Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2025

Aprobó: Líder de proceso	Aprobó: Subdirectora de Planeación
Ivonne Adriana Martínez Zapata	Sandra Patricia Peñuela Arias

TABLA DE CONTENIDO

1. OBJETIVO

Brindar al IDT una herramienta que proporcione las pautas necesarias para el adecuado tratamientode los riesgos a los que están expuestos los activos de información, que permitan una adecuada tomade decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la entidad, así como permitir la recuperación delactivo de información o la trasferencia del problema a un tercero.

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento podrá ser aplicada sobre cualquier proceso del IDT, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de losriesgos de seguridad de la información.

3. MARCO NORMATIVO

Ley Estatutaria 1266 de 200: Por la cual se dictan las disposiciones generales del hábeas data
y se regula el manejo de la información contenida en bases de datos personales.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.

Ley Estatutaria 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras

disposiciones.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de2014 y se dictan otras disposiciones.

Decreto 1078 de 2015: Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de seguridad y Privacidad - MSPI de MINTIC.

CONPES 3854 de 2016: Política de Seguridad Digital del Estado Colombiano

Decreto 1499 de 2017: El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Ley 1928 de 2018: Por medio de la cual se aprueba el "Convenio sobre La Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

CONPES 3995 de 2020: Política Nacional De Confianza y Seguridad Digital

Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos Materia de acceso a la Información pública, accesibilidad web, seguridad digital, y datos abiertos.

Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.

Norma NTC-IEC/ISO 31010-2020: Técnicas de Valoración del Riesgo MIGP, Dimensión 2- Direccionamiento Estratégico y Planeación.

Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital - Versión 6 emitida por el DAFP.

Modelo de Seguridad y Privacidad de la Información de MINTIC: Tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

4. MARCO CONCEPTUAL

De conformidad con la Guía para la Administración del Riesgo a continuación, se relacionan los conceptos más importantes que tienen relación con la administración del riesgo:

- **Activo de Información:** aquello que tiene algún valor para la entidad y por lo tanto debe protegerse. Que contiene o manipula información relevante para la entidad. Abarca elementos tales como información, software, hardware, servicios, personas, entre otros.
- **Amenaza**: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Ciberseguridad**: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control o Medida**: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para ellogro de objetivos de los procesos de una entidad.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos deseguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Probabilidad**: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar elriesgo.
- **Riesgo**: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generandoun impacto negativo al negocio evitando cumplir con sus objetivos.
- **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, laspersonas o en las políticas y procedimientos.

5. POLÍTICA DE ADMINISTRACION DE RIESGOS

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte del IDT y obtener los resultados esperados, basándose en la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la entidad, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la entidad y en la probabilidad de su ocurrencia.

6. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

6.1. Generalidades.

"El Instituto Distrital de Turismo fortalece, promociona y posiciona a Bogotá como destino turístico competitivo, sostenible, seguro, accesible e incluyente, mediante la formulación e implementación políticas, planes y proyectos enfocados en las dinámicas locales. A través de la generación de información, el desarrollo de productos turísticos y la promoción de la ciudad como destino atractivo y diverso, a nivel nacional e internacional."
Misión IDT 2025

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

- Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente.
- Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos
- Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet
- Intangibles: Activo que no es tangible y no puede ser percibido físicamente.
- Componentes de Red: Equipos de infraestructura tecnológica.
- Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

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

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

6.2. Técnicas de Gestión de Riesgo.

El Instituto Distrital de Turismo mediante la herramienta de "Riesgos IDT establece 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, su priorización y estrategia de tratamiento de estos.

El objetivo de esta etapa es establecer una valoración y priorización de los riesgos, con el fin de definir los controles. Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

6.2.1. Clasificación de la probabilidad.

Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgose ha presentado en un determinado tiempo o pudiese presentarse.

ESCALA DE PROBABILIDAD		
NIVEL	**PROBABILIDAD**	**DESCRIPCION**
100%	Muy Alta	La actividad se realiza más de 1500 veces al año.
80%	Alta	La actividad se realiza entre 366 a 1500 veces al año.
60%	Media	La actividad se realiza entre 13 a 365 veces al año.
40%	Baja	La actividad se realiza entre 5 a 12 veces al año..
20%	Muy Baja	La actividad se realiza máximo 4 veces al año.

6.2.2. Clasificación del impacto.

Impacto: Hace referencia a las consecuencias que puede ocasionar en el IDT la materialización del riesgo; se refiere a la magnitud de sus efectos.

IMPACTO			
NIVEL	**PROBABILIDAD**	**DESCRIPCIÓN ECONÓMICA O PRESUPUESTAL**	**DESCRIPCIÓN REPUTACIONAL**
100%	Catastrófico	Pérdida económica superior a 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel internacional
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV.	Solo de conocimiento de algunos funcionarios

El análisis se realiza con los encargados que más conocen el proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas. Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, daños personales, entre otros. Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información.

