SECRETARÍA DISTRITAL DE PLANEACIÓN

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Responsables:

Líder de Gobierno Digital - Director de Sistemas
Representante de la Alta Dirección - Subsecretario/a de Información y Estudios Estratégicos
Dirección de Planeación

Tabla de contenido

1 INTRODUCCIÓN

La Alta Dirección de la Secretaría Distrital de Planeación, SDP, ha establecido una política clara de apoyo y compromiso frente a los temas relacionados con la Seguridad de la Información, que se ve reflejada en la Resolución 0137 de 2018, "*por la cual se ajusta el Sistema Integrado de Gestión de la Secretaría Distrital de Planeación…*", la aprobación de la Política de Seguridad de la Información - A-LE-429, la Resolución 1771 de 2018, "*por la cual se establecen los responsables de la Política de Gobierno Digital*" y demás instrumentos que reglamentan ésta política.

De igual forma, teniendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soportará el habilitador transversal de la Seguridad de la Información de la SDP; dentro de los instrumentos que apoyan la implementación del MSPI de la Entidad, en la Fase 3 – Implementación, se encuentra la necesidad de definir el Plan de Tratamiento de Riesgos de Información que permitirá la identificación, análisis, valoración y tratamiento de riesgos relacionados con la información institucional ya sea física o digital, en cada uno de sus procesos, con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad.

2 OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica alineada al instructivo para la Gestión del Riesgo (E-IN-005), que permita a los responsables de los procesos de la SDP gestionar los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información que hacen parte del Registro de Activos de Información de la SDP (RAI) y que sean identificados con una criticidad alta por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad.

3 ALCANCE

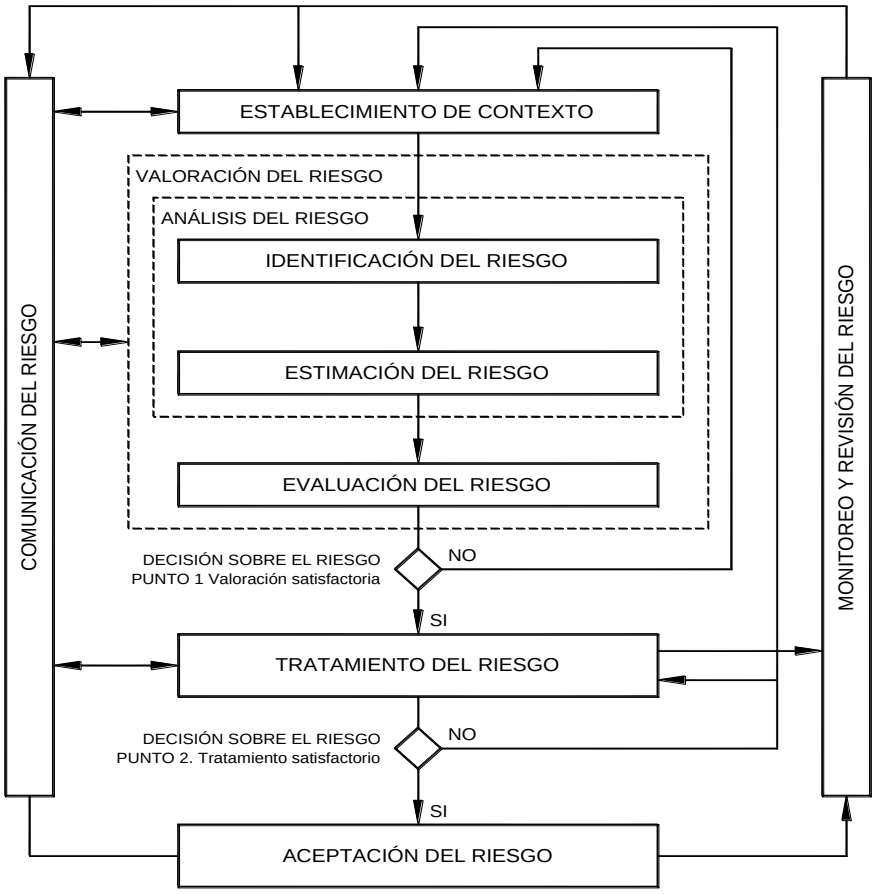
La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información de la SDP identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información de la SDP (RAI); con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4 VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

La Secretaría Distrital de Planeación asume la gestión de los riesgos de información (incluyendo los riesgos tecnológicos) con base en la Política Institucional de Administración del Riesgo y recomendaciones de las ISO 31000 y 27005.

Se tomará como base para la gestión de los riesgos de información, el ejercicio documentado de identificación del contexto organizacional, aplicado a cada uno de los procesos estratégico, misional y de apoyo de la entidad; de igual forma se parte de la metodología de tratamiento de riesgo de la Entidad, definido en el Instructivo para la Gestión del Riesgo (E-IN-005), razón por la cual este documento solamente abordará las etapas de identificación y clasificación del riesgo cuando se trata de un “Riesgo de Seguridad Digital”

Modelo de Gestión de Riesgos De Seguridad de la Información



Proceso para gestión de riesgos de acuerdo a ISO 27005

5 IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD DIGITAL

Este documento apoya al dueño de la información o delegado para la etapa de identificación y clasificación del riesgo cuando se trata de un "Riesgo Seguridad Digital", alineado con el Instructivo para la Gestión del Riesgo (E-IN-005) – Pasos 4 y 5, en donde es necesario tener en cuenta que estos riesgos serán tratados en sus etapas iniciales y finales de acuerdo al mencionado instructivo y para los activos de información que en el Registro de Activos de Información de la SDP (RAI) (A-LE-283) hayan sido clasificados como de criticidad "Alta" por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad, razón por la cual se consideraría que existe un riesgo de la información en alguno de éstos tres pilares.

Al respecto, se debe tener en cuenta que la criticidad de los activos de información fue valorada de acuerdo a la Guía para la Gestión y Clasificación de Activos de Información de Min TIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital, midiéndose por los tres pilares de la seguridad de la información "CONFIDENCIALIDAD", "INTEGRIDAD", "DISPONIBILIDAD" según la clasificación que determina el numeral 7 de dicha Guía, de la siguiente manera:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1: Criterios de Clasificación

Tras la valoración del activo de información por cada uno de los tres pilares en el Formato Registro De Activos De Información (RAI) (A-FO-209) se clasifica el Activo en el nivel de criticidad “ALTA”, “MEDIA” ó “BAJA”), de acuerdo a las condiciones de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC de la siguiente manera:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2: Niveles de Clasificación

El resultado de esta valoración se refleja finalmente en el documento SIG Registro de Activos de Información (RAI) (A-LE-283), a partir del cual se seleccionan para tratamiento de riesgos, todos los activos de información clasificados con nivel de criticidad “ALTA”

De acuerdo con lo especificado en en la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas y con ayuda del Módulo de Gestión del Riesgo del sistema SIPG se deberá especificar la amenaza de acuerdo a la siguiente tabla de referencia:

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

Tras el registro de una amenaza, se deberán especificar las vulnerabilidades, de acuerdo con la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas y con ayuda del Módulo de Gestión del Riesgo del aplicativo SIIP, se deberá especificar la vulnerabilidad de acuerdo a la siguiente tabla de referencia:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla

Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005

4 TERMINOLOGÍA

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los

métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: 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.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la 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 Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.