POLITICA DE ADMINISTRACIÓN DEL RIESGO

2019

Control de Cambios del Documento

Elaborado Por	Descripción del Cambio	Fecha
Oficina Asesora de Planeación	Se definen los lineamientos para la Gestión del Riesgo en la Superintendencia de Transporte	4-4-2016
Oficina Asesora de Planeación	Se modifica la Política de Gestión del Riesgo, de acuerdo con los lineamientos de la Guía para administración del riesgo del Departamento Administrativo de la Función pública V3 de diciembre de 2014 y la Guía para la Gestión del Riesgo de Corrupción de la Secretaria de Transparencia - 2015	Julio de 2018
Oficina Asesora de Planeación Oficina de Tecnologías de la Información y las Comunicaciones	Se modifica la Política de Administración del Riesgo, de acuerdo con los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 – Octubre de 2018. Se incluye la gestión de riesgos de seguridad digital, para la Superintendencia de Transporte y los lineamientos del Decreto 2409 de 2018	Septiembre 2019

Tabla de contenido

1. Administración del Riesgo en la Supertransporte

La Superintendencia de Transporte se compromete a administrar adecuadamente los riesgos asociados a los procesos institucionales, adoptando la metodología adecuada para su gestión, determinando las acciones de control detectivas y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

La entidad establece las herramientas necesarias con la participación de los servidores públicos y contratistas para promover la integridad que permita controlar y responder a los acontecimientos potenciales o aquellos en los que puedan desencadenar la materialización de los riesgos.

2. Objetivo

Establecer los lineamientos para la gestión integral del riesgo en la Superintendencia de Transporte, con el fin de identificar, administrar, hacer monitoreo, revisión y seguimiento a aquellos posibles eventos negativos, tanto internos como externos, que puedan afectar el cumplimiento de los objetivos institucionales.

Estandarizar el proceso de gestión de riesgos de seguridad digital, generando mecanismos para establecer los elementos que permitan identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital, proponiendo estrategias para ejecutar planes de acción para mitigar los riesgos generados en el entorno digital.

3. Alcance

La política de administración del riesgo es aplicable a los objetivos institucionales, todos los procesos de la Entidad y a todas las acciones ejecutadas por los servidores públicos y contratistas durante el ejercicio de sus funciones y cumplimiento de obligaciones. Con un enfoque hacia el entorno digital que permitan la identificación de activos, catálogo de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital, controles para los riesgos de seguridad digital, reportes de riesgos de seguridad digital, y todos los aspectos necesarios para llevar a cabo una adecuada gestión de riesgo en todos los contextos institucionales.

4. Términos y Definiciones

- **Aceptar el riesgo:** Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Administrar el riesgo:** Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus

diferentes elementos le permite a la entidad pública auto controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de Riesgo:** Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente)
- **Calificación del riesgo:** Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- **Causa:** Conjunto de hechos, recursos, actuaciones o condiciones internos y externos que solos o en combinación con otros, facilitaron o permitieron o pueden permitir la ocurrencia de un evento..
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Controles:** Medida que modifica al riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas u otras acciones que modifican al riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Establecimiento del contexto.** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.
- **Evento:** Incidente o situación, que ocurre en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.
- **Evaluación del riesgo.** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Gestión del riesgo.** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo; proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del Riesgo:** Se realiza determinando las causas, con base en el contexto interno, externo y de los procesos ya analizados para la entidad, y que pueden afectar el logro de los objetivos.
- **Integridad:** Propiedad de exactitud y completitud.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Mapa de Riesgos**: Documento con la información resultante de la gestión del riesgo.
- **Plan de manejo de riesgos:** Formato que contempla la identificación de los riesgos, los controles para la de mitigación y el seguimiento a los mismos.
- **Política para la gestión del riesgo.** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **Política de administración de riesgos de corrupción:** Es el conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al riesgo
- **Probabilidad:** grado en el cual es probable que ocurra de un evento, este se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.
- **Proceso para la Gestión del Riesgo:** Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento y monitoreo.
- **Reducir el riesgo**: Implica tomar medidas encaminadas a disminuir la probabilidad (medidas de prevención). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.
- **Riesgo**: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de corrupción**: La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente**: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **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. Actualizado a Anexo 4: Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas de MINTIC
- **Riesgo residual:** nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **Tolerancia al riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Tratamiento del riesgo.** Proceso para modificar el riesgo.
- **Valoración del Riesgo:** "*Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).* Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.
- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. Niveles de Responsabilidad y Autoridad frente al Riesgo

A continuación, se definen los roles que desarrollarán la administración del riesgo en la Superintendencia de Transporte, de acuerdo con el Modelo Integrado de Planeación y gestión – MIPG, estas instancias participan en la definición y ejecución de las acciones, métodos y procedimientos de control y de gestión del riesgo y la "*Guía para la administración del Riesgo y el diseño de controles en entidades públicas" Riesgos de Gestión,*

Corrupción y Seguridad Digital, versión 4. Octubre de 2018, del Departamento Administrativo de la Función Pública de la siguiente manera:

