# Plan de Seguridad y Privacidad de la Información y Tratamiento de riesgos de seguridad y privacidad de la información

## Versión 1

## TABLA DE CONTENIDO

# Plan de seguridad y privacidad de la información

## 1. Objetivo del Plan de Seguridad

Definir las actividades de Seguridad y Privacidad de la Información, con las cuales se busca establecer un marco de seguridad, aplicar controles y realizar seguimiento a la seguridad, privacidad y protección de los activos de la información física y electrónica de la Alcaldía Distrital de Barranquilla, alineados al Modelo de Seguridad y Privacidad de la Información del MINTIC y la NTC/IEC ISO 27001:2013.

## 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 (compartir, utilizar, recolectar, procesar, intercambiar, consultar, modificar, custodiar, almacenar y circular), física y electrónica de la entidad distrital.

## 3. Política de seguridad y privacidad de la información

La Alcaldía Distrital de Barranquilla, es una Entidad que se caracteriza por brindar a la ciudadanía bienes y servicios, y en el desarrollo de su gestión como administrador de la información, requiere asegurar la confiabilidad, garantizar su buen uso y mantener la privacidad de los datos que se allegan; la Entidad está comprometida en proteger los activos de información, está orientada en el cumplimiento de los principios de la transparencia, normas que avalen su funcionamiento y acceso a la información pública.

De modo que sus esfuerzos están enfocados a la preservación de la confidencialidad, integridad, disponibilidad y a la continuidad de las operaciones gestionando los riesgos de seguridad de la información y fomentando la creación de una cultura y conciencia de seguridad en los funcionarios, contratistas y terceros.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar el funcionamiento y servicios que brinda la Alcaldía Distrital de Barranquilla, por lo que es responsabilidad de todas las partes interesadas, garantizar la seguridad de la información, velar por que no se realicen actividades que contradigan el buen nombre de la Entidad, que puedan generar consecuencias, tales como el robo, daño o filtraciones de la información, divulgación de información sensible o reservada, perdida o daño de la documentación y desconfianza en los ciudadanos entre otros.

***"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. "***

La política de seguridad de la información aplica a todas las formas de información, incluyendo:

- Comunicaciones enviadas y recibidas por correo electrónico.
- La almacenada y procesada a través de servidores, computadores, portátiles, tablets, celulares.
- La almacenada en cualquier tipo de medios extraíbles: CD, DVD, cinta, memoria USB, tarjeta de memoria, discos externos.
- La almacenada en medios externos que se acceden a través de Internet, como son los servicios de almacenamiento en la nube: Dropbox, Google Drive, OneDrive, entre otros.
- La recopilada en medios físicos como libros de minutas y planillas entre otros.
- La recopilada y almacenada en cámaras de seguridad y DVR.
- Todo tipo de documentos físicos que genere o reciba la Alcaldía Distrital de Barranquilla.

### 3.1 Objetivos de la política

- Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
- Definir marco de seguridad y privacidad de la información necesarios para la implementación de la política.
- Facilitar la gestión de los riesgos de seguridad y privacidad de la información.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Alcaldía Distrital de Barranquilla.
- Incrementar la transparencia en los trámites y servicios de la gestión pública de la Entidad brindando seguridad y privacidad de la Información.
- Promover el uso de las buenas prácticas de seguridad y privacidad de la Información en la Alcaldía Distrital de Barranquilla por parte de los funcionarios, contratistas o terceros.
- Implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física.
- Garantizar la continuidad del negocio frente a incidentes.
- Garantizar el manejo y organización del sistema de administración de documentos, archivos físicos y electrónicos a partir de la noción de Archivo total bajo los principios de eficiencia, economía, control, transparencia, oportunidad, disponibilidad, agrupación, protección del medio ambiente, responsabilidad, confidencialidad, seguridad y accesibilidad.
- Generar un cambio organizacional a través de la conciencia y apropiación de la Seguridad y Privacidad de la Información.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información.

