidad del negocio.
Legal	Incumplimiento de requisitos legales, sanciones o penalizaciones.
Financiero	Pérdidas económicas el cual afecta el presupuesto de la empresa.
Reputacional	Afectación en la imagen corporativa.
Economía Nacional	Afectación de recursos de la nación.
Imagen de la Nación	Afectación de la imagen de la nación a nivel interno y externo.

Tabla 3. Tipos de Impacto.

Valoración del Impacto

Se determinará el nivel de impacto que las amenazas pueden afectar a los activos de información. De esta manera, se definen a continuación los siguientes criterios de valoración de los impactos:

Valor	Nivel	Valoración Cualitativa	Valoración Cuantitativa
1	Bajo	Impacto mínimo en los activos de información.	El impacto genera pérdidas económicas menores a 0,5% del capital o patrimonio de la empresa.
2	Medio	Impacto moderado en los activos de información.	El impacto genera pérdidas económicas entre el 0,5% y 2% del capital o patrimonio de la empresa.
3	Alto	Impacto alto en los activos de información.	El impacto genera pérdidas económicas entre el 3% y el 7% del capital o patrimonio de la empresa.
4	Extremo	Impacto grave en los activos de información.	El impacto genera pérdidas económicas entre el 7% y el 10% del capital o patrimonio de la empresa.
5	Catastrófico	Impacto crítico en los activos de información.	El impacto genera pérdidas económicas mayores al 10% del capital o patrimonio de la empresa.

Tabla 4. Criterios de niveles de Impacto.

Ref	Tipo de Impacto	NIVEL DE IMPACTO (*I*)				
		Bajo	Medio	Alto	Extremo	Catastrófico
1	.	1	2	3	4	5
2	.	1	2	3	4	5
3	.	1	2	3	4	5
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
N	.	.	.	.	.	.

Tabla 5. Registro de valoración por Impacto.

Criterios de Probabilidad de Ocurrencia de la Amenaza

La probabilidad de ocurrencia se valorará en función del número de veces que presente o se pueda presentar la afectación de una amenaza en los activos de información de la organización. De esta manera, se ha establecido los siguientes criterios de probabilidad de ocurrencia:

Nivel	Criterio	Descripción
1	Baja	Es poco probable que la amenaza pueda atacar el activo y vulnere los controles del mismo.
2	Media	Es probable que la amenaza pueda atacar el activo y vulnere los controles del mismo.
3	Alta	Es muy probable que la amenaza pueda atacar el activo y vulnere los controles del mismo.
4	Muy Alta	La amenaza frecuentemente puede atacar el activo y vulnerar los controles permanentemente.

5	Extremadamente Alta	La amenaza permanentemente puede atacar el activo y vulnerar los controles del mismo.

Tabla 6. Criterios de Probabilidad de Ocurrencia.

vi. Evaluación de riesgo

Luego de haber hecho el respectivo análisis de riesgo se procede a evaluar los riesgos identificados con el fin de determinar su nivel y así obtener los más críticos de ellos.

Nivel de riesgo del activo

En la organización se establecerá el nivel de riesgo por activo considerando la probabilidad de ocurrencia de amenazas y el impacto que pueden generar. De esta manera, se aplicará la siguiente operación:

$$NRA = PO*NI$$

NRA: Nivel de Riesgo del Activo.
PO: Probabilidad de Ocurrencia.
NI: Nivel de Impacto.

Considerando lo anterior, la operación para obtener el nivel de riesgo del activo se obtendrá a partir del producto de la probabilidad de ocurrencia (PO), por el nivel de impacto (NI).

Criterios de niveles de riesgo

De acuerdo al resultado obtenido del nivel de riesgo del activo se clasificará en los siguientes criterios de niveles de riesgo:

Escala	Criterio	Descripción
1-3	Riesgo Bajo	Riesgo aceptable
4-6	Riesgo Moderado	La materialización del riesgo puede impactar moderadamente las operaciones del negocio
8-12	Riesgo Extremo	La materialización del riesgo puede causar un impacto grave en las operaciones del negocio
15-25	Riesgo Crítico	La materialización del riesgo puede impactar las operaciones del negocio de manera crítica

Tabla 7. Criterios de Nivel de Riesgo

Nivel de aceptación del riesgo

De acuerdo al análisis del contexto de la organización de la organización, a factores legales, operacionales, tecnológicos, financieros y económicos se establece un nivel de riesgo aceptable para la organización menor o igual al riesgo bajo máximo en valoración de escala a 3. Esto contribuirá a mantener un margen mínimo de aceptación para la organización en el cual asegurará pérdidas económicas mínimas o insignificantes de acuerdo a su capitalización y patrimonio, e igualmente, a ninguna o poca probabilidad de sanciones penales por incumplimiento de requisitos legales, como también a mantener una imagen aceptable a nivel corporativo y de la nación entre otros impactos que podrían controlarse como parte de la preservación adecuada de la integridad, disponibilidad y confidencialidad de la información, siendo este el eje fundamental del negocio de proveer información confiable a sus clientes o partes interesadas.

Mapa de Riesgos

A continuación se establece el mapa de riesgos o de calor para la organización:

			IMPACTO				
			1	2	3	4	5
			Bajo	Medio	Alto	Extremo	Catastrófico
PROBABILIDAD	5	Extremadamente Alta	5	10	15	20	25
	4	Media	4	8	12	16	20
	3	Alta	3	6	9 R11	12	15
	2	Media	2	4	6 R6, R10	8 R7, R8, R9, R12	10 R1, R2
	1	Baja	1	2	3 R5	4	5 R3, R4

Figura 2. Mapa de Riesgos.

vii. Tratamiento de Riesgos

Los riesgos de la organización serán tratados considerando lo siguiente:

Seleccionar y aplicar controles

Se identificarán los controles existentes o nuevos para la mitigación del riesgo. Estos controles podrán ser seleccionados de normas NTC ISO/IEC 27001 en su Anexo A y en la NTC ISO/IEC 27002, de otras buenas prácticas o experiencias de la organización.

Valoración de controles

Los controles seleccionados se valorarán de acuerdo al costo beneficio de la organización de la organización, como parte fundamental en la mitigación de los riesgos asociados a los activos de información. De esta manera, se aplicarán los controles de acuerdo a lo establecido en los siguientes criterios:

Criterio Mitigación del Control	Valor
El control mitiga el 99% del riesgo	5
El control mitiga máximo el 70% del riesgo	4
El control mitiga máximo el 50% del riesgo	3
El control mitiga máximo el 20% del riesgo	2
El control no mitiga el riesgo	1

Tabla 8. Criterios de Valor del Control.

Costo de Implementación Control	Valoración
El costo del control supera más del 50% del valor del activo.	1
El costo del control equivale entre el 30% y 50% del valor del activo.	2
El costo del control equivale entre el 20% y el 30% del valor del activo.	3
El costo del control equivale entre el 10% y el 20% del valor del activo.	4
El costo del control equivale a menos del 10% del valor del activo.	5

Tabla 9. Criterios de Costo de Aplicación del Control.

