



# Política de Administración del Riesgo

Oficina Asesora de Planeación

Instituto de Tránsito de Boyacá  
Versión  
2023



Contenido

1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO .....	3
1.1 CONCEPTOS BÁSICOS .....	3
2. OBJETIVO .....	4
3. ALCANCE .....	4
4. METODOLOGÍA APLICADA.....	4
5. NIVELES DE RESPONSABILIDAD.....	4
6. COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLÍTICA DE GESTIÓN DEL RIESGO .....	5
7. SEGUIMIENTO AL CUMPLIMIENTO DE LA POLÍTICA MONITOREO Y REVISIÓN DE RIESGOS.....	6
7.1 Monitoreo de la Primera Línea de Defensa .....	6
7.2 Monitoreo de la Segunda Línea de Defensa .....	6
7.3 Seguimiento de la Tercera Línea de Defensa .....	7
8. IDENTIFICACIÓN DEL RIESGO .....	7
9. VALORACIÓN DEL RIESGO .....	7
9.1 NIVEL DE RIESGO (RIESGO RESIDUAL) .....	7
9.2 ANÁLISIS DE RIESGOS .....	7
9.3 EVALUACIÓN DEL RIESGO .....	8
10. NIVELES DE ACEPTACION DEL RIESGO .....	9
11. SOBRE EL ANÁLISIS DE RIESGO FISCAL.....	10
12. SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN... 10	
13. SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. ....	10
14. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS .....	11
15. INCUMPLIMIENTO DE LA POLÍTICA.....	12

## 1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Son actividades encaminadas a la intervención de los riesgos del Instituto de tránsito de Boyacá, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos, de forma que mejoremos continuamente. Tiene carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión -MIPG-, la guía de administración del riesgo versión 6 y con la participación de todos los servidores de la entidad.

### 1.1 CONCEPTOS BÁSICOS

**Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Tener en cuenta: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el talento humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

**Riesgo Inherente:** Se establece a partir de la combinación con el impacto, nos permite determinar el nivel del riesgo dentro de unas escalas de severidad.

**Riesgo Residual:** El resultado aplicar la efectividad de los controles al riesgo inherente. El riesgo no es viable desaparecerlo o llevarlo a bajo en todos los casos.

**Probabilidad:** Posibilidad de ocurrencia del riesgo, dada por la exposición al riesgo. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de (1) un año.

**Impacto:** Consecuencias que puede ocasionar a la entidad por la materialización de un riesgo evento reputación y afectación económica

**Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

\* **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.

**Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

## 2. OBJETIVO

Fortalecer la implementación y desarrollo de las prácticas de la administración del riesgo en el instituto de tránsito y transporte de Boyacá ITBOY, a través del adecuado tratamiento de los riesgos identificados en cada uno de los procesos, que permita definir controles, mitigar los riesgos y asegurar el logro de los objetivos institucionales.

## 3. ALCANCE

Cubre a todos los procesos del Instituto Transito de Boyacá ITBOY, Inicia con la adopción de la política de Administración del riesgo y finaliza con la remisión del informe consolidado de monitoreo a la oficina de control interno.

## 4. METODOLOGÍA APLICADA

El Instituto de tránsito de Boyacá toma como referente los parámetros del "Modelo Integrado de Planeación y Gestión" y demás herramientas diseñadas por el Departamento Administrativo de la Función Pública – DAFP, específicamente en la guía de administración del riesgo y el diseño de controles en entidades públicas (Versión No.6 de 2023).

La metodología está definida en el procedimiento de "Administración de Riesgos" adoptado por el Instituto de tránsito de Boyacá.

## 5. NIVELES DE RESPONSABILIDAD

Para la administración de riesgos en el Instituto de Tránsito de Boyacá, se determinan los roles de los diferentes actores, teniendo en cuenta las directrices del Departamento Administrativo de la Función Pública y el Modelo Integrado de Planeación y Gestión. La responsabilidad está definida mediante las líneas de defensa así:

**Línea de Defensa Estratégica,** El Comité de Gestión y Desempeño Institucional, Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. Adicionalmente, deben definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control y hacer recomendaciones de mejoras a la política para la administración del riesgo.

En lo que corresponde a Control Interno deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta, revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. Analizar los riesgos, vulnerabilidades, amenazas institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.