### 3.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la política, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del

Sistema de Gestión de la Seguridad de la Información - SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de parte interesadas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.[1]
- Ejecutar las actividades de planeación técnica de los documentos durante su ciclo de vida, su creación, valoración, y el control de versiones, mediante esquemas e instrumentos archivísticos.
- Asegurar la conservación y preservación a largo plazo de los documentos, mediante programas y planes en el marco del sistema integrado de conservación.
- Identificar documentos vitales, con fines de conservación, con fines de acceso (índice de información clasificada y reservada), documentos vitales (identificación).
- Cumplir con la responsabilidad de asegurar y preservar la información clasificada y reservada de acuerdo a los niveles de protección y privacidad de los documentos.[2]

## 4. Roles y responsabilidades

La seguridad y privacidad de la información debe ser una cultura, en la cual se deben involucrar todos los colaboradores, tanto servidores públicos, usuarios y contratistas pues son los directamente responsables de la información que se genera o ingresa en la Alcaldía Distrital de Barranquilla, y son los primeros en contribuir a crear un clima de seguridad tanto al interior como al exterior de la entidad.
A continuación, se listan los roles y responsabilidades de los definidos para el marco de seguridad y privacidad de la información de la entidad:

[1]. Manual Elaboración de la política general de seguridad y privacidad de la información Guía No 2, MINTIC.
[2] Modelo de Gestión Documental y Administración de Archivos MGDA, Archivo General de la Nación Colombia.

*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`S. 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.<br>• Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.<br>• Gestionar el comité técnico de seguridad de la información, definiendo roles, responsabilidades, entregables y tiempos.<br>• Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos. |
| 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.<br>• Proveer dirección y experiencia técnica para asegurar que la información se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan.<br>• Prevenir pérdidas patrimoniales o que comprometan los recursos de |

| ROL | ACTIVIDADES | RESPONSABILIDADES |
|---|---|---|
| | | información de la Entidad.<br>• Revisar el estado de la seguridad de la información.<br>• 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.<br>• 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 con el fin de prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y servicios que presta la Gerencia TIC´S<br>• Velar por la implementación efectiva de las políticas y procedimientos adoptados por la organización en materia de protección de datos personales. |
| 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.<br>• Velar porque se eviten la generación de riesgos de Seguridad de la Información |
| 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.<br>• Comunicar a la Gerencia TIC`S cualquier incidencia respecto a la seguridad de la información. |

## 5. Términos y Definiciones.

### 5.1 Activos de la Información.

La identificación del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

La realización del inventario y clasificación de activos de información física y electrónica es parte fundamental en la administración de la seguridad y privacidad de la información efectiva, ayuda al cumplimiento del control del Anexo A del estándar ISO/IEC 27001:2013 (inventario de activos, propiedad de activos, clasificación de la información, etiquetado y manipulado de la información).

Los activos de información constituyen un gran valor en todos los procesos de la entidad, pues son parte esencial del mismo, y se proporcionan a los funcionarios, servidores públicos, contratistas y proveedores, para cumplir con el propósito de la función pública.

*Tabla 2. Clasificación por confidencialidad, Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC*

| | |
|---|---|
| **INFORMACIÓN PÚBLICA RESERVADA** | Información disponible sólo para un proceso de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. |
| **INFORMACIÓN PUBLICA CLASIFICADA** | Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. |
| **INFORMACIÓN PÚBLICA** | Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. |
| **NO CLASIFICADA** | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada. |

### 5.2 Información documentada

La Alcaldía Distrital de Barranquilla, en ejercicio de sus funciones de bienestar y servicio, en cada proceso de la entidad, ejecuta diferentes acciones que le permiten producir o recibir documentos oficiales, físicos y electrónicos; a través de la página web, correo electrónico, en el sistema SIGOB u otros sistemas de información, los cuales deben cumplir con ciertas características que permitirán asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información.

### 5.3 Incidentes de Seguridad de la Información.

De acuerdo con la norma ISO 27001:2013 un incidente de seguridad de la información está definido como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información”.

Teniendo en cuenta que esta entidad tiene como función principal administrar y brindar bienes y servicios, generando bienestar a los ciudadanos, y para el cumplimiento de ese rol puede verse afectado por amenazas como:

- Pérdida o robo de la información.
- uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Perdida o daño de la documentación.
- Modificación no autorizada.
- Diligenciamiento errado de formatos.

