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

2023

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La materialización de los riesgos de seguridad de la información afecta el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales y en este sentido, los activos de información deben alinearse a la Política de Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, cumpliendo las actividades de identificar, analizar, controlar y mitigar los riesgos de seguridad de la información que podrían afectar de manera negativa el logro de los objetivos institucionales.

Bajo esa perspectiva, la gestión de riesgos de seguridad de información se presenta como una herramienta para el desarrollo, implementación y mejora continua de la Entidad frente a la prestación de servicio y manejo de la información, tanto física como digital.

Es así como, internacionalmente la norma ISO (Organización Internacional de Normalización) 31000:2018 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.

En virtud de lo expuesto, se define el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023, de acuerdo con las necesidades de la Entidad y al cumplimiento normativo aplicable, dando continuidad a los procesos de mejora continua a partir de la identificación de riesgos inherentes asociados con la integridad, confidencialidad y disponibilidad de la información.

2. OBJETIVOS

2.1. Objetivo General

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información acorde con los lineamientos definidos en la Política de Administración de Riegos de la Entidad, con el propósito de adoptar medidas y acciones encaminadas a reducir y/o eliminar riesgos de Seguridad de Información mediante la definición, valoración y aplicación de controles.

2.2. Objetivos Específicos

a. Revisar y actualizar los activos de información de acuerdo con las Tablas de Retención Documental y la normatividad vigente aplicable a cada uno de los procesos de la Entidad.
b. Gestionar los riesgos de Seguridad y Privacidad de la información de acuerdo a lo definido en la Política de Administración del Riesgo de la Entidad.
c. Fortalecer y apropiar el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información.
d. Definir un cronograma de actividades que permita la administración y gestión de los riesgos de la Entidad a nivel de Seguridad de la Información.

3. ALCANCE

El plan de tratamiento de riesgos aquí propuesto, establece los criterios de gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, buenas prácticas que contribuyen a prevenir y/o mitigar los incidentes que afectan el logro de los objetivos.

El presente documento aplica lo definido en la Política de Administración de Riesgos PO-DS-1 versión 7, para desarrollar las actividades de Identificación y/o actualización de activos de la información, de riesgos Inherentes, Valoración de riesgos, Identificación y evaluación de controles, así como la efectividad de la aplicación de los mismos

4. GLOSARIO.

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta a la definición de términos establecidos en el Ítem 3 “Glosario de Términos” del MA-GT-01 “Manual de Seguridad y Privacidad de la información” aprobado para la Entidad.

5. MARCO NORMATIVO.

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta al Ítem 4 “Marco Legal” establecido en el MA-GT-01 “Manual de Seguridad y Privacidad de la

información" aprobado para la Entidad.

6. JUSTIFICACIÓN.

El Gobierno Nacional plantea la Política de Gobierno Digital, con la cual se genera un nuevo enfoque, en donde no sólo la Administración Pública sino también los diferentes actores de la sociedad tales como el ciudadano, la empresa privada, entes externos, etc., son elementos fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas de las entidades, determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público y aporte a la sociedad.

La transformación digital del estado colombiano es una fuente de generación y uso de información, originando riesgos que deben ser identificados, analizados y gestionados de manera efectiva. El Gobierno Nacional plantea el "Modelo Integrado de Planeación y Gestión "– MIPG, el cual da directrices de como las entidades deben manejar la administración y gestión de riesgos.

De acuerdo a lo requerido por el Artículo 1 del Decreto 612 del 2018 expedido por el Gobierno Nacional, la Política de Administración del Riesgo de la Entidad y las directrices dadas por el Ministerio de Tecnologías de las Tecnologías de las Información y las Comunicaciones – MinTIC, se hace necesario actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023, en el que se definen las acciones para gestionar los riesgos de seguridad de la información salvaguardando los principios de integridad, confidencialidad y disponibilidad.