✦ **Primera Línea de Defensa,** Servidores en general, líderes de procesos y sus equipos de trabajo, en sus principales responsabilidades:

- a) Realizar la identificación y actualización de los Riesgos en todas sus etapas (Contexto Estratégico, identificación, análisis y valoración del riesgo) que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.
- b) Definir, adoptar, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.
- c) Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo

**Segunda Línea de Defensa, Oficina Asesora de Planeación y sus principales responsabilidades:**

- a) Orientar y acompañar a los líderes de procesos en la identificación, análisis y valoración del riesgo.
- b) Realizar la consolidación del mapa de riesgos de corrupción del Instituto de tránsito de Boyacá.
- d) Participar en la Construcción de los mapas de Riesgos en todas sus etapas (Contexto Estratégico, identificación, análisis y valoración del riesgo).
- e) Aplicar los diferentes controles identificados para cada riesgo.
- f) Monitorear y evaluar el estado de los controles y la gestión del riesgo de manera permanente.

Para el caso de los riesgos tecnológicos y de seguridad de la información la información en la segunda línea de defensa estará incluido el proceso de Gestión tecnológica, que tendrá como responsabilidad orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia y deberá supervisar la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.

**Tercera Línea de Defensa, Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad de los riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos, La tercera línea de defensa está conformada por la Oficina de Control Interno la cual revisa de manera independiente e imparcial el cumplimiento de los objetivos institucionales y de procesos, a través del seguimiento a la adecuada gestión de riesgos, sus responsabilidades principales son:**

- a) Asesorar de forma coordinada con la Oficina de Planeación y con la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
- b) Realizar el seguimiento y evaluación a los mapas de riesgos de los procesos con énfasis en el diseño e idoneidad de los controles establecidos en los procesos
- c) Elaborar informes de seguimiento a los mapas de riesgo de la entidad y remitir a los responsables de procesos y al Comité Institucional de Coordinación de Control Interno, los resultados con el fin que emprendan las acciones necesarias.

## 6. COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLÍTICA DE GESTIÓN DEL RIESGO

- Tal como se expone en la quinta dimensión: Información y Comunicación del Modelo Integrado de Planeación y Gestión - MIPG, "la comunicación hace posible difundir y transmitir la información de calidad que se genera en toda la entidad". Siendo este un

ejercicio sistémico y de relación directa con la gestión de riesgos, se hace necesario, en cuanto a la comunicación de resultados, la revisión, el monitoreo y la evaluación, priorizar:

1. El mapa de Riesgos deberá ser divulgado y estará cargado en la página web institucional para consulta al interior del instituto de tránsito de Boyacá ITBOY.
2. Los líderes y responsables de cada proceso deben divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de acción definido.
3. La Oficina asesora de planeación impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo, con el fin de mejorar el conocimiento y apropiación del pensamiento basado en riesgos
4. Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros serán dadas a conocer, por parte de los líderes y responsables de cada proceso.
5. La consolidación del Mapa de Riesgos de Corrupción le corresponde realizarla a la oficina asesora de planeación, quien servirá de facilitador en el proceso de Gestión de Riesgos con todos los procesos.

## 7. SEGUIMIENTO AL CUMPLIMIENTO DE LA POLÍTICA MONITOREO Y REVISIÓN DE RIESGOS

El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 el Modelo Estándar de Control Interno (MECI) y las líneas de defensa como eje articulador para identificar la responsabilidad de la gestión del riesgo y control.

### 7.1 Monitoreo de la Primera Línea de Defensa

Es la actividad realizada por los líderes de procesos, planes y proyectos y sus equipos de trabajo, mediante la cual se actualizan los mapas de riesgos a su cargo y se monitorea que se estén ejecutando los controles y los planes de acción establecidos para la mitigación de los riesgos. La actualización de los mapas de riesgos de gestión, corrupción y seguridad de la información se debe realizar a más tardar el 31 de enero de cada vigencia, y se podrán realizar los ajustes y modificaciones necesarias orientadas a su mejoramiento durante el año de vigencia.

La primera línea de defensa debe reportar a la Oficina Asesora de Planeación, un informe sobre la actualización y el monitoreo realizado en los riesgos de gestión, corrupción y seguridad de la información a su cargo, teniendo en cuenta los seguimientos cuatrimestrales y la entrega de los informes los primeros 10 días del mes siguiente.

### 7.2 Monitoreo de la Segunda Línea de Defensa

La oficina Asesora de planeación brindará el apoyo metodológico a la primera línea de defensa para la identificación, análisis evaluación y tratamiento de los riesgos de gestión, corrupción y seguridad de la información. En esta etapa también se efectúa monitoreo con un mínimo de tres veces al año. La oficina asesora de planeación identificará las necesidades de revisión, actualización o mejora en los mapas de riesgos

### 7.3 Seguimiento de la Tercera Línea de Defensa

Es la etapa realizada por la Oficina de Control Interno, donde se valora de manera independiente la gestión de riesgos, verificando la efectividad de los controles, mediante actividades de evaluación y seguimiento. La Oficina de Control Interno, dentro de su función asesora presentará, luego de los respectivos seguimientos sus resultados de retroalimentación a los responsables de los procesos y subprocesos, con el fin que ellos emprendan las acciones necesarias; y en caso en que se requiera, presenten propuestas de mejoramiento y tratamiento a las situaciones detectadas.

