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

SECRETARÍA DISTRITAL DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVOS 4
3. ALCANCE 5
4. DEFINICIONES TECNICAS 5
5. REFERENCIAS NORMATIVAS 8
6. DOCUMENTOS DE REFERENCIA 9
7. JUSTIFICACIÓN 10
8. ACTIVIDADES A DESARROLLAR 11
9. CONTROL DE CAMBIOS 14

1. INTRODUCCIÓN

Las tendencias tecnológicas de los últimos años han permitido crear de manera exponencial cantidades de información que jamás en la historia de la humanidad se había creado, transportado, transformado o compartido, cambiando la manera de ver las cosas por parte de todos nosotros. Particularmente en las entidades del estado, se hace necesario contar con la conciencia del poder de la información, el alcance que tiene la misma y principalmente la entrega oportuna que se debe dar a la ciudadanía.

En la Secretaría Distrital de Seguridad, Convivencia y Justicia se cuenta con gran volumen de información, relevante para el Distrito, manejada física, digital y electrónicamente, en su mayoría con el propósito de dar cumplimiento a los objetivos de la entidad, requiriendo utilizar mecanismos adecuados para cuidar el derecho a la intimidad personal, familiar y al buen nombre de todos los beneficiarios de la entidad, permitiendo el acceso a los documentos públicos y evitando el acceso a los que se consideren reservados o confidenciales.

Para lograr la toma de decisiones con base en información de altos estándares de calidad, en materia de política y gestión de Seguridad, Convivencia y Acceso a la Justicia, que permita tomar decisiones, resolver problemas y prestar los servicios a los ciudadanos y funcionarios de la entidad, es necesario que esta sea real, oportuna y de acceso a las personas que lo requieren.

Internacionalmente la norma ISO (Organización Internacional de Normalización) 30001:2009 establece un Sistema de Gestión de Riesgos de cualquier tipo, incluyendo riesgos asociados a la información, esto permite reducir las falencias propias de la información a través de un tratamiento continuo y apropiado de los controles que mitiguen las afectaciones negativas a la organización. Permite identificar, divulgar y medir los posibles incumplimientos a los objetivos institucionales de la entidad.

La Secretaría Distrital de Seguridad, Convivencia y Justicia, establece la actualización para el segundo semestre del 2020 del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Cabe resaltar que en el primer semestre se desarrollaron actividades asociadas al autodiagnóstico de seguridad de la información con corte a diciembre 2019, por tal motivo se definen y actualizan las actividades del Plan de Tratamiento de Riegos de Seguridad y Privacidad de la Información para el segundo semestre del año 2020, con el fin de incrementar los niveles de confidencialidad, integridad y disponibilidad de la información de la entidad. Adicionalmente se adoptan los lineamientos generales del Plan Nacional de Desarrollo 2018-2022 que traza el curso de acción en la construcción de respuestas a los grandes problemas globales (terrorismo, ciberseguridad, lucha contra las drogas, corrupción, ausencia de democracia) buscando fortalecer la Inteligencia y Contrainteligencia en el Ciberespacio identificando las oportunidades, riesgos y amenazas que afectan a Colombia. También se tomaron las recomendaciones dadas por la OCI respecto a la auditoría realizada a la dirección de Tecnologías y Sistemas de Información durante el segundo semestre del 2020. Se desarrolla el ejercicio de alinear el presente documento a lo descrito en el Plan Anual de Adecuación y Sostenibilidad SIGD-MIPG 2020. Por otro lado, la Dirección de Tecnologías y Sistemas de información viene trabajando en la formulación de un plan de trabajo para la actualización y/o elaboración de 24 procedimientos, 3 planes, 3 políticas y 1 manual, para las vigencias 2020 - 2024. Adicionalmente se tiene la meta de desarrollar "El 50% de la Política de Seguridad Digital acorde a la normativa distrital y nacional en la Secretaría de Seguridad, Convivencia y Justicia" asociada al Plan Distrital de Desarrollo.

2. OBJETIVOS

Objetivo General

Plan de actividades para identificar posibles afectaciones a la información física, digital y electrónica que almacena, recolecta, produce y gestiona la Secretaría Distrital de Seguridad, Convivencia y Justicia, la identificación de controles físicos o

lógicos para mitigar los daños e incrementar los niveles de confidencialidad, integridad y disponibilidad de la información.