7. RESULTADOS ACTUALES.

De acuerdo a las actividades realizadas para la actualización de los activos de información y riesgos de seguridad digital para la vigencia 2022 se obtuvieron los siguientes resultados así:

7.1. Levantamiento Activos de Información.

Se realiza actualización de los documentos Guía G-FD-1 "**Guía de Gestión de Activos de Información**". Ver. 4 -2022 y Formato F-FD-513 "**Registro Activos de Información**" Ver. 5 – 2022 de acuerdo con las directrices

establecidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas version 5 – 2022 y el Modelo Nacional de Gestión de riesgo de seguridad de la información Anexo 4. DAFP

Enlace de consulta de los documentos:

Guía de Gestión de Activos de Información G-FD-1:
https://portalmipg.scj.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaWktLUTArYmlHSEIzelBHdXVtcGhPRFg1aTFkR2lpTHYxZDl0TWxydng5b0E9PQ==&nivel2=dTcwZ2cySTlSVklwaldXTUh1WU4rZUl4aUFyenpLV3VsU1ZmL24zR29sYz0=
Registro de Activos de Información F-FD-513:
https://portalmipg.scj.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaYjlZMUF6QVBjMk9XYWRlVW5KWUI5MHhKckpUc3RnRTdPZFJLVU02STBkemc9PQ==&nivel2=QXU4S3ZKa1JJcTVUSmpEUW9HeDRRTzVzZHNnVXZyWklBNlYwOVhPaUxCYz0=

El levantamiento de activos de información de la entidad se realizó para los 18 procesos y 26 áreas que la conforman, de acuerdo con la actualización de las tablas de retención documental, donde se validaron y aprobaron mediante acta para toda la entidad un total de 331 activos de información, los cuales fueron valorados por el personal de las áreas encargadas de acuerdo con los principios de confidencialidad, integridad y disponibilidad de información, de los cuales 79 activos fueron clasificados con una valoración de criticidad Alta, 164 activos fueron clasificados con una valoración de criticidad Media y 88 activos fueron clasificados con una valoración de criticidad Baja.

Se realiza la aprobación de los activos de información de acuerdo con las mesas de trabajo con las diferentes áreas que conforman la Entidad, mediante Acta de aprobación de activos de información y la publicación del registro de activos de información en el sitio web https://datosabiertos.bogota.gov.co/ y en el sitio web de la entidad www.scj.gov.co

Enlace de consulta de los documentos:

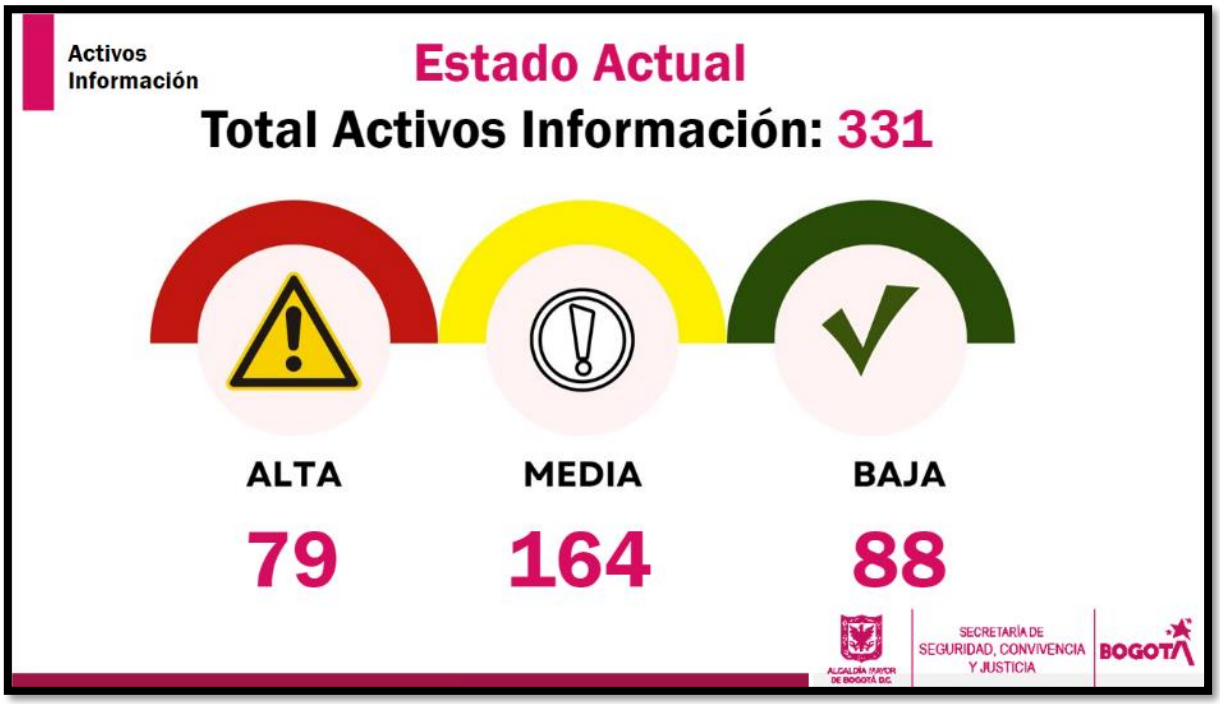
Datos Abiertos Bogotá:

https://datosabiertos.bogota.gov.co/dataset?organization=secretaria-distrital-de-seguridad-convivencia-y-justicia&tags=activos

