icontec ISO 9001 SC-CER103099
icontec ISO 14001 SA-CER756031
IQNET CERTIFIED MANAGEMENT SYSTEM

Plan Estratégico De Seguridad y Privacidad De La Información

Alcaldía Distrital de Barranquilla

2024-2027

TABLA DE CONTENIDO

Contenido

Introducción

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, y se actualizó con el decreto 767 de 2022, la cual busca fortalecer la relación Estado-Ciudadano, mejorando la prestación de servicios por parte de las entidades, y generando confianza a través del uso y aprovechamiento de las TIC. Al mismo tiempo que fortalece la gestión de la entidad ya que hace parte del Modelo Integrado de Planeación y Gestión - MIPG.

Esta política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos de Gobernanza, Innovación Pública Digital, Habilitadores, Líneas de Acción e Iniciativas Dinamizadoras, los cuales se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos para alcanzar los logros de la política.

Los habilitadores que soporta el Modelo de Seguridad y Privacidad de la información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, y cuya adopción por parte de las entidades del Estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyado en un proceso de gestión del riesgo que cree condiciones de uso confiable en el entorno digital, brindando confianza a las partes interesadas.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del Estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado es obligatoria, como establece el decreto 612 de 2018 en el artículo 1, que debe integrarse y planificarse a los planes institucionales en el ámbito del modelo integrado de planeación y gestión.

Así mismo, la resolución 0500 de marzo 10 del 2021 precisa que los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y

Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información.

En atención a lo anterior, se presenta el Plan de Seguridad y Privacidad de la Información enfocado en la seguridad informática frente a ciberamenazas de activos de tecnologías de información de la entidad.

1. Objetivo del Plan de Seguridad

Minimizar el impacto de los riesgos de seguridad digital a los que está expuesta la entidad para mantener la integridad, confidencialidad y disponibilidad de los activos de información de la alcaldía, a través de la implementación de un marco de seguridad, definido en este documento para las vigencias 2024 – 2027.

1.1 Objetivos Específicos

- Definir las actividades del marco de seguridad de la información.
- Identificar y proteger los activos de información de la Alcaldía, con base a los criterios de confidencialidad, integridad y disponibilidad.
- Identificar los riesgos de seguridad de la información.
- Sensibilizar a funcionarios, contratistas y terceros acerca del modelo de seguridad y privacidad de la información, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramienta de diagnóstico.
- Implementar acciones correctivas y de mejora para el marco de seguridad y privacidad de la información.
- Implementar los instrumentos requeridos en lineamientos y directrices gubernamentales, la estrategia de Gobierno Digital y la normatividad relacionada en seguridad de la información y protección de datos personales para mantener el nivel de cumplimiento.
- Definir plan de trabajo a seguir durante las vigencias 2024-2027 en seguridad digital.

2. Alcance

El alcance del Plan de Seguridad y Privacidad de la Información aplica a todos los procesos, funcionarios, contratistas y terceros de la Alcaldía Distrital de Barranquilla, que realicen tratamiento de la información, física y electrónica de la entidad distrital.

3. Marco normativo

Interno:

Política de Seguridad de la Información.
Política de Privacidad y Tratamiento de Datos Personales.

Externo:

- 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*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- 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*".
- Decreto 338 de 2022 "Fortalecer la gobernanza de la seguridad digital y aplicar el modelo de seguridad y privacidad"
- Resolución 746 de 2022, "Fortalecer las relaciones de las entidades públicas con los proveedores. Proporciona lineamientos para que las entidades puedan proteger sus datos adquiridos en nube"
- Ley 1581 de 2012 y decretos reglamentarios "Se dictan disposiciones generales para la protección de datos personales"
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