Línea de Defensa	Roles	Responsabilidad frente al riesgo
Estratégica	Alta Dirección Comité Institucional de Coordinación de Control Interno Comité Institucional de Gestión y Desempeño	. Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad. . Establecer la Política de Administración del Riesgo. . Establecer los lineamientos encaminados a controlar los riesgos que pueden llegar a incidir en el cumplimiento de los objetivos institucionales . Hacer seguimiento a la adopción, implementación y aplicación de controles. . Realizar seguimiento y analizar los riesgos de manera periódica (mínimo una vez al año).
Primera Línea	Responsables de Proceso Secretario General, Superintendentes Delegados, Jefes de Oficina, Directores y Coordinadores de Grupo	. Identificar y valorar los riesgos que puedan afectar el logro de los objetivos institucionales. . Definir y diseñar los controles a los riesgos de los procesos a cargo . Realizar seguimiento y análisis a los controles de los riesgos según periodicidad establecida . Actualizar el mapa de riesgos cuando se requiera . Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
	Oficina de Tecnologías de la Información y las Comunicaciones	. Realizar las actividades necesarias para la identificación de activos, análisis, evaluación y tratamiento de los riesgos . El responsable de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte como para la gestión y tratamiento de estos riesgos.
Segunda Línea	Responsables y Líderes de Proceso	. Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo . Realizar el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar
	Oficina Asesora de Planeación	. Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo. . Informar sobre la incidencia de los riesgos en el logro de los objetivos y evaluar si la valoración del riesgo es la apropiada. . Liderar la elaboración y consolidación del mapa de riesgos y elaborar informes consolidados para las diversas partes interesadas (en caso de requerirse).

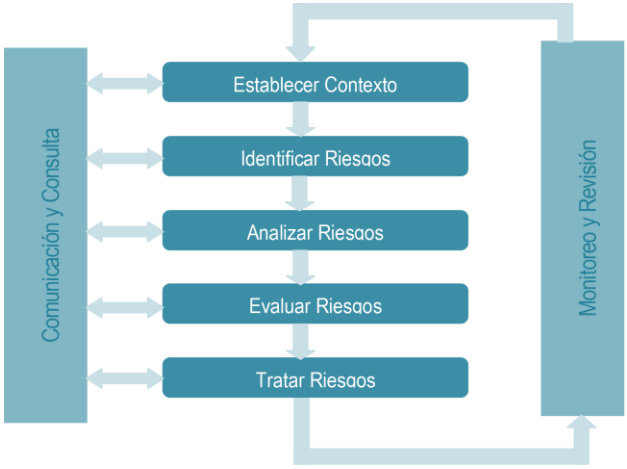
Línea de Defensa	Roles	Responsabilidad frente al riesgo
		. Monitorear con los responsables de los procesos, los cambios del entorno, las nuevas amenazas y los controles aplicables . Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar. . Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude.
	Oficina de Tecnologías de la Información y las Comunicaciones	. Liderar la Implementación de los planes de tratamiento de riesgos de seguridad digital . Liderar la Implementación del tratamiento de actividades de monitoreo y revisión de riesgos y sus residuales . Liderar la Implementación de las actividades de Mejoramiento continuo.
Tercera Línea	Oficina de Control Interno	. Comunicar al Comité de Coordinación de Control Interno (si la entidad cuenta con él) posibles cambios e impactos en la evaluación del riesgo, detectados en seguimientos o auditorías internas. . Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. . Alertar sobre la probabilidad del riesgo de fraude o corrupción en las áreas objeto de seguimiento o auditoría interna. . Asesorar en la metodología para la identificación de riesgos institucionales con la segunda Línea de Defensa conformada por los servidores responsables de monitoreo y evaluación de controles y gestión del riesgo (Jefe de Planeación, supervisores e interventores de contratos o proyectos, comité de contratación, entre otros) . Analizar el diseño e idoneidad de los controles determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos . Realizar seguimiento periódico de la gestión de riesgos en los distintos procesos . Realizar seguimiento a los riesgos de corrupción según periodicidad establecida por la Secretaría de Transparencia.

**Elaboración Propia*

Lo anterior, teniendo en cuenta el criterio diferencial para la implementación y aclarando que la entidad actualmente se encuentra en un nivel de implementación MECI – Intermedio.

6. Estructura para administración del riesgo

En el siguiente capítulo se presenta la metodología para la administración del Riesgo en la Superintendencia de Transporte, la cual cuenta con la siguiente estructura:



Fuente: Norma ISO 31000

6.1 Establecer Contexto

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Para establecer el contexto es fundamental tener claridad de la misión, los objetivos institucionales y contar con una visión sistémica del negocio de manera que la gestión del riesgo se incorpore como una herramienta gerencial que contribuye al desarrollo organizacional. La entidad debe analizar los objetivos estratégicos y su alineación con la Misión y la Visión, asegurando que los objetivos de proceso contribuyan al cumplimiento de los objetivos estratégicos, e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

Por lo tanto, el diseño se establece a partir de la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos. En esta fase se establece:

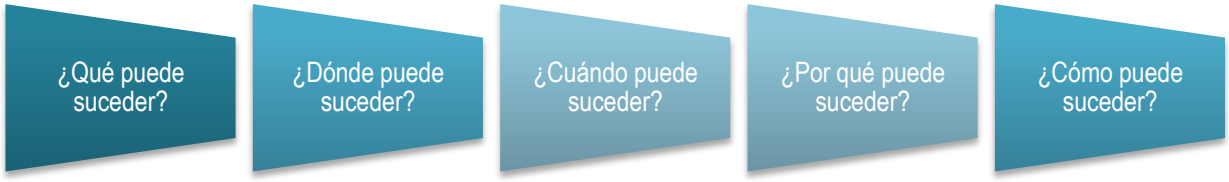
- ✓ El Contexto Externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.
- ✓ El Contexto Interno: Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.
- ✓ El Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Como herramienta básica para el análisis del contexto del proceso se sugiere utilizar las caracterizaciones de estos, donde es posible contar con este panorama.