Objetivos Específicos

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información da cumplimiento a uno de los objetivos generales de la Política de Seguridad de la Información asociados a los riesgos de la entidad, a través de los siguientes objetivos específicos:

1. Analizar el riesgo que deberá cubrir la totalidad del alcance establecido del tratamiento en donde se tomará la Matriz de Activos de Información cuyo resultado de Criticidad sea alto.
2. Establecer lineamientos para Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Secretaría.
3. Identificar los riesgos de Seguridad y Privacidad en la entidad.

3. ALCANCE

Establecer las actividades a realizar en el año 2020 para la identificación de riesgos de Seguridad y Privacidad de la Información con sus correspondientes controles, alineado al cumplimiento de la Política de Seguridad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, en el objetivo de Gestionar los riesgos de Seguridad y Privacidad de la Información de la entidad.

4. DEFINICIONES TECNICAS

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:

1. Personas: Incluyendo sus calificaciones, competencias y experiencia.
2. Intangibles: Ideas, conocimiento, conversaciones.

3. Electrónicos: Bases de datos, archivos, registros de auditoria, aplicaciones, herramientas de desarrollo y utilidades.
4. Físicos: Documentos impresos, manuscritos y hardware.
5. Servicios: Servicios computacionales y de comunicaciones.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Falla: Daño o afectación de un dispositivo por un periodo determinado. Las fallas las podemos clasificar dependiendo del tipo de evento que la ocasione en: fallas accidentales, intencionales o naturales.

Información: Entendemos por información cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:

1. Una noticia que escuchamos por la radio.
2. Una señal de tráfico que advierte un peligro.
3. Una fórmula que usamos en un problema.

Acción de tratamiento: Actividad planificada, temporal y única, diseñada y ejecutada para eliminar o reducir las causas de los riesgos o disminuir el impacto de una eventual materialización de los mismos.

Control: Actividad de monitoreo ejecutada sistemáticamente y definida en el marco de actividades establecidas en los procesos, definida con el propósito de reducir la probabilidad o el impacto de la materialización de los riesgos, dando seguridad razonable el cumplimiento de los objetivos

Causas: Fallas, debilidades, condiciones, restricciones o circunstancias ciertas o potenciales, que pueden dar lugar al evento, pueden aumentar la exposición al riesgo o potenciar sus consecuencias.

Consecuencias: Efectos directos e indirectos sobre los recursos y objetivos del proceso si el riesgo se materializa.

Evento: Incidente u ocurrencia interna o externa al proceso, que se da en un lugar o espacio de tiempo particular, de forma súbita o accidental y que impacta el cumplimiento de los objetivos de un proceso.

Indicador de riesgo: Es una herramienta de medición que permite monitorear, de manera preventiva, el comportamiento de los riesgos. Indica cambios en el nivel o exposición a los mismos y permite la identificación de tendencias en el comportamiento de los mismos, generando alarmas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización.

Riesgo: Todo evento de ocurrencia incierta que de materializarse genera un impacto, positivo o negativo, en el logro o cumplimiento de los objetivos de los procesos o proyectos. Se puede medir en términos de la probabilidad de ocurrencia y el impacto de sus consecuencias.

Riesgo de Seguridad de la Información: Evento que afecta o amenaza la confidencialidad, integridad y disponibilidad de la información y puede impactar las funciones el logro de los objetivos organizacionales.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

Confidencialidad: propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.

Integridad: propiedad de exactitud y completitud.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por la entidad.

Gestión del riesgo: un 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.

ICC: Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.

Impacto: se entienden 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.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

Riesgos 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, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

Riesgo residual: nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

5. REFERENCIAS NORMATIVAS

- NTC/ ISO/IEC 27001: Se centra en las buenas prácticas para gestión de la seguridad de la información, utilización de la norma para apoyar la implantación

del SGSI en cualquier tipo de organización.

- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices
- Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- CONPES 3854 del 11 de abril de 2016, 3.2. Estrategia de gestión de riesgos de seguridad digital. El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco.
- Decreto 612 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
- Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones.
- Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 y se establece el Modelo Integrado de Planeación y Gestión (MIPG).

6. DOCUMENTOS DE REFERENCIA

- Política de Administración de Riesgos PO-DS-1 2020 en la cual se estructuran las pautas de la Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ para identificar, analizar, controlar y mitigar los Riesgos por Proceso, Riesgos de Corrupción y Riesgos de Seguridad Digital
- Resolución 000851 del 31 de diciembre de 2019 por la cual se adopta la Política de Seguridad y Privacidad de la Información y se define lineamiento para su uso, actualización y aplicación.
- Guías de Seguridad y Privacidad establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.
- Manual de Gobierno Digital Versión 7 de abril del 2019

- Decreto 612 del 2018 Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del estado.