### 8. IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control del Instituto de Tránsito De Boyacá, usando el contexto estratégico, la caracterización de cada proceso, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Para esta identificación se hace un análisis de los objetivos estratégicos y los objetivos de cada proceso del ITBOY, incluyendo el "qué", "como", "para qué", "cuando" y "cuanto".

Posteriormente se define la identificación de los puntos de riesgo (indicios de que pueden ocurrir eventos de riesgo operativo), identificando las áreas de impacto (la consecuencia económica o reputacional) y la identificación de las áreas de factores de riesgo (fuentes generadoras de riesgo).

Para la identificación de las áreas de factores de riesgo, se hace sobre los factores determinados a través de la guía versión 6 que incluye los factores proceso, talento humano, tecnología, infraestructura y eventos externos.

### 9. VALORACIÓN DEL RIESGO

Esta valoración consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia de impacto, con el fin de estimar la zona de riesgo inicial, que es la llamada zona de riesgo inherente.

#### 9.1 NIVEL DE RIESGO (RIESGO RESIDUAL)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. (matriz administración del riesgo)

#### 9.2 ANÁLISIS DE RIESGOS

Para establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

**PROBABILIDAD:** Se entiende como la posibilidad de ocurrencia del riesgo bajo los criterios de la tabla expuesta a continuación.

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%

ALTA	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000	80%
MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en unidades públicas v6

**IMPACTO:** Se definen impactos económicos y reputaciones como variables principales, se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, temas que se agrupan en impacto económico y reputacional.

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Crítico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

### 9.3 EVALUACIÓN DEL RIESGO

En esta etapa se busca confrontar los resultados del análisis de riesgo inicial (riesgo inherente) frente a los controles establecidos, con el fin de determinar la zona o nivel de riesgo final (riesgo residual). La evaluación del riesgo requiere el diseño y la valoración de los controles. Los controles son aquellas medidas orientadas a reducir o mitigar un riesgo, y se clasifican primariamente de la siguiente manera:

**Control Preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

**Control Detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

**Control Correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Adicionalmente, se cuenta con temáticas generales asociadas a los controles como se muestra en la siguiente tabla, las cuales facilitan el proceso de diseño y redacción de los mismos.

**Control manual:** controles que son ejecutados por personas.

**Control automático:** son ejecutados por un sistema.

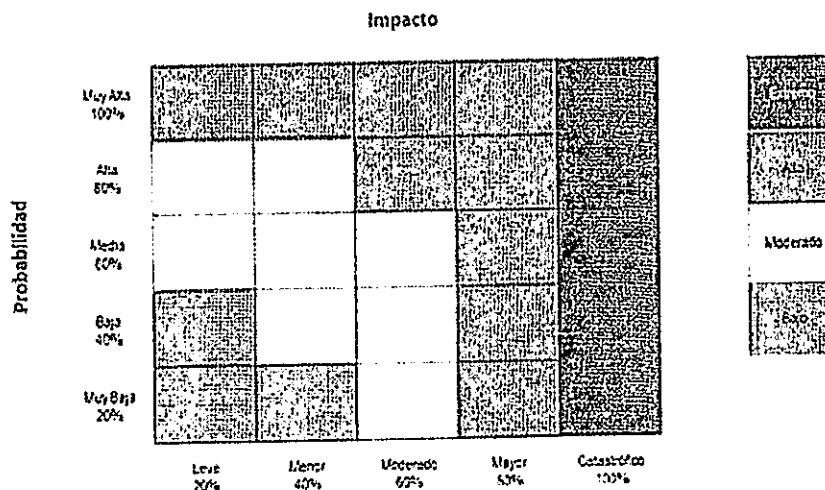


Los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla Atributos para el diseño de controles se puede observar la descripción y peso asociados a cada uno así:

CARACTERÍSTICAS		DESCRIPCIÓN	PESO	
ATRIBUTOS DE EFICIENCIA	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
ATRIBUTOS INFORMATIVOS	Frecuencia	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en el proceso	-
		Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	-
	Evidencia	Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
		Con Registro	El control deja un registro permite evidencia la ejecución del control.	-
	Sin registro	El control no deja registro de la ejecución del control.	-	

### 10. NIVELES DE ACEPTACION DEL RIESGO

Teniendo en cuenta los lineamientos de la guía 6 del Departamento Administrativo de la Función Pública DAFP, es importante mencionar que en los riesgos de gestión y seguridad digital identificados en zona baja tienen un nivel de aceptación por lo que no se da importancia de hacer planes de acción para fortalecerlos, en cuanto a los riesgos de corrupción no tienen un nivel de aceptación y se debe hacer estrategias de fortalecimiento.