DEFINICIÓN DE FACTORES POR TIPO DE CONTEXTO		
CONTEXTO EXTERNO	**CONTEXTO INTERNO**	**CONTEXTO DE PROCESOS**
Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.	**Financieros**: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.	**Diseño del Proceso**: claridad en la descripción del alcance y objetivo del proceso
Sociales y Culturales: Demografía, responsabilidad social, orden público	**Personal:** competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.	**Interacciones con Otros Procesos**: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
Económicos y Financieros: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.	**Procesos:** capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.	**Transversalidad**: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno digital, vigilados, proveedores, normativa, entorno cultural.	**Tecnología:** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.	**Procedimientos asociados:** Pertinencia en los procedimientos que desarrollan los procesos.
Ambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Estratégicos:** Direccionamiento estratégico, Planeación institucional, liderazgo, trabajo en equipo.	**Responsables del proceso:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
Legales y Reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).		**Comunicación entre los procesos:** Efectividad en los flujos de información determinados en la interacción de los procesos.
Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.	**Comunicación Interna:** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	**Activos de seguridad digital del proceso**: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. V4. Dirección de gestión y desempeño institucional

6.2 Identificar Riesgos

Para identificar los riesgos, se debe determinar toda situación que pueda afectar el normal desarrollo de las funciones de la entidad, en este elemento de control se establecen varias de las características que presenta el riesgo como la fuente, las causas que lo generan y las consecuencias o efectos a que se expone la Superintendencia de Transporte, si estos llegan a ocurrir. La identificación del riesgo debe ser muy rigurosa y cuidadosa, tratando de cubrir todos los posibles eventos, incluyendo la gestión de riesgos de seguridad digital. En la identificación del riesgo se debe dar respuesta a cinco preguntas esenciales:



Estas preguntas proporcionan los elementos básicos de identificación del riesgo, sus fuentes o causas, eventos generadores, escenarios, que lo caracteriza.

6.3 Clasificación del Riesgo

Durante la identificación del Riesgo, se deben clasificar teniendo en cuenta los siguientes conceptos:

Riesgos de los Procesos:

Riesgo	Descripción
Riesgo Estratégico	Se asocia con la forma en que se administra la entidad. El manejo de riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Riesgos Operativo	Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
Riesgo Tecnológico	Son aquellos que tienen que ver con la capacidad de la entidad y organismo para que la tecnología disponible satisfaga sus necesidades actuales y futuras en aras de garantizar el cumplimiento de su misión y objetivos institucionales.
Riesgo de Cumplimiento	Se asocian con la capacidad de la entidad para cumplir con los requisitos regulatorios, legales, contractuales, de ética pública y en general con su compromiso ante la comunidad
Riesgo de imagen	Son los relacionados con la percepción y la confianza por parte de la ciudadanía hacia la organización
Riesgo Financiero	Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejo de excedentes de tesorería y manejo de bienes o recursos. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad
Riesgo de Corrupción	Posibilidad de que, por acción u omisión, mediante el uso indebido del poder de los recursos o de la información, se lesionen los intereses de la entidad y en consecuencia del Estado, para obtención de un beneficio particular.
Riesgo de Seguridad Digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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.

Riesgos de Corrupción:

Estos riesgos, se identifican en los procesos, determinando acciones de mejora permanentes para evitar su materialización. Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN	**+**	**USO DEL PODER**	**+**	**DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO**	**+**	**EL BENEFICIO PRIVADO**

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Para la identificación de los riesgos de corrupción, deberá tenerse en cuenta los delitos contra la administración pública, como lo establece la Ley 1474 de 2011:

Ley 1474 de 2011 - Delitos contra la administración pública	
Peculado (Capítulo I)	El servidor público para beneficio propio o de un tercero se apropia de bienes muebles o inmuebles, los use indebidamente, les dé un uso diferente al que están destinados o los deje extraviar o perder.
Concusión (Capítulo II)	El servidor público que abusando de su cargo o de sus funciones constriña o induzca a alguien a dar o prometer al mismo servidor o a un tercero, dinero o cualquier otro utilidad indebidos
Cohecho propio (Capítulo III)	El servidor público que reciba para sí o para otro dinero u otra utilidad, o acepte promesa remuneratoria, directa o indirectamente, para retardar u omitir un acto propio de su cargo, o para ejecutar uno contrario a sus deberes
Cohecho impropio (Capítulo III)	El servidor público que acepte para sí o para otro, dinero u otra utilidad o promesa remuneratoria, directa o indirecta, por acto que deba ejecutar en el desempeño de sus funciones
Interés ilícito en la celebración de Contratos (Capítulo IV)	El empleado oficial obtenga un provecho ilícito para sí, para el contratista o para un tercero
Contratos si incumplimiento de requisitos legales (Capítulo IV)	El empleado oficial obtenga un provecho ilícito para sí, para el contratista o para un tercero
Tráfico de Influencias (Capítulo V)	Un servidor público o particular que invoque influencias reales o simuladas para recibir, hacer dar o prometer para sí o para un tercero dinero o dádiva, con el fin de obtener cualquier beneficio de parte de servidor público en asunto que éste se encuentre conociendo o haya de conocer.
Enriquecimiento ilícito (Capítulo VI)	El empleado oficial que por razón del cargo o de sus funciones, obtenga incremento patrimonial no justificado
Utilización indebida de información privilegiada (Capítulo VI)	El servidor público o el particular que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad pública o privada que haga uso indebido de información que haya conocido por razón o con ocasión de sus funciones
Prevaricato por acción (Capítulo VII)	servidor público que profiera resolución, dictamen manifiestamente contrario a la ley
Prevaricato por omisión (Capítulo VII)	El servidor público que omita, retarde, rehúse o deniegue un acto propio de sus funciones
Prevaricato por asesoramiento ilegal (Capítulo VII)	El servidor público que asesore, aconseje o patrocine de manera ilícita a persona que gestione cualquier asunto público de su competencia
Abuso de autoridad por acto arbitrario o injusto (Capítulo VIII)	El empleado oficial que fuera de los casos especialmente previstos como delito, con ocasión de sus funciones o excediéndose en el ejercicio de ellas, cometa acto arbitrario o injusto,
Abuso de autoridad por omisión de denuncia	empleado oficial que teniendo conocimiento de la comisión de un delito cuya averiguación deba adelantarse de oficio, no dé cuenta a la autoridad,

