AQUÍ SÍ PASA BOGOTÁ MI CIUDAD MI CASA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2026

BOGOTÁ

CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
Acta de aprobación No 02 de 2026 del Comité Institucional de Gestión y Desempeño	29/01/2026	1.0	Adopción

CONTENIDO

1. INTRODUCCIÓN

La seguridad y privacidad de la información en las entidades tiene como objetivo la protección de cualquier tipo de activo de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad y privacidad de la información, que permitan gestionar y reducir los riesgos e impactos a los cuales está expuesta la entidad y se logre alcanzar el máximo retorno de inversión con relación al cumplimiento de la misión y visión institucionales. Por tanto, en el presente documento cuando se hable de riesgos de seguridad digital será lo mismo que decir riesgos de seguridad de la privacidad de la información digital.

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, a través de la implementación de la guía de gestión de riesgos, gestiona los riesgos de seguridad digital con el fin de reducir su probabilidad de ocurrencia y mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la protección de los activos de información y la custodia de los datos personales de los ciudadanos.

Las actividades de valoración de riesgos, en cumplimiento del Modelo Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información MINTIC, la política de seguridad digital y la Guía para la Gestión Integral del Riesgo en Entidades Públicas 2025, serán una herramienta para el logro de los objetivos encaminados a mantener los activos de información protegido de amenazas internas, externas y/o deliberadas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Gestionar los riesgos de seguridad de la información, privacidad de la información, seguridad digital, ciberseguridad y continuidad tecnológica del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, mediante la identificación, análisis, evaluación y tratamiento de los riesgos, con el fin de mantener y proteger la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la continuidad de los servicios tecnológicos institucionales.

2.1.1 Objetivos Específicos

El Plan de tratamiento de riesgos de seguridad y privacidad de la información da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

- Acompañar a los procesos en la identificación y valoración de los riesgos relacionados con los activos de información.
- Realizar seguimiento y monitoreo a los controles definidos por los procesos para gestionar los riesgos de Seguridad Digital.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la información aplica a todos los procesos y sedes de la entidad, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión y cumplimiento de sus objetivos estratégicos del IDPYBA.

4. MARCO NORMATIVO

El diseño e implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI del Instituto Distrital de Protección y Bienestar Animal - IDPYBA se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC y demás entidades que regulan en la materia:

- **Ley 1266 de 2008.** "Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."
- **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"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **Ley 1581 de 2012.** "Por la cual se dictan disposiciones generales para la protección de datos personales."
- **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 886 de 2014**. "Por el cual se reglamenta el Registro Nacional de Bases de Datos."
- **Decreto 103 de 2015.** "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones."
- **Decreto 1083 de 2015** del Departamento Administrativo de la Función Pública, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.
- **Decreto 1499 de 2017.** "Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión."
- **Decreto 728 de 2017.** "Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para

fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico."

- **Decreto 1008 del 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 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- **CONPES 3975 DE 2019.** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **Resolución 1519 del 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 en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos."
- **CONPES 3995 de 2020** - Política Nacional de Confianza y Seguridad Digital.
- **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 No. 500 de 2021".
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
- **Decreto 767 de 2022.** "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 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **NTC-ISO/IEC 27001:2022.** Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de seguridad de la información. Requisitos.
- **Decreto 472 de 2024 – Gobernanza de Ciberseguridad Distrital:** Por el cual se adopta el Modelo de Gobernanza de Seguridad Digital para el Distrito, se modifica el artículo 5 del Decreto Distrital 025 de 2021 y se dictan otras disposiciones.
- **Directiva 002 de 2025 – Alcaldía Mayor de Bogotá, D.C.:** Reconoce la seguridad de la información como un componente para proteger datos, TIC y garantizar la privacidad, según lineamientos distritales de seguridad digital. Objetivo: Integrar la seguridad digital en procesos distritales.
- **Resolución 2277 de 2025.** Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 7** del Departamento Administrativo de la Función Pública, de Agosto de 2025.

- **Decreto Distrital 640 de 2025:** Establecer la obligación de realizar Evaluaciones de Impacto en la Privacidad (PIA) en las entidades del Distrito Capital, con el fin de identificar, evaluar y mitigar riesgos asociados al tratamiento de datos personales en soluciones tecnológicas.

5. DESARROLLO DEL PLAN

La metodología para la identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes del IDPYBA se basa en la NTC-ISO 31000, la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP, en su versión 7, además de lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones, que permiten la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles fortaleciendo el desempeño de los procesos y la transparencia en la gestión Institucional y aplica para todos los procesos del IDPYBA.

Continuando con el proceso de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información, en el Plan de tratamiento de riesgos de seguridad y privacidad de la información, apoyándose en los requisitos legales y normativos, se desarrollarán las siguientes actividades para la vigencia 2026:

6. SEGUIMIENTO Y EVALUACIÓN

El seguimiento de plan se realizará de manera trimestral y se tiene como meta por lo menos la ejecución del 90% de las actividades.

7. CRONOGRAMA

COMPONENTE O ETAPA O EJE	ACTIVIDAD	RESPONSABLE	P/E	PRIMER TRIMESTRE DE ENERO A MARZO			SEGUNDO TRIMESTRE DE ABRIL A JUNIO			TERCER TRIMESTRE DE JULIO A SEPTIEMBRE			CUARTO TRIMESTRE DE OCTUBRE A DICIEMBRE		
				1	2	3	4	5	6	7	8	9	10	11	12
Documentación	Socialización de los lineamientos relacionados con la identificación y clasificación de riesgos de seguridad y privacidad de la Información.	Gestión Tecnológica	P		50%	50%									
			E												
Identificación y Valoración	Identificación, documentación, análisis y valoración de Riesgos de seguridad y privacidad de la información en la herramienta institucional.	Lideres de las áreas con el apoyo del proceso de Gestión Tecnológica	P				30%	30%	40%						
			E												
	Definición de los planes de Tratamiento de Riesgos Seguridad y privacidad de la Información	Cada líder de proceso con el apoyo del proceso de Gestión Tecnológica	P				30%	30%	40%						
			E												
Seguimiento	Hacer seguimiento a los planes de tratamiento y controles de los riesgos de seguridad	Gestión Tecnológica	P								50%				50%
			E												
Mejora Continua	Definición del Plan de Tratamiento de Riesgos de Seguridad para la vigencia 2027	Gestión Tecnológica	P												100%
			E												

REFERENCIAS Y BIBLIOGRAFÍA

Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 – 2025 – Departamento Administrativo de la Función Pública

Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI – 2025. Ministerio de tecnologías de la información y las comunicaciones.