Costo-Beneficio del Control

El costo beneficio del control será el resultado del producto del valor de mitigación del control por el costo de aplicación del control:

Criterio Costo Beneficio	Descripción Beneficio	Valoración Costo Beneficio	Recomendación
Óptimo	La aplicación del control mitiga el riesgo a un nivel mínimo riesgo aceptable y el costo de su implementación no superan el 10% del valor del activo.	**15-25**	La organización debe aplicar el control
Importante	La aplicación del control mitiga el riesgo a nivel mínimo moderado y el costo de su implementación no supera el 20% del valor activo.	**8-12**	La organización debe aplicar el control
Bajo	La aplicación del control mitiga el riesgo a nivel mínimo de riesgo extremo y el costo de su implementación se encuentra entre el 20% y el 50% del valor del activo.	**4-6**	La organización debe poner a consideración la aplicación o no del control
Insignificante	La aplicación del control no mitiga el riesgo y el costo de su implementación supera el 50% del activo.	**1-3**	La organización no debe aplicar el control

Tabla 10. Criterios de Costo-Beneficio de Aplicación del Control.

Valoración de la efectividad del control

En la organización se valorará la efectividad de los controles implementados considerando los siguientes criterios:

Criterio Efectividad Control	Escala	Descripción
Alta	4-5	• El costo del control es máximo del 10 % del valor del activo. • El tiempo de implementación del control es menor al establecido en el plan de tratamiento. • El control mitiga el riesgo y tiene un nivel de riesgo residual menor al nivel de riesgo inherente.
Media	3-4	• El costo del control es máximo del 20 % del valor del activo. • El tiempo de implementación del control es menor o igual al establecido en el plan de tratamiento. • El control mitiga el riesgo y tiene un nivel de riesgo residual menor al nivel de riesgo inherente.
Baja	2-3	• El costo del control es máximo del 50 % del valor del activo.

		• El tiempo de implementación del control es mayor al establecido en el plan de tratamiento. • El control mitiga el riesgo y tiene un nivel de riesgo residual menor o igual al nivel de riesgo inherente.
Mínima	1-2	• El costo del control es mayor al 50% del valor del activo. • El tiempo de implementación del control es mayor al establecido en el plan de tratamiento. • El control mitiga el riesgo y tiene un nivel de riesgo residual mayor al nivel de riesgo inherente.
Cero	0	• El costo del control es mayor al 70% del valor del activo. • El tiempo de implementación del control es excesivamente mayor al establecido en el plan de tratamiento. • El control no mitiga el riesgo.

Tabla 11. Criterios de Efectividad del Control.

Aplicación de controles

De acuerdo a los criterios de costo beneficio y efectividad en relación a la aplicación del control en la organización solo se aplicarán aquellos controles que representen un beneficio catalogado como “Óptimo” o “Importante” y que tengan un nivel de efectividad. De no tenerse proyectado este beneficio, en la organización se deberá identificar otro(s) control(es) que permitan mitigar el riesgo a una inversión adecuada para la organización.

Criterios de Tratamiento de Riesgos

Una vez obtenidos los resultados de la valoración y evaluación de riesgos para los activos de información debe implementarse el plan de tratamiento de riesgos con el fin de lograr mitigarlos. Se define a continuación, los criterios para el tratamiento de riesgos:

Criterios de Tratamiento de Riesgos de TI	
Tipo de Tratamiento	**Descripción**
Mitigar	El riesgo es tratado con recursos propios de la organización mediante la aplicación de controles.
Transferir	La organización no cuenta con los recursos, medios y/o personal especializado para mitigar el riesgo identificado. En este caso, el tratamiento del es remitido a un tercero o una empresa externa, con recursos y personal especializado para tratar el riesgo.
Aceptar	El riesgo es aceptado por la organización ya que no representa ser crítico y generar un impacto significativo en la seguridad de la información.

Tabla 12. Criterios de Tratamiento de Riesgos de TI.

Plan de tratamiento del riesgo

El plan de tratamiento del riesgo para la organización contemplará los siguientes factores:

- Los controles a implementar.
- Tipo de tratamiento del riesgo (mitigar, transferir, aceptar).
- Tiempo de implementación de controles.
- Costos de implementación de controles.
- Responsables de la implementación de controles.
- Supervisión de la aplicación del control.

*** **Nota:** *Los controles identificados se implementarán por prioridad de acuerdo al nivel de riesgo establecido (del más crítico al menos crítico).*

Riesgo Residual

El riesgo residual en la organización será el residuo que resulta de haber implementado los controles existentes o en producción. De esta manera, para conocer el riesgo residual se realizará nuevamente un análisis de riesgos, luego de haber implementado los controles establecidos sobre el riesgo inherente.

Consideraciones del Riesgo Residual

Sobre el riesgo residual se tendrán presentes las siguientes consideraciones:

- El riesgo residual será la diferencia entre haber o no implementado el control y la efectividad del mismo respecto al riesgo inherente.
- El riesgo residual resultará de haber realizado un nuevo análisis de riesgo.

- El riesgo residual contemplará un mapa de riesgos residual cumpliendo los criterios establecidos para evaluar el riesgo inherente. Es decir se utilizará misma estructura del mapa de riesgos inherente.
- El riesgo residual podrá ser tratado nuevamente si no llega al nivel de aceptación del riesgo establecido en la organización.
- Para obtener el riesgo residual se debe evaluar la eficiencia de los controles implementados sobre el riesgo inherente.

viii. Monitoreo y revisión

Se realizará un monitoreo contante de los riesgos detectados y de los Planes de tratamiento establecidos para los mismos, ya que los cambios en el entorno pueden generar variaciones en las prioridades de los riesgos y de esta forma los controles no pueden ser los más efectivos en un instante dado.

ix. Comunicación y consulta

La comunicación y consulta resultan de vital importancia en cada una de las fases del proceso de gestión de riesgos. Esta comunicación se hará bidireccional entre las partes interesadas y la consulta debe ser una prioridad.

Reportes de la gestión de riesgos

En la organización se presentarán a la Alta Dirección los resultados obtenidos de la gestión de riesgo, en el cual se mostrará como mínimo lo siguiente:

- Valoración del riesgo Inherente.
- Plan de tratamiento.
- Valoración del riesgo residual.

- Costo Beneficio de Implementación de Controles.

Fomentar la comunicación, participación y cultura organizacional

Para lograr una comunicación y una cultura organizacional en el personal de la organización se desarrollará un plan de comunicaciones que permita mantener informado a todo el personal sobre la gestión de riesgos. Igualmente, se desarrollarán capacitaciones y una serie de campañas publicitarias en la organización.

Formación y Sensibilización

En la organización se promoverá la formación y sensibilización de gestión de riesgos y seguridad de la información como parte de un proceso que fomentará la cultura organizacional en el manejo de los riesgos. Para lograrlo inicialmente se realizará lo siguiente:

- Validar la cultura actual en gestión de riesgos de seguridad de la información.
- Identificar las brechas entre lo actual y lo requerido.

Condiciones Generales:

- Contar con un presupuesto aprobado para las actividades de capacitación y entrenamiento.
- Los cambios tecnológicos, exigencias del mercado, cambios de normatividad y otras necesidades, podrán sugerir y solicitar capacitaciones adicionales.
- Todas las capacitaciones que sean realizadas directamente por la organización, deberán registrar la asistencia de los funcionarios en un formato de registro.
- Cuando se adquiera un sistema o aplicativo para la organización, debe contemplarse la capacitación a los funcionarios que lo utilicen, a fin de garantizar la Seguridad del mismo.