Ley 1474 de 2011 - Delitos contra la administración pública	
(Capítulo VIII)	
Revelación de secreto (Capítulo VIII)	El empleado oficial que utilice en provecho propio o ajeno, descubrimiento científico, u otra información o dato llegados a su conocimiento por razón de sus funciones, y que deban permanecer en secreto o reserva
Abandono del cargo (Capítulo VIII)	El empleado oficial que abandone su cargo sin justa causa
Asesoramiento y otras actuaciones ilegales (Capítulo VIII)	El empleado oficial que ilegalmente represente, litigue, gestione o asesore en asunto judicial, administrativo o policivo
Intervención en política (Capítulo VIII)	El empleado oficial que forme parte de comités, juntas o directorios políticos o intervenga en debates o actividades de este carácter
Empleo ilegal de la fuerza de pública (Capítulo VIII)	El empleado oficial que obtenga el concurso de la fuerza pública o emplee la que tenga a su disposición para consumar acto arbitrario o injusto, o para impedir o estorbar el cumplimiento de orden legítima de otra autoridad
Usurpación de funciones públicas (Capítulo IX)	El particular que sin autorización legal ejerza funciones públicas.
Abuso de función pública (Capítulo IX)	El empleado oficial que abusando de su cargo realice funciones públicas diversas de las que legalmente le correspondan.
Simulación de investidura o cargo (Capítulo IX)	El que únicamente simulare investidura o cargo público o fingiere pertenecer a la fuerza pública.

En caso de detectar un riesgo de Fraude, en coherencia con la norma NIA 240, se deberá tipificar como riesgo de corrupción y en la parte descriptiva indicar por qué es un riesgo de fraude.

Riesgos de Seguridad Digital

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”. Se encuentran alineados con lo establecido en las Políticas de Seguridad de la información (Resolución 60362 de 2017), la Norma NTC-ISO-IEC 27001-2013 y el modelo de Seguridad y Privacidad de la Información –MSPI definido por el MINTIC, teniendo en cuenta la posible vulneración de los pilares principales de la seguridad de la información:

Modelo de Seguridad y Privacidad de la información – MSPI (Clasificación de activos de información)	
CONFIDENCIALIDAD (MSPI y ley 1712 de 2014)	De acuerdo a la Confidencialidad la información se debe clasificar en: INFORMACION PÚBLICA RESERVADA: Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

Modelo de Seguridad y Privacidad de la información – MSPI (Clasificación de activos de información)	
	INFORMACION PÚBLICA CLASIFICADA: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. INFORMACION PÚBLICA: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. NO CLASIFICADA: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.
INTEGRIDAD (MSPI)	De acuerdo a la integridad la información se clasifica en: A (ALTA): Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. M (MEDIA) Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. B (BAJA) Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos. NO CLASIFICADA Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.
DISPONIBILIDAD (MSPI)	De acuerdo a la disponibilidad, la información se clasifica en: 1 (ALTA) La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos. 2 (MEDIA) La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad. 3 (BAJA) La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. NO CLASIFICADA Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Para la evaluación de los riesgos de seguridad digital, se analizará el registro de activos de información conforme a los *"Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas*" del Ministerio de las Tecnologías de la Información y las comunicaciones. Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

- Fases de Gestión de Riesgos de Seguridad Digital

Para llevar a cabo el control y manejo del Riesgo digital en la Superintendencia de Transporte, se lleva a cabo la siguiente metodología:

Fase 1: Planificación

- Definición del contexto interno, externo y de los procesos de la Superintendencia de Transporte.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

Fase 2: Ejecución

- Definición de cronogramas cumplibles para que se ejecuten las tareas en los tiempos pactados y que los recursos se ejecuten según lo planeado.

Fase 3: Monitoreo y revisión

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.
- Implementar los controles necesarios frente al reporte de incidentes de seguridad digital remitidos por las autoridades del Gobierno Nacional encargadas de la Seguridad digital.

Fase 4: Mejoramiento Continuo de la gestión del riesgo de seguridad digital

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.
- Socializar la Política de Gestión de Riesgos de Seguridad Digital al interior de la entidad.
- Proponer Capacitaciones a nivel de Seguridad Digital para los funcionarios y contratistas de la entidad.

6.4 Identificación de Activos de Seguridad Digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de Superintendencia de Transporte, los servicios web, redes, información física y digital, que se utiliza pare el funcionamiento, tanto interno (BackOffice) y externo (FrontOffice), que aumente la confianza de los ciudadanos en la interacción con el Estado.