Secretaria Distrital de Seguridad, Convivencia y Justicia:

https://scj.gov.co/es/transparencia/datos-abiertos/registros-activos-informacion

Los activos de información son la base fundamental requerida por la Política de Administración de Riesgos, para realizar el levantamiento de riesgos de seguridad digital.



7.2. Riesgos de Seguridad Digital.

El levantamiento de Riesgos de Seguridad Digital de la entidad se realizó para los 18 procesos y 26 áreas que la conforman de acuerdo a los parámetros establecidos en la Política de Administración de Riesgos, de lo cual se realizaron mesas de trabajo con cada uno de las áreas de forma presencial y virtual donde se dio amplia información sobre las actividades referentes al diligenciamiento del F-DS-898 “Matriz de Riesgos de Seguridad Digital” para lograr la consolidación de la

información requerida, así como el desarrollo de ejercicios prácticos sobre levantamiento de riesgos de seguridad digital.

Sobre el ejercicio de levantamiento de riesgos de seguridad digital se tomaron como referencia los 79 activos de información clasificados con una valoración de criticidad alta aprobados en las actividades previas de levantamiento de activos y validados mediante acta para toda la entidad, con un total de 28 riesgos de Seguridad Digital de acuerdo a los principios de confidencialidad, integridad y disponibilidad de información, donde se realizó la definición de 36 controles estructurados de acuerdo a los parámetros establecidos en política de administración de riesgos de la Entidad.

La matriz de riesgos de seguridad digital identificados para la vigencia 2022, se encuentra publicada en la página Web de la Secretaría Distrital de Seguridad Convivencia y Justicia en el siguiente enlace:

https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion

8. ACTIVIDADES A DESARROLLAR.

El Plan definido da cumplimiento a las actividades asociadas a la gestión del Sistema de Gestión de Seguridad de la Información y la Política de **Administración de Riesgos" – PO-DS-1**.

El detalle de las actividades a realizar, tiempo de ejecución de estas, responsable y participantes, para adelantar la implementación de este plan se definen a continuación.

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN
1	Socialización y Divulgación	Socializar y divulgar de la matriz de riesgos de seguridad Digital aprobada y publicada para la vigencia 2022.	Dirección de Tecnologías y Sistemas de la Información	01/01/2023	28/02/2023

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN
2	Actualizar el formato de la matriz de riesgos de Seguridad Digital.	Realizar la actualización del formato F-DS-898 "Matriz de Riesgos de Seguridad Digital" publicado en el portal MIPG de acuerdo a los parámetros establecidos en la Política de Administración de Riesgos.	Dirección de Tecnologías y Sistemas de la Información	01/03/2023	30/06/2023
3	Seguimiento fase de tratamiento	Seguimiento estado de controles de tratamiento de riesgos de seguridad digital y verificación de evidencias.	Dirección de Tecnologías y Sistemas de la Información	01/07/2023	30/11/2023
4	Monitoreo y revisión	Generación, presentación y reporte de indicadores	Dirección de Tecnologías y Sistemas de la Información	01/02/2022	30/11/2023
6	Mejoramiento	Identificar oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Dirección de Tecnologías y Sistemas de la Información	01/09/2023	30/11/2023
7	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2024.	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Dirección de Tecnologías y Sistemas de la Información	01/09/2023	30/11/2023

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción
23/07/2018	1	Creacion del Documento
13/03/2020	2	Se ajustan logos de la Alcaldia 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 Tecnologias y Sistemas de la Información, seajusta nuevamente y actuliza el documento.

Fecha	Versión	Descripción
08/07/2021	5	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2021, aprobado en la sesión del 08 de julio del 2021 de la Mesa Técnica de Seguridad Digital.
26/01/2022	6	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022.
26/01/2023	7	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023.

La información de elaboración, revisión y aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” https://portalmipg.scj.gov.co/