



SISTEMA INTEGRADO DE TRANSPORTE
DE VALLEDUPAR

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN


SISTEMA INTEGRADO DE TRANSPORTE DE
VALLEDUPAR SIVA S.A.S

KATRIZZA MORELLI AROCA
GERENTE
2021

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 1 de 14

TABLA DE CONTENIDO

1	INTRODUCCION.....	2
2	OBJETIVOS	2
2.1	Objetivo general.....	2
2.2	Objetivos Específicos.....	3
3	MARCO NORMATIVO.....	3
4	DEFINICIONES	4
5	METODOLOGIA.....	5
5.1	IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS.....	6
5.1.1	Programación y Agendamiento de Entrevistas.....	8
5.1.2	Entrevista con los Líderes.....	8
5.1.3	Identificación y Calificación de Riesgos.....	8
5.1.4	Valoración del Riesgo Residual	10
5.1.5	Mapas De Calor Donde Se Ubican Los Riesgos.....	11
5.2	TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION.....	11
5.3	SEGUIMIENTO Y CONTROL.....	12
6	CRONOGRAMA	12
8.	RECURSOS.....	13
9.	INDICADORES.....	13

 <p>SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR</p>	<p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</p>	<p>VERSIÓN: 1.0</p>
		<p>FECHA: 28/01/2021</p>
		<p>Página 2 de 14</p>

1 INTRODUCCION

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información. El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

El plan de tratamiento de riesgos de seguridad, se encuentra alineado con el Plan estratégico 2020-2023, dentro del escenario estratégico de Desarrollo Institucional, en la línea de acción Gestión de la Información, cuyo objetivo es disponer de la información apropiada para el desarrollo de las funciones.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorías internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC, dentro de su política de gobierno Digital.

El seguimiento al plan de tratamiento de riesgos, se realizará de acuerdo con la GUIA PARA LA ADMINISTRACIÓN DE RIESGO v5 de la DAFP y se integrará con los riesgos de seguridad digital y de la información.

2 OBJETIVOS

2.1 Objetivo general

Brindar una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 3 de 14


en la Entidad, así como permitir la recuperación del sistema o la transferencia del problema a un tercero.

2.2 Objetivos Específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
 - Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad

3 MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 4 de 14

NTC / ISO 27001:2018	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2018	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública diciembre de 2020

4 DEFINICIONES

- **Activo:** cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo:** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa:** Elemento específico que origina el evento.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno¹:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles:** Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos²:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente:** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.

¹ ISO 31000:2018

² Ibid.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 5 de 14


- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo³:** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Riesgo aceptable:** Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Riesgo:** Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

5 METODOLOGIA

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, se basa en analizar el impacto que puede tener una organización al ser vulnerada, buscando identificar las amenazas que pueden llegar a afectar el funcionamiento de la compañía. Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos. Está dividida en tres partes. La primera parte hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos de acuerdo a la norma ISO 27001.

La segunda parte es el inventario activo de información que puede utilizar la empresa para enfocar el análisis de riesgo, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

³ ISO 31000:2018

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 6 de 14

Por último, son las técnicas que Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