### 11. SOBRE EL ANÁLISIS DE RIESGO FISCAL

La política de administración del Riesgo como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

En consecuencia, el instituto de Tránsito de Boyacá deberá analizar si existen, de acuerdo con su contexto y particularidades puntos de riesgos y circunstancias inmediatas diferentes a los identificados en el catálogo guía versión 6 (ver manual de administración del riesgo) y tenerlas en cuenta en la identificación de sus riesgos fiscales.

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta el ITBOY en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones. Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero.

### 12. SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Los riesgos de corrupción se establecen sobre procesos. Y para el caso del instituto de tránsito de Boyacá se seguirá lo establecido en el Manual de administración de riesgos y el procedimiento de administración de riesgos que permita la adecuada identificación y valoración del riesgo, además de la realización de los respectivos monitoreo y seguimientos para evitar su materialización.

### 13. SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al Modelo de Seguridad y Privacidad de la Información, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: Seguridad de la información, Arquitectura, Servicios ciudadanos digitales.

La identificación de los riesgos de seguridad de la información está determinada por las amenazas o vulnerabilidades relacionadas con los activos de información que tiene cada proceso bajo su responsabilidad.

Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de información del instituto de tránsito de Boyacá ITBOY, y algunas de ellas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

Activos de información: Un activo de información es cualquier elemento que tenga valor para la organización y que participe en el tratamiento de información, sin embargo, en el contexto de seguridad de la información son activos de información elementos tales como: hardware, software, red, personal, lugar y organización.

#### 14. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

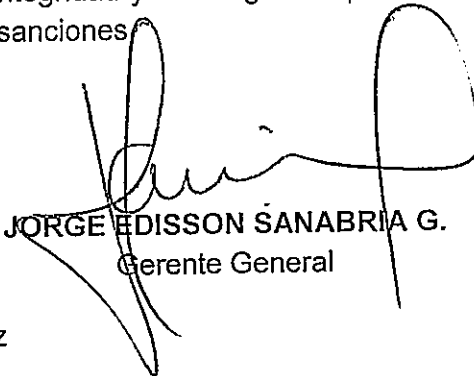
TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgo de corrupción	Líder de Proceso	<ol style="list-style-type: none"> <li>1. Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado de posible materialización.</li> <li>2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario.</li> <li>3. Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento.</li> <li>4. Efectuar el análisis de causas y determinar acciones preventivas y de mejora.</li> <li>5. Revisar los controles existentes y actualizar el mapa de riesgos.</li> </ol>
Riesgo de corrupción	Control Interno	<ol style="list-style-type: none"> <li>1. Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar.</li> <li>2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. <ul style="list-style-type: none"> <li>• Informar a discreción los posibles actos de corrupción al ente de control.</li> </ul> </li> </ol>
Riesgos de Gestión y Seguridad digital	Líder de Proceso	<ol style="list-style-type: none"> <li>1. Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo.</li> <li>2. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento.</li> <li>3. Realizar los correctivos necesarios frente al cliente e</li> </ol>

		iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos.
Riesgos de Gestión y Seguridad digital	Oficina de Control Interno	<ol style="list-style-type: none"> <li>1. Informar al líder del proceso sobre el hecho encontrado</li> <li>2. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.</li> <li>3. Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente.</li> <li>4. Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.</li> </ol>


Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

### 15. INCUMPLIMIENTO DE LA POLÍTICA

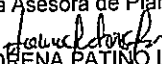
La oficina de control interno como tercera línea de defensa dando cumplimiento a la responsabilidad de evaluar la gestión de riesgos del Instituto de Transito de Boyacá determina dos formas para el incumplimiento de la política: por acción o por omisión, dando cumplimiento al código de integridad y el código disciplinario estos serán los parámetros para definir la aplicación de sanciones.



JORGE EDISSON SANABRIA G.  
Gerente General



Reviso: YESIKA TÉLLEZ MONTAÑEZ  
Jefe Oficina Asesora de Planeación



Realizo: LORENA PATINO LOPEZ  
Contratista