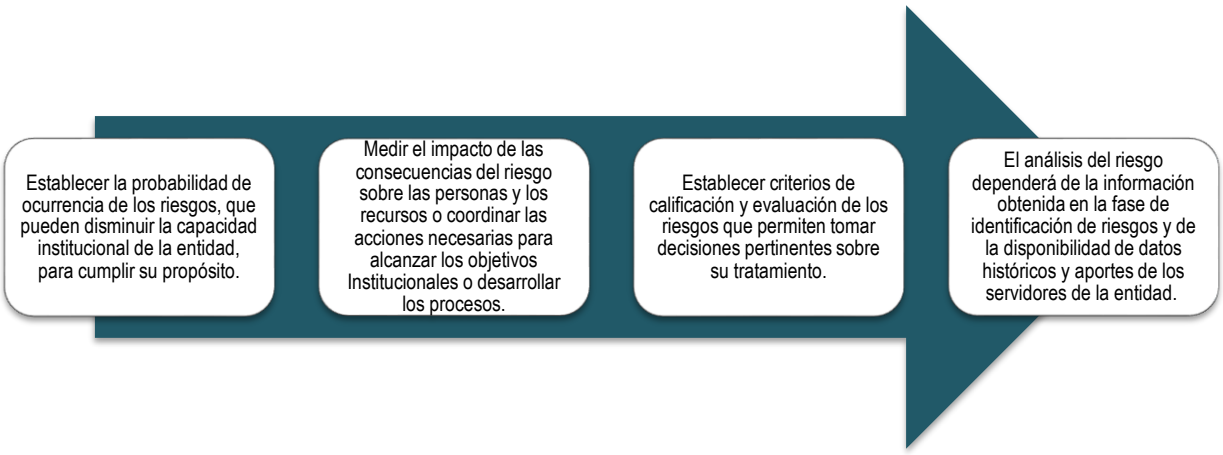
Una vez se ejecute la identificación de los activos, la Superintendencia de Transporte, definirá si gestiona los riesgos de todos los activos del inventario o solo aquellos de nivel de criticidad Alto, debidamente documentado y aprobado por la Línea Estratégica – Alta Dirección

6.5 Análisis de riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Con este análisis se establece la probabilidad de ocurrencia de los eventos de riesgo y el impacto de sus consecuencias o efectos, calificándolos y evaluándolos a fin de determinar la capacidad de la Entidad para su aceptación y manejo.

En esta etapa se busca lograr lo siguiente:



6.6 Riesgos Inherentes de Seguridad Digital

Se presentan por:

- Pérdida de la confidencialidad
- Pérdida de la Integridad
- Pérdida de la disponibilidad

6.7 Evaluación del Riesgo

La evaluación o valoración del riesgo consiste en establecer los niveles adecuados de calificación tanto de la probabilidad como del impacto para determinar realmente el nivel de vulnerabilidad de la Superintendencia de Transporte ante situaciones previsibles.

En este proceso, también se deben tener en cuenta los Factores de Riesgo enunciados durante la Etapa de Identificación.

En el caso de los riesgos de seguridad digital se deben generar indicadores para medir la gestión realizada en cuanto a la eficacia y efectividad de los planes de tratamiento implementados. Se tendrán en cuenta los siguientes indicadores en la entidad:

INDICADOR DE EFICACIA:	INDICADOR DE EFECTIVIDAD:
Porcentaje de actividades realizadas = (# de actividades realizadas / # de actividades programadas)* 100	# Riesgos materializados de confidencialidad = (# de riesgos que afectaron la confidencialidad de un activo)
Descripción: con este indicador se realiza la medición de los controles o actividades implementadas, frente a las actividades programadas.	Descripción: Con este indicador se miden los riesgos que materializados en la entidad a nivel de seguridad de la información y la afectación de alguno de los pilares de la seguridad (integridad, confidencialidad y disponibilidad).

6.7.1 Probabilidad

Nivel de ocurrencia del riesgo que puede ser determinada en términos de frecuencia o teniendo en cuenta la presencia de factores internos y/o externos que pueden propiciarlo, aunque no se haya materializado.

Entendiendo la Probabilidad como el número de veces en que puede ocurrir o se ha presentado o al menos se ha intentado presentar el riesgo.

Se puede analizar la frecuencia con la que se presentan estos eventos, teniendo en cuenta la cantidad de eventos totales que se realizan en la operación, este elemento se considera especialmente para los casos donde hay un número alto de registros para analizar y donde seguramente se han presentado los eventos, este resultado se puede considerar de acuerdo a la siguiente tabla:

Escala de probabilidad		
1	**Muy Baja**	La probabilidad de que se materialice el riesgo es menor al 10%
2	**Baja**	La probabilidad de que se materialice el riesgo es mayor o igual al 10% y menor al 20%
3	**Alta**	La probabilidad de que se materialice el riesgo es mayor o igual al 20% y menor al 50%
4	**Muy Alta**	La probabilidad de que se materialice el riesgo es mayor o igual al 50%

6.7.2 Impacto

En el impacto se evalúa la magnitud de las consecuencias que puede ocasionar al cumplimiento de los objetivos de la entidad, la materialización del riesgo, es decir, se evalúa el grado en que se afectan los objetivos de los procesos involucrados o los de la Entidad.

Para la evaluación del impacto se contemplan dos aspectos importantes:

- La Evaluación se realiza teniendo en cuenta todos los aspectos que el riesgo puede afectar, teniendo en cuenta los mismos criterios para todos los riesgos.
- El nivel de exposición en el que se encuentra la organización teniendo en cuenta la magnitud de elementos de la organización que se puedan ver afectados por el riesgo.

Los criterios que se utilizan para medir y valorar el Impacto del Riesgo, son los siguientes:

Escala de Impacto		
8	**Leve**	No afecta el logro de los objetivos del Proceso
13	**Moderado**	Afecta mínimamente el logro de los objetivos del Proceso
21	**Crítico**	Afecta medianamente el logro de los objetivos del Proceso y los de la entidad
34	**Muy Crítico**	Afecta altamente el logro de los objetivos del proceso y los de la entidad

6.7.3 Riesgo de Corrupción

De acuerdo con los lineamientos de la Ley Anticorrupción, para la evaluación del impacto del riesgo de corrupción, ninguno se evaluará con impacto leve, esto teniendo en cuenta que tratándose de riesgos de corrupción el impacto siempre será negativo.