- Respecto al desarrollo de la cultura de organizacional en gestión del riesgo en seguridad de la información, el Encargado de la Seguridad de la Información, deberá conducir el programa de concienciación sobre esta temática de la organización focalizado a grupos de usuario, con el apoyo de los programas de capacitación y entrenamiento establecidos.
- El programa de concienciación en gestión del riesgo de seguridad de la información, debe estar acorde con la implementación de la Política de Seguridad de la Información de la organización revisándose continuamente para mantenerlo actualizado.

Las capacitaciones en Gestión del Riesgo de Seguridad de la Información, serán abordadas desde los siguientes frentes:

Metas	Instrumentos	Periodicidad
Mantener actualizado a los funcionarios de la organización, en los aspectos relacionados con la Gestión de Riesgos de Seguridad de la Información, así como la coyuntura e innovación al respecto.	**MEDIOS:** Boletín enviados por el Encargado de Seguridad de la Información. **CONTENIDO:** Incluir temas de interés de Seguridad de la Información.	Por lo menos 2 veces al año
INDUCCIÓN		
Dar a conocer la Estructura y Estrategia de Gestión de Riesgos Seguridad de la Información a los funcionarios de la	**MEDIOS:** Inducción organizacional y/o plataforma de E-learning.	Al ingreso a la organización.

organización, explicándoles cuales van a ser los roles generales frente a la gestión de riesgos de Seguridad de la Información, así como sus principales políticas.	**CONTENIDO:** Metodología de Gestión de Riesgos de Seguridad de la Información, conceptos básicos, Roles y Responsabilidades.	
CAPACITACIONES DE REFUERZOS		
Dar a conocer conceptos específicos asociados al buen funcionamiento de la gestión de riesgos de seguridad de la información	**MEDIOS:** Presentación presencial o plataforma E-learning. **CONTENIDO:** Conceptos específicos de Gestión de Riesgos de Seguridad de la Información, Roles y Responsabilidades.	Una (1) vez al año (tercer trimestre de cada año)

Tabla 13. Sensibilización.

Así mismo, las capacitaciones de Inducción y Refuerzo contaran con una evaluación que garantice que se cumplieron con los objetivos de las mismas, cuando los funcionarios no aprueben dicha evaluación deberán presentarlas nuevamente hasta que sean aprobadas.

x. Documentación

El proceso de Gestión de Riesgos en la organización será documentado en forma apropiada, esta documentación incluirá los métodos, fuentes de datos y resultados.

Estrategia de implementación del proyecto de gestión de riesgos en el en la organización

En la organización se sugieren las siguientes actividades para implementar la gestión de riesgos:

Actividades	Justificación
Sensibilizar y conseguir el compromiso a la Dirección de Despacho sobre la gestión de riesgos de seguridad de la información.	Se debe tener conciencia de la alta dirección y su compromiso para apoyar el proyecto de gestión de riesgos de seguridad de la información en la organización.
Designar el área o responsable de la gestión de riesgos de seguridad de la información	Es necesario designar el responsable de la gestión de riesgos de seguridad de la información, quién se encargará de liderar dicho proceso.
Conseguir los recursos para la implementación del proyecto de gestión de riesgos de seguridad de la información en la organización.	Se debe disponer de un presupuesto aprobado por la Dirección de Despacho para poder llevar a cabo el proyecto.
Designar un gestor de riesgos por área.	Un gestor se encargara de organizar y dirigir la actividad y el otro gestor se encargara de revisar-

	confirmar el resultado de la actividad en desarrollo.
Asignarles Roles al personal involucrado	De esta manera el personal tiene un rol asignado con el propósito de ayudar con la implementación y con las necesidades presentadas durante la gestión de riesgos.
Planear el proyecto de gestión de riesgos de seguridad de la información.	Se planeará el proyecto de gestión de riesgos de seguridad de la información de acuerdo a las necesidades en la organización.
Implementar el proyecto de gestión de riesgos de seguridad de la información.	Se implementará el proyecto de gestión de riesgos de seguridad de la información. Implementar la metodología de gestión de riesgos a los procesos de la organización, contemplando los activos de información, amenazas, vulnerabilidades, riesgos, impactos, probabilidad de ocurrencia, controles, riesgo residual, plan de tratamiento y demás elementos establecidos para este proceso.
Seguimiento al proyecto de gestión de riesgos de seguridad de la información.	Se realizará un monitoreo o seguimiento al cumplimiento de las actividades para llevar a cabo el proyecto.
Realizar mejoras al proyecto	Se establecerán las acciones preventivas, correctivas y de

	mejoras para llevar a cabo el proyecto cuando sea necesario.

Tabla 14. Estrategia de Implementación.

5.2.6 Clasificación de la Información

5.2.6.1 Esquema propuesto para identificación y clasificación de la información

En la organización se clasificará su información de acuerdo a su necesidad, prioridad, nivel de protección, sensibilidad, importancia y al cumplimiento de los requisitos legales que apliquen a la organización. Conforme a lo anterior, para la identificar y clasificar la información de la organización se propone el siguiente esquema de acuerdo a las buenas prácticas de seguridad de la información y a requisitos legales vigentes:

A. <u>Criterios de identificación y clasificación de la información</u>

La organización identificará y clasificará su información de acuerdo a su criterio de su valor, requisitos legales, sensibilidad, importancia, naturaleza jurídica, uso o tratamiento, control de acceso, riesgos, impactos, protección de datos, autoridades de control y responsabilidades de los funcionarios y terceros en determinados niveles de clasificación de la información establecidos. En cumplimiento de lo anterior, se definen los siguientes niveles de clasificación de la información:

B. <u>Niveles de clasificación de la información</u>

La información de la organización se clasificará de acuerdo a los siguientes niveles de clasificación establecidos para la organización:

I. Información Pública

II. Información Pública Clasificada:
   - Semiprivada
   - Privada

III. Información Pública Reservada o Confidencial.

I. Información Pública

De acuerdo a lo establecido en la Ley 1712 de 2014 (Ley de Transparencia) toda información calificada como tal según los mandatos de la ley o de la Constitución, que puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Se considera información pública los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.
En razón de lo anterior, la organización cumplirá lo establecido en la Ley mencionada, e igualmente define como información pública la siguiente:

- Información de la Organización

  - Convocatorias.
  - Productos y servicios.
  - Noticias.
  - Historia.
  - Marco estratégico.
  - Objetivos y funciones.
  - Estructura organizacional.
  - Información de las sedes.
  - Contactos.

- Directorios de entidades del sector.
- Directorio sectorial.
- Planes, presupuesto y gestión.
- Normatividad.
- Entes de control.
- Imagen institucional.
- Sistema de gestión institucional.

- Servicio al ciudadano

  - Preguntas y respuestas frecuentes.
  - Glosario.
  - Ayudas para navegar en el sitio.
  - Contactos, peticiones, quejas y reclamos.
  - Ofertas de empleo.
  - Política de tratamiento y protección de datos personales.

- PQRD

  - Formulario de contáctenos.
  - Informes de PQRD.