4. Política de seguridad y privacidad de la información

"La política de Seguridad y Privacidad de la Información de la Alcaldía Distrital de Barranquilla, protege, preserva y administra la confidencialidad, integridad y disponibilidad de la información física y electrónica manejada por los servidores públicos, contratistas, terceros, ciudadanos en general y demás agentes del Estado que tienen acceso a la información de la Alcaldía Distrital de Barranquilla. Esto se

logrará mediante una gestión integral de riesgos y la implementación de controles para prevenir incidentes, continuar con la operación de servicios y cumplir con los requisitos legales. Estos lineamientos se extienden a los recursos físicos y tecnológicos de información (computadores y teléfonos, entre otros) que se conecten o interactúen con la red de comunicaciones del Distrito de Barranquilla y cuyas actividades sean responsabilidad de servidores públicos y demás actores que manejen datos de la Alcaldía Distrital de Barranquilla. "

5. Roles y responsabilidades

La seguridad y privacidad de la información deben ser una cultura, en la que se deben involucrar a los colaboradores, servidores públicos, usuarios y contratistas, pues son los responsables de la información que se genera o ingresa en la Alcaldía Distrital de Barranquilla.

A continuación, se listan los roles y responsabilidades de los definidos para el marco de seguridad y privacidad de la información de la entidad:

TABLA 1. ROLES Y RESPONSABILIDADES

ROL	ACTIVIDADES	RESPONSABILIDADES
Alta Dirección	Velar por el cumplimiento de las políticas de seguridad y privacidad de la información.	• Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la Entidad.
Gerencia de las TIC Gestión Documental	Planear, ejecutar, verificar y realizar seguimiento a la implementación de la Seguridad y privacidad de la Información.	• Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias de la seguridad y privacidad de la información, de manera que cumpla o exceda las necesidades y expectativas de las partes interesadas. • Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. • Gestionar el comité técnico de seguridad de la información, definiendo roles, responsabilidades, entregables y tiempos. • Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos.

ROL	ACTIVIDADES	RESPONSABILIDADES
Comité técnico de seguridad y privacidad de la información.	Cumplir y orientar la planeación, implementación y mejoramiento de la seguridad y privacidad de la información.	• Facilitar la administración y desarrollo de iniciativas sobre seguridad de información en la entidad. • Proveer dirección y experiencia técnica para asegurar la protección adecuada de la información. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan. • Prevenir pérdidas patrimoniales o que comprometan los recursos de información de la Entidad. • Revisar el estado de la seguridad de la información. • Revisar y analizar los incidentes de seguridad suscitados en la entidad que así lo ameriten, es decir incidentes de seguridad con impacto alto, considerados como severos. • Servir de facilitadores para el desarrollo de proyectos de seguridad de información.
Oficial de seguridad y privacidad información.	Garantizar el efectivo ejercicio de la seguridad y privacidad de la información, mediante el establecimiento y cumplimiento de políticas, procedimientos, normas y reglas que aseguren el debido tratamiento de la información.	• Establecer controles de seguridad de la información para prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y servicios de la Gerencia TIC. • Velar por la implementación efectiva de las políticas y procedimientos adoptados por la organización en materia de protección de datos personales. • Estructurar, diseñar y administrar el programa que permita a la organización cumplir con las normas sobre protección de datos. • Establecer los controles de ese programa, su evaluación y revisión permanente • Responsabilidades definidas en actos administrativos internos.
Jefe de Control Interno	Realizar las auditorias integrales a los planes y políticas definidas para la seguridad y privacidad de la información.	• Revisar el cumplimiento de los requisitos de la norma para la seguridad y privacidad de la información de la Alcaldía. • Velar porque se eviten la generación de riesgos de seguridad de la información

ROL	ACTIVIDADES	RESPONSABILIDADES
Funcionarios Contratistas y terceros.	Aplicar las disposiciones establecidas por el Distrito para el cumplimiento de las políticas de seguridad y privacidad de la información	• Garantizar la confidencialidad respecto de la información que reciben, generan y procesan en la Alcaldía. • Comunicar a la Gerencia de las TIC cualquier incidencia respecto a la seguridad de la información.