Escala de Impacto		
13	Moderado	Afecta mínimamente el logro de los objetivos del Proceso
21	Crítico	Afecta medianamente el logro de los objetivos del Proceso y de la entidad
34	Muy Crítico	Afecta altamente el logro de los objetivos del proceso y de la entidad

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los objetivos y fines de la entidad. Para facilitar la asignación del puntaje es aconsejable responder las siguientes preguntas:

Nº	Pregunta Si el riesgo de corrupción se materializa podría…	Respuesta	
		Si	No
1	Afectar al grupo de funcionarios del proceso?		
2	Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	Afectar el cumplimiento de la misión de la entidad?		
4	Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	Generar pérdida de recursos económicos?		
7	Afectar la generación de los productos o la prestación de servicios?		
8	Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	Generar pérdida de información de la entidad?		
10	Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	Dar lugar a procesos sancionatorios?		
12	Dar lugar a procesos disciplinarios?		
13	Dar lugar a procesos fiscales?		
14	Dar lugar a procesos penales?		
15	Generar pérdida de credibilidad del sector?		
16	Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	Afectar la imagen regional?		
18	Afectar la imagen nacional?		
19	Genera daño ambiental?		
Totales		**0**	**0**
Clasificación del Riesgo: Moderado ____ Crítico _____ Muy Crítico ____			

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. V4

Respuestas:

• Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto Moderado.
• Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Crítico.
• Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto Muy Crítico.

6.7.4 Riesgo Inherente

Una vez se ha realizado el análisis y se ha determinado la evaluación de los riesgos, se obtiene el nivel del riesgo inherente, que muestra el panorama de la entidad frente a los riesgos implícitos en los procesos.

Teniendo en cuenta los resultados obtenidos al calificar cada riesgo se ubican en la matriz de impacto y probabilidad, que define las zonas de riesgo.

La forma en la cual la probabilidad y el impacto son expresados y combinados en esta matriz provee la evaluación el riesgo, a través de esta ubicación gráfica se analiza cada uno de los riesgos, determinando su ubicación inicial (riesgo inherente) y la ubicación del mismo cuando transcurran las siguientes etapas.

MATRIZ DE ACEPTABILIDAD						
PROBABILIDAD	4	Muy Alta	32	52	84	136
	3	Alta	24	39	63	102
	2	Baja	16	26	42	68
	1	Muy baja	8	13	21	34
			Leve	Moderado	Crítico	Muy crítico
			8	13	21	34
			IMPACTO			

La siguiente tabla define las zonas donde se ubican los riesgos de acuerdo a la matriz de impacto y probabilidad:

DESCRIPCIÓN DE ZONAS DE ACEPTABILIDAD	
PRIORITARIO	Un riesgo situado en esta zona de la matriz tiene una muy alta capacidad potencial de afectar el logro de los objetivos estratégicos. Por ello estos riesgos requieren una atención inmediata.
ALTO	Un riesgo situado en esta zona de la matriz significa que se requiere desarrollar acciones en el corto plazo para su gestión, debido al alto impacto que tendrían sobre los objetivos estratégicos.
MODERADO	Un riesgo situado en esta zona de la matriz significa que, aunque deben desarrollarse actividades para su gestión, estas tienen una prioridad de segundo nivel, pudiendo desarrollarse en el mediano plazo. Se deben mantener los controles existentes y el monitoreo continuo.
BAJO	Un riesgo situado en esta zona de la matriz significa que la combinación Probabilidad-Impacto no implica una gravedad significativa, por lo que no amerita la inversión de recursos y no requiere acciones adicionales para su gestión. No obstante, se deben mantener los controles existentes y el monitoreo continuo.

La identificación de riesgos, amenazas y vulnerabilidades se realizaran mediante las siguientes metodologías:

- Lluvia de Ideas
- Juicio de Expertos
- Análisis de Escenarios
- Entrevistas
- Encuestas
- Listas de Chequeo

6.8 Valoración de Controles

La herramienta efectiva para gestionar el riesgo son los controles, por esta razón la Superintendencia de Transporte debe enfocarse a implementar, mantener, mejorar y diseñar los controles que ayudan a minimizar o evitar el impacto o la probabilidad de que el riesgo se materialice, por tanto es necesario que se articule con la gestión por procesos, de tal forma que los controles hagan parte de cada uno de los modelos con que cuentan los procesos para su operación, para asegurar una buena operación.

Luego de la identificación de los riesgos, los responsables de los procesos deben identificar los controles que han sido desarrollados en cada uno de los procedimientos.
Para evaluar los controles es necesario tener en cuenta:

Para realizar el análisis de los controles, se puede dar respuesta a las siguientes preguntas:

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUA R EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	No:	0
		Detectivo:	10
		Preventivo:	15
2. Responsable	¿Está(n) definido(s) el (los) responsable(s) de la ejecución del control y del seguimiento, con el nivel de autoridad y responsabilidad adecuado?	No asignado:	0
		Asignado:	15
		Nivel de responsabilidad y Autoridad adecuado:	25

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUA R EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
3. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	No confiable:	0
		Confiable:	15
4. Periodicidad	¿La oportunidad en que se ejecuta ayuda a mitigar el riesgo o a detectar su materialización de manera oportuna?	Inoportuna:	0
		Oportuna:	15
5. Evidencia de la ejecución del control	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	No existe:	0
		Incompleta:	10
		Completa:	15
6. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	No se investigan y resuelven oportunamente	0
		Se investigan y resuelven oportunamente	15

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. V4

De acuerdo con el puntaje obtenido se puede reclasificar el riesgo:

Puntaje	Cuadrantes a disminuir en probabilidad e Impacto
0 - 85	0
86 - 95	1
96 - 100	2

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas

Es importante tener en cuenta:

- ✓ Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.
- ✓ Tratándose de riesgos de corrupción únicamente y si el control es fuerte se puede disminuir la probabilidad. Es decir, para el impacto no opera el desplazamiento.