- Trámites y Servicios

  - Portafolios de servicios.
  - Trámites y servicios.

- Información de Contratación

- Publicaciones

- Información de contacto

II. Información Pública Clasificada

De acuerdo a la Ley 1712 (Ley de Transparencia), es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Semiprivada:

La información semi-privada, es aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

En este contexto y a otras disposiciones de la organización se considerará como información pública clasificada Semiprivada a:

- Información de seguridad social de los empleados.
- Información de comportamiento financiero de los empleados.
- Planes de trabajo.
- Información de registro de capacitaciones.

Privada:

La información privada, es aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

De esta manera, la organización define como información pública clasificada como Privada la siguiente:

- Inventario de activos de información.
- Políticas, Procedimientos, Instructivos y Registros.
- Datos personales que no sean sensibles (Dirección, Teléfono, entre otros), que se encuentren en las bases de datos.
- Bitácoras de registro de acceso a instalaciones.
- Información de incidentes.

III. Información Pública Reservada o Confidencial

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Se considera como Información Pública Reservada a la información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados

"datos sensibles"[20] o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.”

De acuerdo al cumplimiento de lo anterior y a otras disposiciones de la organización podrá considerar como información pública Reservada la siguiente:

- Nómina de los empleados.
- Datos sensibles (considerados en la Ley 1581 de 2012), de cualquier persona registrados en bases datos.
- Hojas de vida de las personas.
- Configuraciones de los sistemas de información.
- Matrices de riesgos.
- Informes y planes de tratamiento de pruebas de hacking ético.
- Informes de auditoría.

C. Directrices para clasificar la información

Todas las áreas de la organización son responsables y encargados de la información, mantenimiento y el nivel de seguridad de la misma.

D. Períodos para la Clasificación de la Información

En la organización todas las áreas actualizarán anualmente el inventario de clasificación de su información, lo enviarán y comunicarán al Comité de Seguridad de la Información para tener su aprobación. Posteriormente, publicarán el inventario de información clasificada al personal autorizado.

E. Etiquetado de la Información

Toda información de la organización de acuerdo al nivel de clasificación deberá ser etiquetada.

Las etiquetas se utilizarán para la información pública reservada e información pública clasificada (semiprivada y privada). La información pública no llevará etiqueta.

Toda información pública reservada e información pública clasificada (semiprivada y privada), que no se encuentre etiquetada, será considerada como información pública, lo que indica que puede ser accedida por cualquier persona. De esta manera, se determinará como un riesgo a ser tratado por el responsable de dicha información.

5.2.7 Documentación de Gestión de Tratamiento de la Información

Para la gestión del tratamiento de la información se considerará una estructura documental a nivel estratégico, táctico y operativo. De esta manera, a nivel estratégico se considerarán documentos relacionados con el plan estratégico y políticas; a nivel táctico se establecerán procedimientos, a nivel operativo se establecerán los instructivos y registros necesarios para la gestión del tratamiento de la información.

Nomenclatura para la Gestión de Tratamiento de la Información:

Nomenclatura	Descripción
MGTI	Modelo de Gestión de Tratamiento de la Información
GTI	Gestión de Tratamiento de la Información
PL	Plan
PO	Política
PR	Procedimiento
ME	Metodología
IN	Instructivo
RE	Registros - Formatos

Tabla 15. Nomenclatura de Gestión de Tratamiento de la Información.

5.2.7.1 Estructura Documental de GTI en Niveles de la Organización

Como parte de la estructura documental se establece en los niveles de la organización:

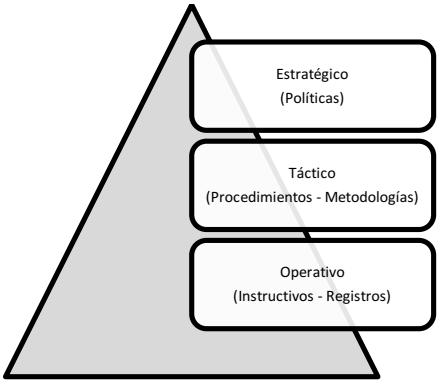

Figura 3. Estructura Documental de GTI en Niveles de la Organización.

La estructura documental de la Gestión de Tratamiento de la Información se establece en la organización a nivel estratégico, táctico y operativo. De esta manera, a nivel estratégico se desarrolla y direcciona en la organización la política de GTI, en el nivel táctico se definen los procedimientos o metodologías relacionadas con la GTI y en el nivel operativo se establecen los instructivos y registros pertinentes de GTI.

5.2.7.2 Aplicación Estructura Documental de GTI

La estructura documental en la Gestión de Tratamiento de la Información se aplicará de la siguiente manera:

Se definirá un código del documento de GTI conformado así:

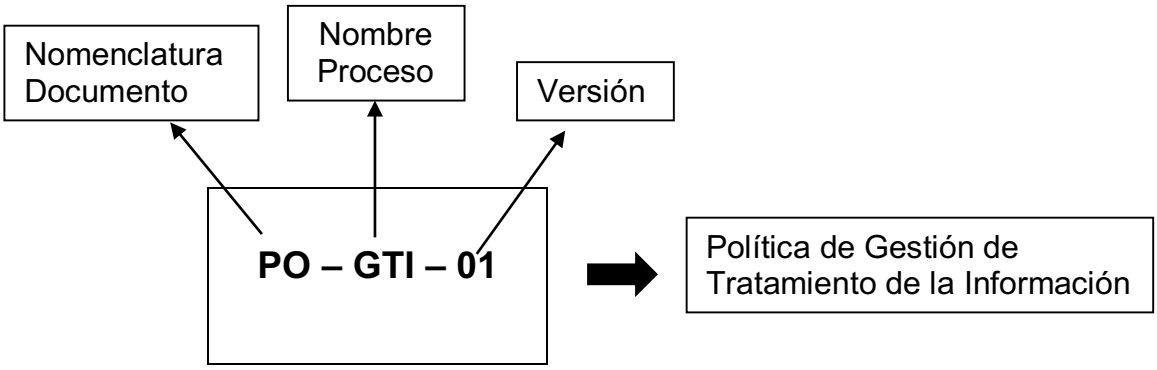

Figura 4. Aplicación Nomenclatura Documental.

De acuerdo a lo anterior, los diferentes documentos de la Gestión de Tratamiento de la Información se generarán así:

Documento	Nomenclatura
Plan	PL-GTI-01
Política	PO-GTI-01
Procedimiento	PR-GTI-01
Metodología	ME-GTI-01
Instructivo	IN-GTI-01
Registro - Formato	RE-GTI-01

Tabla 16. Nomenclatura Documentos GTI.

Nota:

*** Esta estructura documental propuesta para la Gestión de Tratamiento de la Información en cualquier organización se recomienda que vaya alineada con el control de documentos establecido en el Sistema de Gestión Documental.