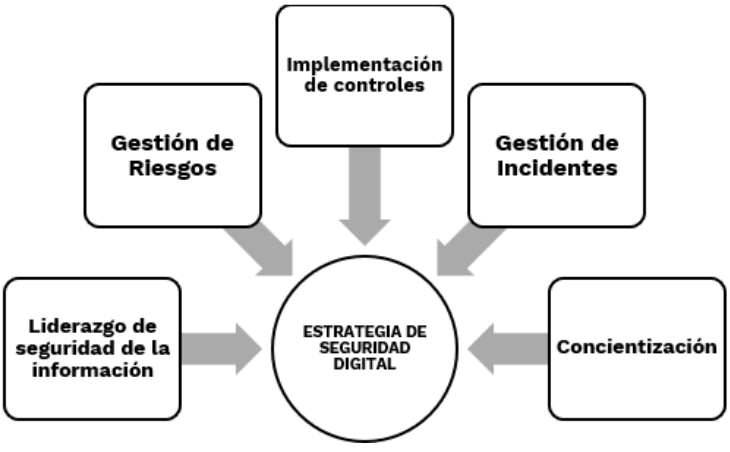
6. Indicador

- Nombre del indicador: Estado de madurez de la seguridad y privacidad de la información de la entidad.
- Medición: Aplicación del instrumento de madurez de MINTIC.

7. Estrategia de seguridad digital

Definir los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, tomando como referencia el Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información, y los procedimiento de: copias de respaldo, gestión de incidentes y plan de continuidad de negocio, y demás procedimientos pertinentes para garantizar la confidencialidad, integridad y disponibilidad de la información digital de la Alcaldía de Barranquilla.

Por lo anterior se definen las 5 estrategias especificas:



7.1 Descripción de las estrategias especificas

A continuación, se define el objetivo de cada estrategia especifica:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Adoptar los lineamientos impartidos por MINTIC con el fin de implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), partiendo de revisión y aprobación de la política de Seguridad de la Información, el compromiso de la alta dirección y el Gerente de las TIC con el fin de mantener la confidencialidad, integridad y disponibilidad de la información en la Alcaldía de Barranquilla.
Gestión de riesgos	Determinar los riesgos de seguridad de la información en todos los procesos de la entidad, buscando prevenir o reducir posibles incidentes de seguridad, teniendo como base la política de administración de riesgos de la alcaldía y la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la cultura de seguridad, haciendo de esta un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para el cumplimiento de la política de Seguridad de la Información, definiendo controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

8. Términos y Definiciones.

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).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

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).

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. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

MSPI: Modelo de Seguridad y Privacidad de la Información, definido por el MinTIC para las entidades del Estado colombiano. Proporciona lineamientos para la implementación de un sistema de gestión de seguridad de la información

Política de seguridad: Documento de alto nivel que establece el compromiso de la alta dirección a través de la Oficina de TI, junto con quienes

se considere, con la seguridad de la información, define los objetivos de seguridad y proporciona un marco para la implementación de controles.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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).

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos o información, tales como la recolección, almacenamiento, uso, circulación o supresión.

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

9. Cronograma de implementación del Plan de Seguridad digital.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende los siguientes cronogramas:

7.1. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	AÑO	Trimestres			
					1	2	3	4
1	**Eje: Liderazgo de seguridad de la información**							
1,1	Designar o ratificar el responsable de la seguridad de la información digital en la alcaldía de Barranquilla	Gerencia TIC	Líder de Proceso	2025				
1,2	Revisar y actualizar política de Seguridad de la Información (anual)	Gerencia TIC	Líder de Proceso	2024-2027				
1,3	Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad (anual)	Gerencia TIC	Líder de Proceso	2024-2027				
1,4	Definir y asignar los roles y responsabilidades en seguridad de la información, formalizados dentro de las políticas de seguridad	Gerencia TIC	Líder de Proceso	2024-2027				
1,5	Convocar al comité técnico de seguridad	Gerencia TIC	Líder de Proceso	2024-2027				
1,6	Convocar equipo de repuesta a incidentes	Gerencia TIC	Líder de Proceso	2025-2027				