5.1 IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

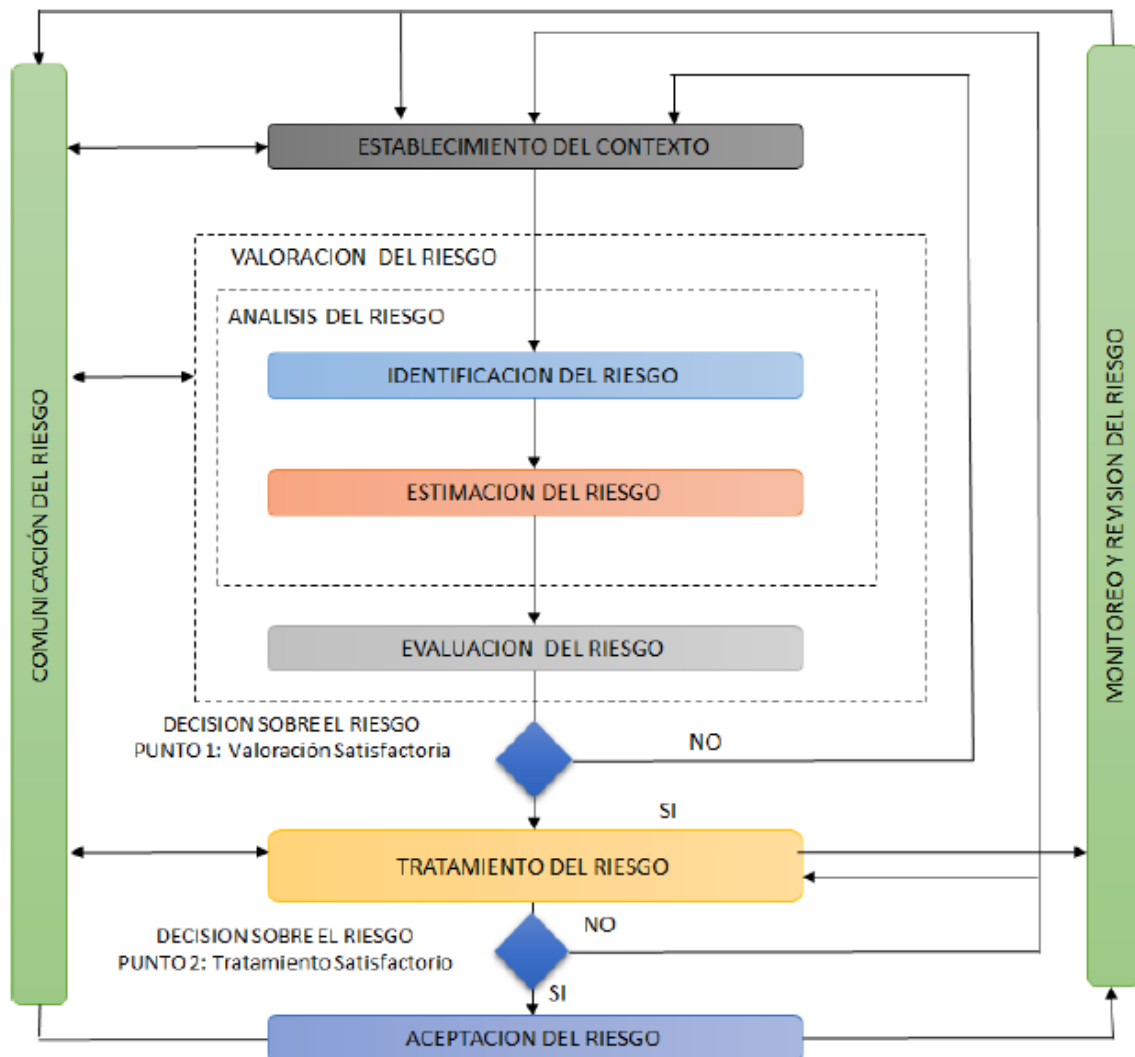
La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5-2020, emitida por el Departamento Administrativo de la Función Pública.



Ilustración 1. Estructura general de la metodología de riesgos


La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2018):

Ilustración 2. Gestión de riesgos



La evaluación de los riesgos de seguridad de la información se enfocará en:

- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de SIVA.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 8 de 14

- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de SIVA.

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para SIVA, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

5.1.1 Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGC y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.


5.1.2 Entrevista con los Líderes

Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

5.1.3 Identificación y Calificación de Riesgos

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los activos de información se clasifican en dos tipos:

 <p>SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR</p>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 9 de 14

a) Primarios:

a. Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) De Soporte

a. Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

b. Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)


c. Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

d. Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

f. Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 10 de 14

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de SIVA.

Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

5.1.4 Valoración del Riesgo Residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.


Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para SIVA, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información:

- Análisis de riesgos

o Identificación de los riesgos`

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 11 de 14

o Estimación del riesgo

- Evaluación del riesgo

5.1.5 Mapas De Calor Donde Se Ubican Los Riesgos

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

Valoración de los Riesgos de Seguridad

La valoración de los riesgos se puede consultar en el documento A-RI-P11-G01 guía para la gestión de riesgos de activos de información.

Tratamiento de Riesgos de Seguridad

El Líder del SGC con su equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados, obtenido con el procedimiento de Gestión del Riesgo de Seguridad de la Información y la Guía asociada a este procedimiento.


Documento de declaración de aplicabilidad.

Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de los mismos y la prioridad de implementación de cada proyecto. Estos planes de proyectos de seguridad de la información son identificados y definidos en conjunto entre el Líder del SGC.

5.2 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el SIVA.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo de la Gerencia, debe definir e implementar los controles

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 12 de 14

necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

A continuación, se definen las siguientes estrategias de tratamiento, asumir los riesgos bajos y moderados y gestionar el riesgo alto y extremo.

5.3 SEGUIMIENTO Y CONTROL

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

6 CRONOGRAMA

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la Gestión administrativa apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

La implementación se desarrolla en 2 fases, las cuales se definen a continuación:



Ilustración 3. Cronograma


8. RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la Gestión administrativa, los recursos de inversión se tomarán del Objetivo del Plan estratégico 2021-2024.

9. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0
		FECHA: 28/01/2021
		Página 14 de 14

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

La gestión administrativa asesora a las áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital, los líderes de las áreas solicitarán a la Profesional de planeación la inclusión de los mismos en el mapa de riesgos institucional, instrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.

La Gestión administrativa apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable.

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.



Fin del documento