6.9 Controles para la Mitigación de riesgos de Seguridad Digital

La Superintendencia de Transportes en aras de mitigar y tratar los riesgos de seguridad digital empleará los siguientes controles amparados en la ISO 27001:

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			
A.5	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE**	**Orientación de la dirección para gestión de la seguridad de la información**

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
		LA INFORMACIÓN	
A.5.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes
A.5.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN			
A.6	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización** **Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**
A.6.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**
A.6.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información
A.6.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).
A.6.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membresía

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
A.6.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.
A.6.2	Responsable de SI	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**
A.6.2.1	Responsable de SI	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Responsable de TICs	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	**Responsable de SI**	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**
A.7.1.1	7	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Gestión Humana	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.1.2	**Responsable de SI/Líderes de los procesos**	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
A.7.2.1	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Responsable de SI/Líderes de los procesos	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Responsable de SI	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Responsable de SI**	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**
A.7.3.1	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
GESTIÓN DE ACTIVOS			
A.8	**Responsable de SI**	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsable de SI**	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**
A.8.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Responsable de SI	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Responsable de SI	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
A.8.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Responsable de SI	Etiquetado de la información	
A.8.2.3	Responsable de SI	Manejo de activos	
A.8.3	**Responsable de TICs**	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**
A.8.3.1	Responsable de TICs	Gestión de medios removibles	
A.8.3.2	Responsable de TICs	Disposición de los medios	
A.8.3.3	Responsable de TICs	Transferencia de medios físicos	
	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.17	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	
A.17.1	**Responsable de la Continuidad**	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**
A.17.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información	
A.17.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,
A.17.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la	

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
		seguridad de la información.	
A.17.2	**Responsable de la Continuidad**	**Redundancias**	**Asegurar la disponibilidad de las instalaciones de procesamiento de la información.**
A.17.2.1	Responsable de la Continuidad	Disponibilidad de instalaciones de procesamiento de información	
	CUMPLIMIENTO		
A.18	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**	
A.18.1	**Responsable de SI**	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**
A.18.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.	
A.18.1.2	Responsable de TICs	Derechos de propiedad intelectual.	
A.18.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales
A.18.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.18.1.5	n/a	Reglamentación de controles criptográficos.	

CONTROLES DE MITIGACIÓN DE RIESGOS DE SEGURIDAD			
ISO	**CARGO**	**ITEM**	**DESCRIPCIÓN**
A.18.2	**Control interno**	**Revisiones de seguridad de la información**	
A.18.2.1	Control interno	Revisión independiente de la seguridad de la información	
A.18.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.
A.18.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
	RELACIONES CON LOS PROVEEDORES		
A.15	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**	
A.15.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores
A.15.2	Responsable de compras y adquisiciones	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores

6.10 Riesgo Residual

La valoración del riesgo residual es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados con el objetivo de establecer prioridades para su manejo y fijación de acciones.
Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

6.10.1 Plan de Manejo del Riesgo

Dentro de las acciones que se deben definir para el tratamiento del riesgo para la entidad, se contemplan las siguientes:

***Evitar el riesgo**:*

- Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos o sistemas se generan cambios sustanciales por mejoramiento, rediseño o eliminación resultado de adecuados controles y acciones emprendidas.

Mitigar el riesgo

- Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Se consigue mediante la optimización de los procedimientos y la implementación y mejoramiento de los controles.

Transferir el riesgo

- Reduce su efecto a través del traspaso o financiación de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad Las acciones están encaminadas a la disminución del impacto y especialmente cuando el aspecto que más afectan estos riesgos esta relacionados con recursos especialmente financieros, humanos o información

Aceptar el riesgo

- Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable de la gestión de este riesgo simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo, se puede utilizar para riesgo con calificaciones que ubican al riesgo en zonas bajas

Una vez identificado el tipo de acciones a seguir para el tratamiento del riesgo y de acuerdo con la evaluación y según el nivel de riesgo residual, se deben definir acciones preventivas a seguir. Es importante tener en cuenta:

- ✓ Las actividades que se determinen, deben estar enfocadas en la definición de nuevos controles que a su vez serán desplegados a través de documentación de los procesos.
- ✓ La actividad de control debe por sí sola mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones.
- ✓ Las actividades que deben incluir medidas para reducir la probabilidad o el impacto del riesgo, o ambos y llegar a la implementación de controles.

6.11 Amenazas

Son aquellas que representan situaciones que pueden hacer daño a los activos y materializar los riesgos, como son:

- Deliberadas
- Fortuitas
- Ambientales

6.12 Seguimiento y Monitoreo

El modelo integrado de plantación y gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control:

Línea de Defensa	Roles	Responsabilidad frente al monitoreo del riesgo
Estratégica	Alta Dirección Comité Institucional de Coordinación de Control Interno Comité Institucional de Gestión y Desempeño	Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno. · Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueda generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. · Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. · Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. · Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.
Primera Línea	Responsables de Proceso Secretario General, Superintendentes Delegados, Jefes de Oficina, Directores y Coordinadores de Grupo Oficina de Tecnologías de la Información y las Comunicaciones	Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. · Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueda generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. · Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. · Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. · Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. · Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. · Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
Segunda Línea	Responsables y Líderes de Proceso	Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar,

Línea de Defensa	Roles	Responsabilidad frente al monitoreo del riesgo
		evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo. • Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueda generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
	Oficina Asesora de Planeación	• Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
Tercera Línea de Defensa	Oficina de Control Interno	La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: • Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. • Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

El seguimiento y monitoreo a los mapas de riesgos, se realizará en el formato establecido para la gestión del riesgo y los Responsables de Procesos, deben reportar cada cuatro meses los avance del plan de manejo y los riesgos materializados en el periodo evaluado a la Oficina de Control Interno.