7.1. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	AÑO	Trimestres			
					1	2	3	4
1,7	Revisar y actualizar las funciones del equipo de respuesta a incidentes	Gerencia TIC	Líder de Proceso	2024-2027				
1,8	Definir los procedimientos pertinentes para la seguridad y privacidad de la información	Gerencia TIC	Líder de Proceso	2024-2027				
1,9	Crear y actualizar el catálogo inicial de servicios de seguridad	Gerencia TIC	Líder de Proceso	2024-2027				
1,10	Actualizar Matriz de verificación de Requisitos Legales y normativo de Seguridad de la Información y privacidad	Gerencia TIC	Asesor Jurídico	2024-2027				
1,11	Identificar nivel de madurez de la gestión de seguridad y privacidad de la información	Gerencia TIC	Agente de Cambio	2024-2027				
2	**Eje concientización**							
2,1	Revisar y actualizar el Plan de cultura y sensibilización en seguridad de la información para funcionarios, contratistas y terceros. (anual)	Gerencia TIC	Líder de Proceso	2024-2027				
2,2	Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.	Gerencia TIC	Líder de Proceso	2024-2027				
2,4	Evaluar el nivel de satisfacción del plan de cultura y sensibilización en seguridad de la información	Gerencia TIC	Líder de Proceso	2024-2027				

7.1. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	AÑO	Trimestres			
					1	2	3	4
2,5	Realizar seguimiento y ajustes al plan de cultura y sensibilización	Gerencia TIC	Líder de Proceso	2024-2027				
3	**Gestión del riesgo**							
3,1	Identificar Riesgos de Seguridad y Privacidad de la Información de todos los procesos	Todas las áreas	Agente de Cambio y líder del proceso	2024-2027				
3,2	Realizar el análisis de riesgos de seguridad y privacidad de la información	Todas las áreas	Agente de Cambio y líder del proceso	2024-2027				
3,3	Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.	Todas las áreas	Agente de Cambio y líder del proceso	2024-2027				
3,4	Elaborar plan de tratamiento de riesgos	Gerencia TIC	Agente de Cambio y Líder de Proceso	2024-2027				
3,5	Socializar Plan de tratamiento de riesgos	Gerencia TIC	Agente de Cambio y Líder de Proceso	2024-2027				
3,6	Establecer el seguimiento a la implementación del plan de tratamiento de riesgos	Gerencia TIC	Agente de Cambio	2024-2027				
4	**Eje Gestión de incidentes**							
4,1	Designar o ratificar los responsables de gestionar y dar respuesta a los incidentes de seguridad, liderados por el responsable de la seguridad.	Gerencia TIC	Líder de Proceso	2024-2027				

7.1. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	AÑO	Trimestres			
					1	2	3	4
4,2	Revisar o ajustar el procedimiento de gestión de incidentes que contenga actividades para las fases de: prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje. (Resolución 500 de 2021)	Comité técnico de seguridad	Líder de Proceso	2025-2027				
4,2	Crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de incidentes	Gerencia TIC	Líder de Proceso	2024-2027				
4,4	Definir plan de mejoramiento según el análisis e investigación de los incidentes materializados.	Gerencia TIC	Agente de Cambio	2024-2027				
5	**Eje: Implementación de controles**							
5,1	Definir los controles pertinentes a cada dominio de la política de seguridad.	Gerencia TIC	Agente de Cambio	2024-2027				
5,2	Actualizar declaración de aplicabilidad con los controles definidos	Gerencia TIC	Agente de Cambio	2024-2027				
5,3	Registrar los seguimientos a los controles en la plataforma definida en la entidad.	Gerencia TIC	Agente de Cambio	2024-2027				

Nota: las actividades relacionadas dentro de las vigencias 2024-2027, se realizan anualmente.