7. JUSTIFICACIÓN

Con la transformación de la Estrategia de Gobierno en Línea a Política de Gobierno Digital, se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público y aporte a la sociedad.

De acuerdo a lo definido por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC “Se debe hacer énfasis en el desarrollo de modelos de seguridad de la información que promuevan el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”

La confianza digital es la principal característica del entorno en donde se relaciona el Estado con los ciudadanos y los demás actores del ecosistema digital, en este entorno se hace fundamental el componente de seguridad digital para las entidades del estado como eje transversal al correcto funcionamiento de la Política de Gobierno Digital implementada en cada entidad, por tal motivo se hace necesario actualizar el cronograma de actividades del Plan de Tratamiento de Riesgos del 2020 para alinearlo al proyecto de inversión para el cuatrienio 2020-2024 y más específicamente para encausar el Modelo de Seguridad y Privacidad de la Información a la meta del Plan Distrital de Desarrollo 2020-2024 “*Implementar el 50% de la Política de Seguridad Digital acorde a la normativa distrital y nacional en la Secretaría de Seguridad, Convivencia y Justicia*, todo esto alineado al Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas.

8. ACTIVIDADES A DESARROLLAR

El Plan da cumplimiento a las actividades asociadas a la seguridad de la información y los riesgos y su tratamiento permiten incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad, a través de la identificación de riesgos, seguimiento y definición de controles, para lo cual se realizarán las siguientes actividades dirigidas a toda la entidad:

Estas actividades se desarrollarán de Julio a diciembre del 2020 en el siguiente orden:

ID	Nombre Actividad/Tarea	Responsable	2020																			
			AGOS				SEPT				OCT				NOV				DICIEM			
		Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	**RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**																					
1.1	Identificar, clasificar los riesgos de Seguridad Digital																					
1.2	Revisar y/o actualizar la Metodología de Riesgos de Seguridad Digital	Contratista de Seguridad de la Información, Profesional Oficina Asesora de Planeación																				
1.3	Revisar de la Matriz de Activos de Información de la SDSCJ (Debe estar 100% diligenciada)	Contratista de Seguridad de la Información																				
2.	**VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL**																					
2.1	Analizar, Identificar y valorar los riesgos de Seguridad y Privacidad de la Información en la Matriz, implementar los mapas de calor y ponderaciones.	Contratista de Seguridad de la Información, Profesional Oficina Asesora de Planeación																				

ID	Nombre Actividad/Tarea	Responsable	2020																			
			AGOS				SEPT				OCT				NOV				DICIEM			
		Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
2.2	Evaluar los riesgos identificados de seguridad y/ o corrupción que se asocien a la valoración y dar posteriormente la aprobación.	Contratista de Seguridad de la Información																				
3.	**TRATAMIENTO DE RIESGOS**																					
3.1	Actualizar el documento de Tratamiento riesgos de Seguridad y Privacidad de la Información	Contratista de Seguridad de la Información																				
4.	**CONSTRUCCION DE LOS PLANES DE SEGURIDAD DE A INFORMACIÓN PARA EL CUATRENIO 2020 A 2024**																					
4.1	Plan de Tratamiento de Riesgos 2020 – 2024	Contratista de Seguridad de la Información																				

9. CONTROL DE CAMBIOS

Control de Cambios		
Fecha	**Versión**	**Descripción**
23/07/2018	1	Creación del documento.
13/03/2020	2	Se ajustan logos de Alcaldía y de la Certificación ISO 9001-2015 Calidad
31/08/2020	3	Se ajusta y actualiza el documento
21/10/2020	4	Por solicitud de la Dirección de Tecnologías y Sistemas de Informacionse ajusta nuevamente y actualiza el documento.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	Francisco Javier Diaz Mendez	Jorge Eliecer Velásquez Perilla Eliecer Vanegas Murcia	Diana Lucia Sánchez Morales
CARGO	Contratista Dirección de Tecnologías y Sistemas de la Información	Contratista Dirección de Tecnologías y Sistemas de la Información Contratista Dirección de Tecnologías y Sistemas de la Información	Directora de Tecnologías y Sistemas de Información.
FIRMA