5.2.8 Indicadores de Gestión de Tratamiento de la Información

La gestión de tratamiento de la información para su medición establece los siguientes indicadores:

Indicador	Descripción	Objetivo	Métrica
Autorización de la Información	Describe el porcentaje de la cantidad de autorizaciones de la información en un periodo de tiempo.	Medir el nivel de autorización de la información anualmente.	AI = (NA / IC) * 100 * 1año. AI: Autorización Información. NA: Número de Autorizaciones. IC: Información Clasificada.
Información Clasificada	Describe el porcentaje de la cantidad de información clasificada en un periodo de tiempo.	Medir la información clasificada anualmente.	IC = (NIC / IT) * 100 * 1año. IC: Información Clasificada. IT: Información Total.
Incidentes Reportados	Describe el porcentaje de la cantidad de incidentes reportados relacionados	Determinar el número de incidentes reportados de tratamiento de	IR = NRI / 1mes. IR: Incidentes Reportados de Tratamiento de la

	con la información en un periodo de tiempo.	la información mensualmente.	Información Información. NRI: Número de Reporte de Incidentes.
Incidentes Tratados	Describe el porcentaje del número de incidentes tratados de la información respecto a los reportados en un periodo de tiempo.	Determinar el porcentaje del número de incidentes tratados de la información respecto a los reportados mensualmente.	ITR = (NIT / NRI) * 100 * 1mes. ITR: Incidentes Tratados. NIT: Número de Incidentes Tratados. NRI: Número de Reporte de Incidentes.
Hallazgos de Auditoría	Describe la cantidad de hallazgos identificados como resultado de auditorías al tratamiento de la información en un periodo de tiempo determinado.	Determinar la cantidad de hallazgos de auditoría identificados del tratamiento de la información en un año.	HA = CHA / 1 año. HA: Hallazgos de Auditoría. CHA: Cantidad de Hallazgos.

Tratamiento de Hallazgos	Describe el porcentaje del número de hallazgos tratados de los identificados en un periodo de tiempo establecido.	Determinar el porcentaje de la cantidad de hallazgos tratados de los identificados en un periodo de un año.	TH = (NHT / NA) * 100 * 1 Año.
Riesgos Identificados	Describe la cantidad de riesgos de tratamiento de la información identificados en un periodo de tiempo determinado.	Determinar la cantidad de riesgos de tratamiento de la información identificados semestralmente.	RTI = NR / 1 Semestre. RI: Riesgos de Tratamiento de la Información NR: Número de Riesgos de Tratamiento de la Información.
Riesgos Tratados	Describe el porcentaje de riesgos tratados de los identificados en un periodo de tiempo.	Determinar el porcentaje de la la cantidad de riesgos de tratamiento de la información identificados semestralmente.	RT = (NRT / NR) * 100 * 1 Semestre. RT: Riesgos Tratados. NRT: Número de Riesgos Tratados.

Cumplimiento Requisitos Legales de Tratamiento de la Información.	Describe el cumplimiento de los requisitos legales vigentes de la organización.	Determinar el porcentaje de cumplimiento de los requisitos legales relacionados con el tratamiento de la información en un periodo mensual.	CRL = (RLC / NRLV)*100*1Mes CRL: Cumplimiento de Requisitos Legales. RLC: Requisitos Legales Cumplidos. NRLV: Número Requisitos Legales Vigentes.

Tabla 17. Indicadores de Gestión de Tratamiento de la Información.

5.2.9 Proceso de Auditoría de Gestión de Tratamiento de la Información

5.2.9.1 Objetivo General de la Auditoría

Llevar a cabo auditoría a la Gestión de Tratamiento de la Información en la organización con el fin de identificar el estado de cumplimiento de los requisitos legales y políticas vigentes establecidas y establecer mejoras que permitan salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información.

5.2.9.2 Objetivos Específicos de la Auditoría

- Evaluar la gestión efectuada por la organización frente al cumplimiento de las disposiciones de tratamiento de la información de acuerdo a lo establecido en la legislación vigente y políticas internas.

- Evaluar mecanismos de apoyo para la identificación y control de las disposiciones normativas que afectan las operaciones de la organización.

5.2.9.3 Alcance de la Auditoría

El alcance de la auditoría se establecerá en evaluar la implementación de la Gestión de Tratamiento de la Información tomando como base el cumplimiento de requisitos legales y normatividad interna vigente.

El alcance aplicará a toda la información de la organización que haga parte de sus operaciones.

5.2.9.4 Lineamientos de la Auditoría

La auditoría de la Gestión de Tratamiento de la Información considerará los siguientes parámetros o lineamientos:

- Se auditará la información identificada en la organización.

- Se realizará inicialmente un diagnóstico del cumplimiento del tratamiento de la información respecto al cumplimiento de la legislación y políticas internas vigentes en tratamiento de la información en la organización.
- Posteriormente se realizarán como mínimo una auditoría anual en tratamiento de la información.

- Se realizarán auditorías por proceso de la organización y por el tipo de clasificación de información establecida.

- Se identificarán hallazgos, observaciones y recomendaciones pertinentes al tratamiento de la información.

- Se realizará un informe preliminar y otro informe final sobre la auditoría realizada sobre el tratamiento de la información.

- Se comunicará a todos los responsables y encargados del tratamiento de la información los informes preliminares y finales como resultado de la auditoría realizada.

- Se hará seguimiento a los planes de mejora levantados como resultado de las auditorías realizadas en tratamiento de la información.

Nota:

***Igualmente, se estima conveniente realizar de manera anual revisión al programa de auditoría, y/o en la periodicidad establecida en la normatividad interna.

5.2.9.5 Procedimiento de Auditoría

La auditoría de Gestión de Tratamiento de la Información se realizará de acuerdo a las siguientes actividades definidas:

1. Informar y solicitar aprobación de la Alta Dirección para la realización de la Auditoría de Gestión de Tratamiento de la Información.
2. Reconocimiento actual de la organización.
3. Identificación de los procesos a auditar.
4. Identificación de responsable del proceso a auditar.
5. Identificación de la información del proceso a auditar.
6. Identificación del responsable y encargado del tratamiento de la información.
7. Identificación de la clasificación de la información del proceso a auditar.
8. Elaboración del programa de auditoría.
9. Definición de las herramientas a aplicar en la auditoría.
10. Solicitar información requerida a los responsables del proceso como apoyo para la auditoría.

11. Programar y realizar entrevistas con los responsables del proceso, responsables y encargados del tratamiento de la información.
12. Realizar las pruebas de auditoría pertinentes sobre la auditoría realizada.
13. Recolectar información de las entrevistas, observación y pruebas realizadas.
14. Realizar análisis de resultados de la auditoría realizada.
15. Realizar informe preliminar de la auditoría.
16. Socializar informe preliminar de la auditoría realizada a los auditados.
17. Realizar informe final de la auditoría.
18. Presentar informe final a la Alta Dirección.
19. Realizar seguimiento al cumplimiento del plan de mejora levantado por el responsable de la información sobre los hallazgos de la auditoría realizada.
20. Realizar informes de seguimiento al cumplimiento del plan de mejora.

5.2.9.6 Herramientas de Auditoría

Para llevar a cabo el desarrollo de la auditoría en Gestión de Tratamiento de la Información se utilizará las siguientes herramientas de evaluación:

- Herramienta Diagnóstica de Cumplimiento de Tratamiento de la información.

- Programa de auditoría (Ver Anexo 2).