10. Cronograma de implementación de la Política de Protección y Tratamiento de Datos Personales.

PLAN DE ACCION PROTECCIÒN Y TRATAMIENTO DE DATOS PERSONALES DE LA ALCALDIA DISTRITAL DE BARRANQUILLA 2026-2027

CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	AÑO	Trimestres			
					1	2	3	4
1	**FASE I: PLANEACIÓN**							
1,1	Revisión y ajuste de actividades pendientes sobre la protección de datos para la vigencia.	Gerencia Tic, Grupo Administrativa	Oficial datos	2026-2027				
1,2	Definir actividades a ejecutar en la actual vigencia.	Gerencia Tic, Grupo Administrativa		2026-2027				
2	**FASE II: MARCO NORMATIVO**							
2,1	Revisar y actualizar el marco legal, requisitos técnicos normativos, documentos, lineamientos y herramientas asociadas a la protección y tratamiento de datos personales y Matriz de verificación de requisitos legales y normativo de Protección y tratamiento de datos personales.	Oficial de datos, Grupo Administrativa	Oficial datos	2026-2027				
2,2	Expedir y publicar lineamientos que fortalezcan y promuevan la implementación y apropiación de la Política de tratamiento de datos.	Gerencia TIC, Comunicaciones, Grupo Administrativa	Oficial de datos	2026-2027				
3	**FASE III: IMPLEMENTACION**							
3,1	Revisión de las bases de datos y sus categorías que se han reportado en la plataforma de Registro Nacional de Bases de Datos Personales (RNBD) de la Superintendencia de Industria y	Gerencia TIC, Procesos de la Alcaldía	Oficial de datos	2026-2027				

	Comercio y para los cuales se establece su recolección y finalidad del tratamiento de los datos personales en la Entidad.							
3,2	Actualización anual del Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio	Oficial de datos, Grupo Administrativa	Oficial datos	2026-2027				
3,3	Revisión de reclamaciones / sanciones ante la Superintendencia de Industria y Comercio segundo semestre 2025. Ley 1581 de 2012.	Gerencia TIC, Grupo Administrativa	Oficial de datos	2026				
3,4	Revisión de reclamaciones / sanciones ante la Superintendencia de Industria y Comercio primer semestre 2026. Ley 1581 de 2012.	Gerencia TIC, Grupo Administrativa	Oficial de datos	2026				
3,5	Revisar nivel anonimización actual de la entidad con reinducciones al personal de la entidad sobre el tema	Gerencia TIC; Grupo Administrativa y Software	Oficial de datos	2026-2027				
3,6	Identificar controles implementados de seguridad en la captura de la información de datos personales.	Gerencia TIC; Grupo Administrativa y Software	Oficial de datos	2026-2027				
3,7	Definir las capacitaciones, socialización o sensibilización de la política de tratamiento de datos personales en la alcaldía de Barranquilla y a los ciudadanos.	Gerencia TIC; Grupo Administrativa y Software	Oficial de datos	2026-2027				
4	**FASE IV: CAPACITACIÓN Y SENSIBILIZACIÓN**							

4,1	Promover la apropiación e implementación de estrategias de gestión para la Protección de Datos mediante programas de formación y sensibilización que fortalezcan la capacidad del personal de la entidad para identificar y responder a amenazas.	Gerencia TIC, Grupo Administrativa	Oficial de datos	2026-2027				
5	**FASE V: GESTIÓN DE INCIDENTES**							
5,1	Realizar reporte de los incidentes de seguridad presentados con las bases de datos ante la Superintendencia de Industria y Comercio en su plataforma de Registro Nacional de Base de Datos.	Oficial de datos, Grupo Administrativa	Oficial datos	2026-2027				
5,2	Elaborar plan de mejora para evitar incidentes en seguridad de datos personales.	Oficial de datos, Grupo Administrativa	Oficial de datos	2026-2027				
6	**FASE VI: SEGUIMIENTO**							
6,1	Realizar seguimiento a las actividades planificadas para la implementación de la política.	Gerencia TIC; Grupo Administrativa	Oficial de datos	2026-2027				