6.3. Roles y líneas de defensa.

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

número de zona de la siguiente manera:

ZONA DE RIESGO
B: Zona de riesgo baja (color verde) 5 zonas siendo la Z-5 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 4 zonas siéndola Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 8 zonas siendo la Z-17 la de mayor riesgo
E: Zona de riesgo extrema (color vinotinto)8 zonas siendo la Z-25 la demás alto riesgo

6.4. Acciones para la apropiación.

Se promueve la transparencia y se fortalece la cultura de autocontrol y prevención, lo cual contribuye a la administración de riesgos, a través de:

- Capacitaciones para el fortalecimiento conceptual y operativo de la gestión integral de riesgos,que garanticen la competencia necesaria de los servidores y colaboradores de la Entidad.

- Estrategias de sensibilización y comunicación, que promuevan el pensamiento basado en riesgos.

- Asesorías y acompañamiento para el desarrollo del enfoque de administración de riesgos enlas actividades diarias.

- Seguimiento prioritario a los riesgos ubicados en las zonas de riesgo “extrema” y “alta” de lamatriz de riesgos, identificada para cada uno de los procesos de la Entidad.

6.5. Comunicación y consulta.

De acuerdo como se expone en la quinta dimensión de MIPG: 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 administración de riesgos, se hace necesaria la comunicación de resultados la revisión, monitoreo y evaluación.

Lo anterior, se realiza a través de SIG-P08 Procedimiento para la administración de riesgos en el IDT.

La herramienta de riesgos que define la entidad, establecida como fuente interna confiable del estado y resultados de la gestión de riesgos, incluye reportes de estados, acciones e indicadores para el manejo de los riesgos por procesos. La información resultante de la

gestión, monitoreo y evaluacióndebe ser publicada en la página web, así:

- 31 de enero de cada año, se publica el mapa de riesgos institucionales y el mapa de riesgos de corrupción a cargo de la Subdirección de Planeación.

- 30 de abril de cada año, posterior al primer ciclo de monitoreo, publicar dentro de los 10 primerosdías de mayo del mismo año, informe de monitoreo y seguimiento a cargo de la Subdirección de Planeación.

- 31 de agosto de cada año, posterior al segundo ciclo de monitoreo publicar dentro de los 10 primeros días de septiembre del mismo año, informe de monitoreo y seguimiento a cargo de la Subdirección de Planeación.

- 31 de diciembre de cada año, posterior al tercer ciclo de monitoreo y evaluación: publicar dentro de los 10 primeros días de enero del siguiente año informe de monitoreo y seguimiento a cargo de la Subdirección de Planeación.

6.6. Tratamiento, seguimiento y evaluación.

Cada líder con su equipo de trabajo presenta anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados, obtenido con el procedimiento.

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

7. NIVELES DE ACEPTACIÓN DEL RIESGO.

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

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

- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas

- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgosde seguridad de la información, desde la Subdirección de planeación se definen esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permite contextualizar una toma de decisiones de manera oportuna.

8. REGISTROS ASOCIADOS.

- SIG-P08 Procedimiento para la Administración de Riesgos en el IDT
- Manual Aplicativo de Riesgos IDT

9. METODOLOGÍA

El Plan de Tratamiento de Riesgos de Seguridad de la Información establece las actividades a desarrollar con el fin de mitigar los riesgos sobre los activos de información identificados por el IDT, de acuerdo con las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información establecida por la Función Pública y los Lineamientos del Ministerio de Tecnologías de Información y las Comunicaciones.

A continuación, se presenta el cronograma del plan de gestión de riesgos para la vigencia 2025.

PLAN DE TRATAMIENTO DE RIEGSO DE SEGURIDAD DE LA INFORMACIÓN 2025

ACTIVIDAD	RESPONSABLE	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
		Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4
Identificación de riesgos asociados a los activos de información.	Lider de TI																																																
Realizar el análisis de riesgos de Seguridad Digital acorde a la realidad operacional del IDT.	Lider de TI																																																
Cargar los Riesgos actualizados en la plataforma de gestión de riesgos del IDT.	Lider de TI																																																
Desarrollar y ejecutar las actividades definidas para mitigar o reducir cada riesgos identificado.	Lider de TI																																																
Reportar y hacer seguimiento a la implementación de controles.	Lider de TI																																																
Identificar y documentar las oportunidades de mejora.	Lider de TI																																																

Es importante mencionar que el IDT ha venido gestionando riesgos de seguridad informática propendiendo por la integridad, seguridad y disponibilidad de la información, en consecuencia, para la identificación y actualización de riesgos de seguridad informática es preciso tener claridad de los activos de información identificados, con el fin de priorizar en implementar controles de acuerdo a su criticidad. Una vez se realice dicha actividad se debe proceder con el respectivo cargue de riesgos en la plataforma definida para tal fin y se ejecutan las actividades pertinentes de manera periódica para reducir, aceptar o mitigar los riegos identificados. Finalmente, y de manera semestral se identifican las oportunidades de mejora en la gestión de riesgos.