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

Aprobó: Líder de proceso	Aprobó: Jefe Oficina Asesora Planeación
René Guarín Cortés	Oscar A. Sarmiento Ceballos

Tabla de Contenido

1. OBJETIVO

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

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será 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 los riesgos de seguridad de la información.

3. MARCO NORMATIVO

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.

- Norma NTC-IEC/ISO 31010-2013: Técnicas de Valoración del Riesgo MIGP, Dimensión 2- Direccionamiento Estratégico y Planeación.
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- 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).
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

4. MARCO CONCEPTUAL

De conformidad con la Guía para la Administración del Riesgo (DAFP, 2018), a continuación, se relacionan los conceptos más importantes que tienen relación con la administración del riesgo:

- **Riesgo**: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **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).
- **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad**: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.
- **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 el logro de objetivos de los procesos de una entidad.

5. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

5.1. Generalidades.

"El Instituto Distrital de Turismo promueve el desarrollo integral y fortalecimiento económico

de Bogotá, a través del turismo como integrador social, económico y mitigante del impacto ambiental; mediante políticas, planes y proyectos desde las vocaciones locales, la generación de información, la promoción de ciudad a nivel nacional e internacional como destino competitivo, sostenible, seguro, accesible e incluyente, que se articula con la región para mejorar la calidad de vida de sus habitantes y los actores de la cadena de valor del sector."
Misión IDT 2020-2024

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

a) **Primarios:**

- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) Soporte

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

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

5.2. Metodología.

El Instituto Distrital de Turismo, conforme a la herramienta de "Riesgos IDT", la estimación 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, su priorización y estrategia de tratamiento de estos.

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

5.2.1. Clasificación de la probabilidad.

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

ESCALA DE PROBABILIDAD		
NIVEL		**DESCRIPCION**
1	**Raro**	Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	**Improbable**	Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	**Posible**	Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	**Probable**	Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	**Casi Seguro**	Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

5.2.2. 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.

VALOR DE IMPACTO			
NIVEL		**DESCRIPCION**	**ESCALA**
1	**Insignificante**	Impacta negativamente de forma leve la imagen y operación de un rol.	**>=1 y <=4**
2	**Menor**	Impacta negativamente la imagen y de manera importante la operación de un proceso.	**>=5 y <=8**
3	**Moderado**	Afecta negativamente la imagen entidad a nivel distrital por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos.	**>=9 y <=12**
4	**Mayor**	Imagen entidad a nivel distrital afectada, al igual que la operación por el incumplimiento en la prestación de servicios.	**>=13 y <=16**
5	**Catastrófico**	Imagen entidad afectada a nivel distrital e nacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la entidad y el incumplimiento de sus objetivos estratégicos. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	**>=17 y <= 20**

Se sugiere realizar este análisis con todas o las personas que más conozcan del 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 que se muestran más adelante. 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.

5.3. 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 matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Las zonas de riesgo 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 siendo la 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 vino tinto) 8 zonas siendo la Z-25 la de más alto riesgo

5.4. 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 en las actividades diarias.
- Seguimiento prioritario a los riesgos ubicados en las zonas de riesgo "extrema" y "alta" de la matriz de riesgos, identificada para cada uno de los procesos de la Entidad.

5.5. 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:
DE-P08. Procedimiento para la administración de riesgos en el IDT

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 evaluación, debe 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 OAP.
- 30 de abril de cada año, posterior al primer ciclo de monitoreo, publicar dentro de los 10 primeros días de mayo del mismo año, informe de monitoreo y seguimiento a cargo de la OAP.
- 31 de agosto de cada año, posterior al segundo ciclo de monitoreo publicar dentro de los 10 primeros días de mayo del mismo año, informe de monitoreo y seguimiento a cargo de la OAP.
- 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 OAP.

5.6. Tratamiento, seguimiento y evaluación.

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

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

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

6. 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 riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

7. REGISTROS ASOCIADOS.

DE-P08 Procedimiento para la Administración de Riesgos en el IDT
DE-F18 Formato de Mapa de Riesgos
Manual Aplicativo de Riesgos IDT

8. METODOLOGÍA

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por IDT, a través de los decretos emitidos. De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar, 2. Planear, 3. Hacer, 4. Verificar, 5. Actuar

CRONOGRAMA	**Marzo**				**Abril**				**Mayo**				**Junio**				**Julio**				**Agosto**				**septiembre**				**Octubre**				**diciembre**			
	S1	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
Valoración de Activos																																				
Realizar la Identificación de los Riesgos																																				
Diseño del Plan de tratamiento de riesgos																																				
Desarrollo, ejecución de Actividades definidas en el plan de tratamiento de riesgos																																				
Valorar del riesgo Residual																																				
Informe de Riesgos a la gerencia																																				