Nota: Al final de cada vigencia, la entidad, realizará una actualización de los cronogramas del ítem 9 y 10. Así mismo estos podrán ser modificados o ajustados de acuerdo con las necesidades o situaciones que surjan en la Alcaldía Distrital de Barranquilla.

11. Plan de tratamiento de riesgos de seguridad y privacidad de la información.

El plan de tratamiento de riesgos contempla las actividades a desarrollar en la vigencia 2026-2027, en aras de mitigar los riesgos sobre los activos identificados por los procesos de la Alcaldía, siguiendo las recomendaciones de la guía de gestión de riesgos de seguridad y privacidad de la información.

Gestión	Actividades	Tareas	Responsables	Sem_1	Sem_2
Gestión de riesgos de seguridad de la información	Alineación de la gestión de riesgos de seguridad digital con la política de gestión de riesgos.	Atender las recomendaciones de la política de riesgos institucional y presentar aspectos propios de la gestión de riesgos de seguridad digital para su evaluación y alineación con la política institucional.	Gerencia de las TIC- Agentes de cambio	✓	
	Sensibilización	Continuar las socializaciones a todos los procesos para la gestión de riesgos de seguridad digital.	Gerencia de las TIC- Agentes de cambio	✓	
	Identificación de los riesgos de seguridad digital.	Identificación, análisis y evaluación de riesgos de seguridad digital.	Enlaces TIC- Agentes de cambio Gerencia TIC	✓	✓
	Tratamiento del riesgo	Definición de controles y planes de tratamiento de riesgos los identificados	Enlaces TIC- Agentes de cambio Gerencia TIC Grupo interno de trabajo para el uso y tratamiento de datos personales.		✓
	Mejoramiento	Revisión y/o actualización de lineamientos de riesgos de seguridad digital de acuerdo con las observaciones presentadas.	Agentes de cambio Gerencia TIC Grupo interno de trabajo para el uso y tratamiento de datos personales.		✓

	Monitoreo y revisión	Realizar mediciones periódicas a los controles definidos por cada proceso	Enlaces TIC- Agentes de cambio Gerencia TIC. Grupo interno de trabajo para el uso y tratamiento de datos personales.		✓

12. Seguimiento

Para mantener una buena gestión en el desarrollo de las actividades de la Entidad, una vez realizado el plan y ejecutado las actividades planificadas, se realizarán las mediciones semestralmente. El Sistema de Gestión es un proceso que se realiza permanentemente, deberá estar en continua revisión por parte de las áreas encargadas, es decir, crear un ciclo que permita establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad y privacidad de la información de la Alcaldía Distrital de Barranquilla.

De esa forma, se protegerá los activos de la entidad y se brindará mayor confianza y credibilidad en las personas que busquen o se beneficien de los servicios que presta la Alcaldía Distrital de Barranquilla.

13. Control de Cambios

Fecha	Versión	Descripción del Cambio.
07-01-2021	Versión 1	Elaboración del Plan
28-01-2022	Versión 2	Actualización de las actividades del plan.
25-01-2023	Versión 3	Actualización del plan
31-01-2024	Versión 4	Se cambia el nombre de plan de seguridad de la información por Plan estratégico de Seguridad de la información en atención a la resolución 500 de 2021 y los lineamientos de MSPI
31-01-2025	Versión 5	Revisión y actualización de las actividades definidas en el cronograma de ejecución de las políticas de seguridad y privacidad de la información.
31-01-2026	Versión 6	Actualización actividades de protección y tratamiento de datos personales.