5.2.9.7 Programa de Auditoría

Para la auditoría de Gestión de Tratamiento de la Información se propone el siguiente plan de auditoría:

DESCRIPCIÓN	REF P/T
Indagar y verificar si existe un modelo de gestión para el cumplimiento regulatorio a nivel de seguridad de la información; en el cual se identifiquen roles y responsabilidades.	

Verificar si se mantiene un registro de todos los requisitos legales, reglamentarios y contractuales a cumplir, su impacto y si requieren acciones de implementación dentro de la organización?.	
Existen claramente definidas y asignadas las funciones del oficial de protección de información?	
Verificar si se tienen definidos e implementados los formatos de autorización de tratamiento de datos y habeas data regulados mediante la ley 1581 de 2012 y decreto 1377.	
Verificar si la organización tiene definida una política de tratamiento de información y aviso de privacidad y si estos se encuentran debidamente publicados en la página web de la organización y en un lugar visible de la recepción.	
Verificar si todas las finalidades de tratamiento de datos realizado por la organización cumple de acuerdo a lo definido en la política y a las actividades desarrolladas.	
Verificar si la organización cumple con todos los criterios definidos en el principio de responsabilidad demostrada en cuanto a la gestión de riesgos particular para la ley.	
Verificar el proceso de selección y la autorización por parte de los candidatos para el tratamiento de datos.	
Verificar si la empresa realiza el tratamiento de información considerada como sensible y si para su recolección se da cumplimiento a lo definido en la ley.	
Verificar que la gestión documental y archivo cuenta con procesos relacionados al tratamiento y almacenamiento de la información	
Existen procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales donde se tengan definidas cláusulas de cumplimiento de la ley de protección de datos, habeas data y confidencialidad?.	

Tabla 18. Propuesta Programa de Auditoría.

5.2.10 Plan de Mejora de Gestión de Tratamiento de la Información

5.2.10.1 Criterios de Plan de Mejora

Como parte de la toma de acciones o mejoras para la Gestión de Tratamiento de la Información se establecen los siguientes criterios:

Criterio	Descripción
Aceptar	Los hallazgos se darán como aceptados cuando la evaluación de riesgo resulte como mitigado en el nivel de aceptación establecido. En este caso no será obligación tomar acción sobre el hallazgo, sin embargo, como buena práctica se recomienda aplicar las acciones recomendadas como parte de la mejora del proceso.
Actuar	En este caso si el nivel de riesgo del hallazgo resulta fuera del nivel de aceptación, se deben tomar las acciones pertinentes. Estas acciones se realizarán de acuerdo al nivel de criticidad de las mismas, con el fin de darle prioridad a aquellos hallazgos más críticos.
Transferir	Las acciones sobre los hallazgos serán transferidos cuando una vez evaluados se considere que no se tiene el alcance pertinente para aplicarlas. De esta manera, podrán ser transferidos a nivel internos entre las áreas, o en caso extremo, a un tercero para dar la solución respectiva.

Tabla 19. Criterios de Plan de Mejora.

5.2.11 Propuesta Plan de Mejora

Complementario a las auditorías propuestas para la Gestión de Tratamiento de la Información se propone el siguiente formato de plan de mejora:

Propuesta Formato Plan de Mejora

Ref.	Hallazgo	Nivel de Riesgo	Acción	Responsable	Fecha Inicio	Fecha Fin
1						
2						
3						
.						
.						
.						

Tabla 20. Propuesta Formato Plan de Mejora.

ENTREGABLE 3 Objetivo 3 de Proyecto

5.3 MODELO DE GESTIÓN DE TRATAMIENTO DE LA INFORMACIÓN

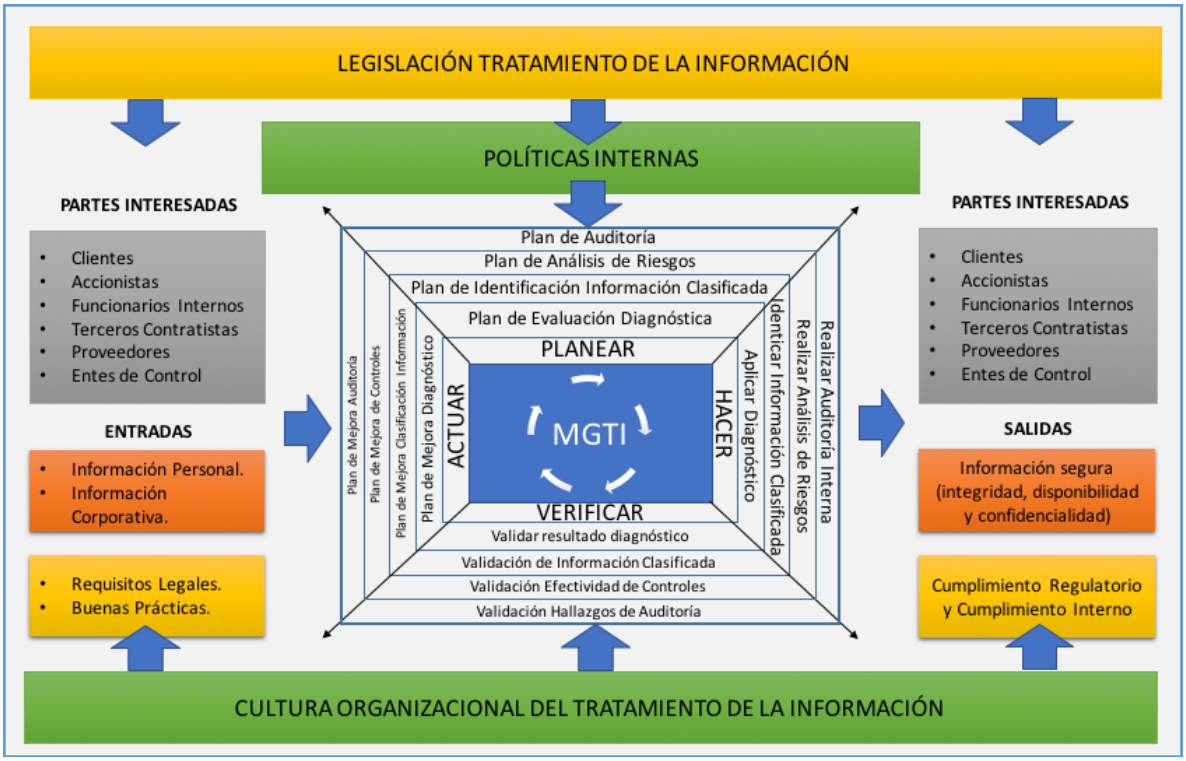

Figura 5. Modelo de Gestión de Tratamiento de la Información.

5.3.1 Componentes del Modelo GTI

El Modelo de Gestión de Tratamiento de la Información se encuentra conformado por los siguientes componentes:

- Legislación del Tratamiento de la Información.
- Políticas Internas.
- Partes Interesadas (Clientes, Accionistas, Funcionarios Internos, Terceros Contratistas, Proveedores, Entes de Control).
- Entradas de Información (Información Personal y Corporativa, Requisitos Legales, Buenas Prácticas).

- Salidas (Información Segura, Cumplimiento de Regulación y Cumplimiento Interno).
- Cultura Organizacional del Tratamiento de la Información.
- Cuerpo del Modelo de Gestión de Tratamiento de la Información que incluye un ciclo PHVA y actividades por cada etapa de Planear, Hacer, Verificar y Actuar.