El seguimiento y monitoreo debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la implementación de acciones preventivas.

De acuerdo con el análisis y el nivel de avance realizado, los Responsables de Proceso, podrán generar acciones de mejora que consideren convenientes para asegurar el control de los riesgos.

6.13 Mapa de Riesgos Institucional

El mapa de riesgos institucional, estará conformado por los riesgos identificados en los procesos, los riesgos de seguridad digital y los riesgos de corrupción, que tengan las siguientes características:

- Se incluirán dentro del mapa de riesgos institucional, riesgos de los procesos, cuyo nivel del riesgo residual se encuentre ubicado en la zona de riesgo PRIORITARIA y ALTO.
- TODOS los riesgos tipificados como “Corrupción” y “de seguridad digital” hacen parte del Mapa de riesgo Institucional y aunque queden en la zona de riesgo BAJA se establecen acciones preventivas para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

La Oficina Asesora de Planeación, con corte a 31 de Enero de cada año, realizará la consolidación del mapa de riesgos institucional y su publicación en la página web, adicionalmente realizará las modificaciones que se requieran de acuerdo con las actualizaciones que se realicen a los mapas de riesgos de los procesos.

6.14 Comunicación y consulta (aspecto transversal)

La Superintendencia de Transporte, debe establecer mecanismos de comunicación y consulta con las partes involucradas, tanto internas como externas, durante las diferentes etapas del proceso para la gestión del riesgo, implementando estrategias para lograr el trabajo en equipo, de tal forma que se desarrollen los siguientes aspectos:

- ✓ Ayudar a establecer correctamente el contexto para los procesos.
- ✓ Garantizar que se toman en consideración las necesidades de los usuarios.
- ✓ Ayudar a garantizar que los riesgos estén correctamente identificados.
- ✓ Reunir diferentes áreas de experticia para el análisis de los riesgos.
- ✓ Garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso.
- ✓ Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica.

7. Niveles de Aceptación del Riesgo

La Superintendencia de Transporte, establece la aplicación de la administración del Riesgo a partir de la operación de los procesos, con base en las actividades definidas y manteniendo los siguientes lineamientos en todas sus actuaciones:

- Fortalecer en todos los niveles de la Entidad el desarrollo de una cultura de prevención con gestión proactiva.
- Los riesgos cuyo nivel de riesgo residual los ubique en las zonas prioritaria o alta deberán ser tratados de tal forma que su evaluación en cada vigencia permita llevarlos tan cerca como sea posible de la zona anterior, para esto las acciones definidas en el plan de manejo de riesgos deberán ser de aplicación inmediata.
- Por ninguna razón serán aceptados los riesgos de corrupción, deberán siempre tener un plan de manejo.
- Las acciones definidas en el tratamiento de los riesgos ubicados en las zonas baja y moderada deberán asegurar por lo menos mantener la misma evaluación en la revisión que se realice de los riesgos en cada vigencia.
- Los controles identificados y evaluados para actuar frente a los riesgos deberán ser idóneos y estar alineados con los riesgos y los establecidos en la documentación de los procesos en la cadena de valor.
- Los Responsables de los procesos deberán establecer planes de contingencia que permitan constituir acciones frente a la materialización de los riesgos, especialmente aquellos cuya evaluación los ha ubicado en zonas de riesgo prioritaria y alta y realizar una nueva evaluación del riesgo de acuerdo con la situación presentada.
- Los procesos donde sean identificados riesgos que no posean controles deberán diseñar controles idóneos para evitar la materialización del mismo.
- Cuando sean identificados nuevos riesgos o implementados nuevos controles para la gestión de los riesgos existentes los Responsables de procesos, deberán hacer la inclusión en el mapa de riesgos del proceso y solicitar el acompañamiento de la Oficina Asesora de Planeación para realizar la actualización y publicación correspondiente y de ser necesario la actualización del mapa de riesgos institucional.
- Cuando se identifiquen riesgos de corrupción, la probabilidad se basará en una posible ocurrencia y se evaluará el impacto como moderado, crítico o muy crítico.
- Los Responsables de los procesos que incurran en incumplimiento de los lineamientos de esta política, deberán adelantar acciones correctivas, que permitan eliminar la causa del incumplimiento.
- Los mapas de riesgos y los resultados obtenidos, se revisarán al menos una vez al año y se ajustarán si es necesario para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.
- La administración de riesgos es un proceso continuo que fluye por toda la entidad.
- Brindar atención prioritaria a los riesgos de carácter negativo y de mayor impacto potencial.
- La implementación, desarrollo y resultados deberán ser comunicados adecuada y oportunamente para una gestión más efectiva y utilización de la información por las partes interesadas.
- Se debe dar cumplimiento al artículo 73 de la Ley 1474 de 2011, relacionado con la prevención de los riesgos de corrupción – mapa de riesgos de corrupción.
- La administración del Riesgo de la Entidad es Responsabilidad de todos los servidores públicos y contratistas de la Superintendencia de Transporte.