5.3.2 Operación del Modelo GTI

El Modelo de Gestión de Tratamiento de la Información está conformado en su cuerpo central por un ciclo PHVA (Planear, Hacer, Verificar y Actuar), mediante el cual operan diversas actividades que conllevan al cumplimiento del mismo. De esta manera, a continuación se describe el funcionamiento del Modelo del GTI:

5.3.2.1 Partes Interesadas

En el modelo se encuentran identificadas las partes interesadas como parte de entradas y salidas del proceso de gestión de tratamiento de la información. Dichas partes interesadas ingresan información a la organización que luego es tratada por la misma, dando un resultado de dicho tratamiento que se debe ver reflejado en la seguridad a nivel de integridad, disponibilidad y confidencialidad, dando a su parte interesada la tranquilidad y confianza de un adecuado tratamiento de su información.

5.3.2.2 Entradas

Para la gestión del tratamiento de la información de acuerdo al modelo establecido se presentan entradas relacionadas con información personal y de tipo corporativo. Información personal que hace parte de todos aquellos datos que las partes interesadas dan a la organización como parte de una finalidad en sus procesos internos. E igualmente, la información corporativa que es aquella que se recibe,

genera, procesa o almacena en la organización en su contexto de empresa en sus procesos internos.

Otro tipo de información de entrada que hace parte de la gestión del tratamiento de la información presente este modelo, es la legislación, políticas internas y buenas prácticas que se relacionan en esta temática como parte del cumplimiento de un marco regulatorio a nivel interno y externo de la organización.

5.3.2.3 Ciclo PHVA del Modelo GTI

El modelo se encuentra fundamentado en un ciclo PHVA por el cual realiza su operación principal. De esta manera, en su real hacer dentro del mismo una vez se han identificado las entradas al modelo se describe su forma de operar:

Planear

En la fase del planear inicialmente se ha definen los planes del mismo iniciando de desde lo más interno al lo externos como lo indican las flechas de color negro. En otras palabras de adentro hacia fuera. Considerando lo anterior, en esta fase se iniciaría con la planeación de la evaluación diagnóstica, el cual luego continuaría en su fase del hacer, verificar y actuar posteriormente. Una vez terminado el ciclo, se pasa a una nueva etapa de la planeación relacionada con el plan de identificación de información clasificada, el cual igualmente, pasaría a su fase de hacer, verificar y actuar. Una vez terminado el ciclo se pasaría al otro nivel de la planeación denominado plan de de análisis de riesgos, el cual como las anteriores pasaría a su etapa del hacer, verificar y actuar. Finalmente al haber terminado el ciclo se pasaría a la última etapa de la planeación relacionada con la definición del plan de auditoría, que a su vez, cumpliría los ciclos restantes del hacer, verificar y al actuar. De esta manera, se considera la etapa del planeación del modelo.

Hacer

En la fase del hacer realmente se debe ejecutar todo lo planeado. Así, considerando lo establecido en la fase de planeación, igualmente operaría de adentro hacia fuera en relación a las actividades del modelo. En este caso, se haría el análisis diagnóstico, para luego cumplir el ciclo restante del PHVA; luego cumplido esta etapa, se pasaría a identificar la información clasificada, e igualmente, cumplir las etapas de verificar, actuar y planear del ciclo PHVA; posteriormente, se realizaría el análisis de riesgo, que seguiría su curso en la etapa de verificar, actuar y planear, respectivamente, y finalmente se realizaría la auditoría interna, que a su vez cumpliría el resto de etapas del ciclo PHVA.

Verificar

Como parte del verficar, el modelo opera igualmente que las fases anteriores, de adentro hacía a fuera a medida que se van realizando las actividades pertinentes. De esta manera, una vez se haya ejecutado el análisis diagnóstico en esta etapa se validan los resultados obtenidos con el fin de identificar el cumplimiento de los requisitos legales y de políticas internas de tratamiento de la información, para posteriormente, levantar un plan de mejora en la siguiente etapa y continuar el ciclo. Luego, cuando se haya identificado la información clasificada, se validará la misma conforme a las políticas establecidas respecto a su clasificación (pública, semiprivada, privada, reservada o confidencial), el cual luego pasará a una etapa de mejora y continua las etapas del ciclo. Después, al haber realizado el análisis de riesgo en la etapa previa, se espera validar los controles y la efectividad de los mismos como parte de su adecuada y eficiente operación en relación al tratamiento de la información, y así continúa el ciclo a la etapa de mejora y posteriores. Finalmente, al recibir los resultados de auditorías internas de tratamiento de la información se validarán los hallazgos encontrados con el fin de realizar el plan de tratamiento en la etapa posterior y seguir el ciclo PHVA.

Actuar

En esta etapa del actuar se definen todos los planes de mejora del proceso realizado. Esta etapa opera, como las anterior del interior al exterior del modelo. Así, una vez se haya validado los resultados del análisis diagnóstico se establecerá el plan de mejora diagnóstico pertinente y continua el ciclo. Igualmente, una vez validada la clasificación de la información se establecerá el plan de mejora clasificación de la información y continua el ciclo. Luego, de haber validado la efectividad de los controles como parte del análisis de riesgos, se establece el plan de mejora de controles y continua el ciclo. Y finalmente, al haber validado los hallazgos de auditorías internas, se establece el plan de mejora de auditoría para continuar con el proceso en el Ciclo PHVA.

5.3.2.4 Salidas

Como parte de las salidas de este proceso en general se espera la satisfacción de las partes interesadas, conforme a un tratamiento seguro de su información y al cumplimiento de la regulación a nivel interno y externo de la organización.

5.3.2.5 Cultura Organizacional del Tratamiento de la Información

Como parte transversal a todo el proceso se encuentra la cultura organizacional del tratamiento de la información que se debe ir generando con el paso de los ciclos (PHVA), en el cual se fomenta una formación, hábito, costumbre o una razón más para continuar un adecuado tratamiento de la información en la organización en cumplimento de su misión y visión empresarial

6. CONCLUSIONES

El tratamiento adecuado de la información y una buena gestión de riesgos en la organización es una propuesta que permite optimizar las operaciones del negocio, de tal manera que contribuya al logro de sus metas establecidas.

Con el resultado de las acciones implementadas se busca que se documente y mantengan actualizados los riesgos sobre el tratamiento de la información, que se registren de eventos identificados con las actividades de la organización, y así mismo, se valore la probabilidad de ocurrencia e impacto y las medidas de control que se establezcan para una buena mitigación.

Mantener la seguridad de la información en el cual se preserva la integridad, disponibilidad y confidencialidad de la misma, permitirá a la organización manejar los procesos de una forma segura y de calidad, como parte importante en la optimización de recursos, dar buena imagen corporativa, cumplir con requisitos legales y dar confianza a sus clientes.

El Modelo de Gestión de Tratamiento de la Información logrará dar a la organización una solución viable al tratamiento de la información, fundamentada en una investigación científica, teórica y de la experiencia relacionada con la seguridad de la información en las organizaciones.

7. BIBLIOGRAFÍA

- Alcaldía de Bogotá. Recuperado de: www.alcaldiabogota.gov.co/sisjur/normas

- Asociación Colombiana de Ingenieros. 2017. Lista de Empresas de Seguridad Informática. Recuperado de:http://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

- Díaz de Iparraguirre Ana Mercedes.(2009) Tesis doctorales de Economía. Carabobo-Venezuela: Casa publicadora Recuperado de http://www.eumed.net/tesis-doctorales/2009/amdi/index.htm

- Díaz de Iparraguirre Ana Mercedes. (15 de julio) La Gestión Compartida Universidad-Empresa en la Formación del Capital Humano. Su Relación con la Competitividad y el Desarrollo Sostenible. Capítulo IV. Carabobo – Venezuela: Tratamiento de la Información. Recuperado de: http://www.eumed.net/tesisdoctorales/2009/amdi/TRATAMIENTO%20DE%20LA%20INFORMACION%20EN%20LA%20GESTION%20COMPARTIDA%20UNIVERSIDAD%20EMPRESA.htm

- Ecopetrol (11,09,2014) Declaración de Tratamiento de la Información Personal en Ecopetrol S.A. Recuperado de: http://www.ecopetrol.com.co/wps/portal/es/ecopetrol-web/responsabilidad-corporativa/relaciones-de-confianza-con-nuestros-grupos-de interes/declaracion-de-tratamiento-de-la-informacion-personal-en-ecopetrol-s.a

- El profesional de la Información, (mayo 1999) Gestión y tratamiento de la información documental: una propuesta sobre límites y propiedades. El Profesional de la Información. Recuperado de:http://www.elprofesionaldelainformacion.com/contenidos/1999/mayo/gestin_y_tratamiento_de_la_informacin_documental_una_propuesta_sobre_lmites_y_propiedades.html

- Iniciativa presidencial Urna de Cristal, 1de abril de 2013. portal de participación ciudadana. Recuperado de: http://www.urnadecristal.gov.co/video/qu-subsidios-da-gobierno-adulto-mayor

- Institución Universitaria Politécnico Grancolombiano Módulo Opción de Grado I. Especialización Seguridad de la Información.

- Institución Universitaria Politécnico Grancolombiano. Módulo Evaluación de Proyectos. Especialización Seguridad de la Información.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 2007 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: Recuperado de: ICONTEC, 2007. NTC ISO/IEC 27002.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 2013 Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.: Recuperado de: ICONTEC, 2013. NTC ISO/IEC 27001.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN.2009 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. Bogotá D.C.: Recuperado de: ICONTEC, 2009. NTC ISO/IEC 27005.

- Jorge Burgos Salazar1, Pedro G. Campos1. Modelo para la Seguridad de la Información en TIC. Recuperado de: http://ceur-ws.org/Vol-488/paper13.pdf

- Ministerio de Tecnologías de la Información y las Comunicación. Modelo de Seguridad. Ministerio TIC. Recuperado de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- Ministerio de Tecnologías de la Información y las Comunicación.29.07.2016 y Comunicación. Modelo de Seguridad y Privacidad de la Información.

Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/articles8253_modelo_seguridad.pdf

- Molina Sánchez, Víctor Isaías; 03.2013. Modelo de gestión del tratamiento de datos personales en la universidad pública. Repositorio Académico de la Universidad de Chile. Recuperado de: http://repositorio.uchile.cl/handle/2250/113179

- Politécnico GranColombiano Módulo. Análisis de Riesgo.

- Ponjuan Dante Gloria. 2 de mayo 2011. La gestión de información y sus modelos representativos. Valoraciones. Ciencias de la Información Vol. 42, No. 2. Recuperado de: http://www.redalyc.org/pdf/1814/181422294003.pdf

- Project Management Institute. 2013. PMBOK. Fundamentos para la Dirección de Proyectos. Edición 5.

8. ANEXOS

ANEXO 1.

Herramienta Diagnóstica de Cumplimiento de Tratamiento de la Información.

No.	Pregunta	Sí	No
1.	¿En la organización se conoce el tema de tratamiento de la información?		
2.	¿Existen políticas de tratamiento de la información?		
3.	¿Se tiene identificada la legislación y normatividad que aplica sobre el tratamiento de la información?		
4.	¿En la organización se considera importante el tratamiento de la información?		
5.	¿Se considera que un buen tratamiento de la información conlleva a beneficios económicos de la empresa?		

6.	¿ Se considera que un buen tratamiento de la información conlleva a beneficios en el cumplimiento de requisitos legales?		
7.	¿ Se considera que un buen tratamiento de la información conlleva a beneficios reputacionales de la empresa?		
8.	¿ Se considera la información como un activo importante en el desarrollo de sus operaciones?		
9.	¿Existe compromiso por parte de la alta dirección con el tratamiento de la información en la organización?		
10.	¿Se conocen las implicaciones legales de no tratar adecuadamente la información?		
11.	¿La organización dispone de políticas de seguridad de la información?		
12.	¿La organización dispone de políticas de tratamiento de la información?		
13.	¿La organización dispone metodología de gestión de riesgos?		
14.	¿La organización dispone de un responsable para el control del tratamiento de la información?		
15.	¿La organización dispone de recursos para la implementación de proyectos de tratamiento de la información?		
16.	¿La organización cumple con requisitos legales relacionados con el tratamiento de la información?		
17.	¿La alta dirección y la organización conocen sobre el tema del tratamiento de la información?		
18.	¿En la organización se gestionan los incidentes del tratamiento de la información?		
19.	¿La organización dispone de personal idóneo para realizar proyectos de tratamiento de la información?		
20.	¿En la organización se tiene identificada toda la información que se maneja en los procesos?		
21.	¿En la organización se tiene clasificada la información?		

22.	¿En la organización se tienen identificados y asignados los propietarios de la información?		
23.	¿En la organización se tienen identificados y asignados los responsables y encargados de tratamiento de la información?		
24.	¿En la organización se tienen identificados los activos de información?		
25.	¿En la organización se tienen identificados los contenedores de la información?		
26.	¿En la organización se tienen identificadas y definidas todas bases de datos?		
27.	¿En la organización se tienen definidas todas la finalidades de la información por tipo?		
28.	¿En la organización se tienen identificados y definidos los canales de recolección de la información?		
29.	¿En la organización se recolecta la información de manera formal?		
30.	¿En la organización se solicita autorización para la recolección de la información?		
31.	¿Se guarda evidencia del autorización de la información?		
32.	¿Es comunicada a los titulares la finalidad y razones de la información recolectada y tratada?		
33.	¿Se tienen definidos procesos de atención, quejas y reclamos sobre el tratamiento de la información?		
34.	¿En la organización se tienen identificados los terceros que manejan información de la misma?		
35.	¿Se tienen acuerdos o convenios con terceros en la cual se dé formalidad en el tratamiento de la información?		
36.	¿Se transfiere información de la organización a otros países?		
37.	¿Se han registrado las bases de datos a nivel interno o externo de acuerdo a los requisitos normativos internos y legales vigentes?		

38.	¿Se tienen identificados los medios de almacenamiento de la información?		
39.	¿Se tienen establecidos de controles de seguridad de las bases de datos?		
40.	¿Se tienen establecidos y se cumplen los tiempos de retención de la información de acuerdo a los requisitos internos y legales vigentes?		