## 6. Gestión de Riesgos.

Para evaluar los riesgos en seguridad de la información La Alcaldía Distrital de Barranquilla, ha clasificado sus activos de información, de tal modo que la Entidad debe preservar la Confidencialidad, Integridad y Disponibilidad de la información.

*Tabla 3. Criterios de clasificación*

| 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 4. Niveles de clasificación*

| | |
|---|---|
| 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. |

## 7. Cronograma de implementación del Plan de Seguridad y Privacidad de la Información física y digital.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

| Código | Actividad | Áreas que Intervienen | Responsable | Entregables | Herramientas | Duración (Días) | Mes | Semana | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 1 | 2 | 3 | 4 | 5 |
| **1** | **FASE I: DEFINIR MARCO DE SEGURIDAD Y PRIVACIDAD** | | | | | | | | | | | |
| 1.1 | Crear el comité técnico de Seguridad y Privacidad de la información | Todas | Líder de Proceso | Acta de reunión | Convocatoria | 1 | Diciembre | 1 | | | | |
| 1.2 | Definir los roles y responsabilidades en el comité de seguridad y privacidad de la información digital | Comité técnico de seguridad | Profesional Gobierno Digital | Acta | Herramienta MSPI, Revisión de documentación | 1 | Enero | | | | 1 | |
| 1.3 | Definir y documentar las funciones del comité de Seguridad y Privacidad de la información | Comité técnico de seguridad | Profesional Gobierno Digital | Manual de Funciones | Herramienta MSPI, Revisión de documentación | 1 | Enero | | | | 1 | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.4 | Crear el equipo de repuesta a incidentes | Comité técnico de seguridad | Agente de Cambio | Acta de reunión | Convocatoria | 1 | Febrero | 1 | | | | |
| 1.5 | Definir y documentar las funciones del equipo de respuesta a incidentes | Comité técnico de seguridad | Agente de Cambio | Manual de Funciones | Herramienta MSPI, Revisión de documentación | 1 | Febrero | 1 | | | | |
| 1.6 | Identificar el marco legal, requisitos técnicos normativos, documentos, lineamientos y herramientas asociadas a la seguridad y privacidad de la información. | Todas | Agente de Cambio | Documento de Hallazgos | Revisión de documentación, lista de chequeo, Recopilación de información, Análisis de supuestos | 1 | Febrero | | 1 | | | |
| 1.7 | Crear la Matriz de verificación de Requisitos Legales y normativo de Seguridad de la Información y privacidad | Todas | Agente de Cambio | Matriz de requisitos legales y normativos | Recopilación de información | 1 | Febrero | | 1 | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.8 | Identificar estado actual de la gestión de seguridad y privacidad de la información. | Comité técnico de seguridad | Profesional Gobierno Digital | Diligenciamiento de Herramienta | Herramienta MSPI | 1 | Febrero | | | 1 | | |
| 1.9 | Identificar nivel de madurez en la gestión de la seguridad y privacidad de la información | Comité técnico de seguridad | Profesional Gobierno Digital | Diligenciamiento de Herramienta | Herramienta MSPI | 1 | Febrero | | | 1 | | |
| 1.10 | Identificar vulnerabilidades técnicas y administrativas (Insight fases siguientes) | Comité técnico de seguridad | Profesional Gobierno Digital | Documento de Hallazgos | Herramienta MSPI | 1 | Febrero | | | 1 | | |
| 1.11 | Plan de diagnóstico de IPv4 a IPv6 | Infraestructura TI | Comité técnico de seguridad | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. | Guía No 20 - Transición IPv4 a IPv6 | 2 | Febrero | | | | 2 | |
| **2** | **FASE II : ACTIVOS DE INFORMACIÓN** | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.1 | Definir lineamientos para la actualización y levantamiento del inventario de activos de información | Todas | Oficina de gestión documental | Documento de lineamientos | Herramienta MSPI, Revisión de documentación | 2 | Marzo | 2 | | | | |
| 2.2 | Socializar Herramienta para el levantamiento de información | Todas | Profesional Gobierno Digital | Acta de reunión | Plan de Comunicaciones | 1 | Marzo | | 1 | | | |
| 2.3 | Revisión de la información suministrada para actualización del Inventario de Activos de Información | Todas | Oficina de Gestión documental | Herramienta de Inventario Activos de Información | Herramienta MSPI, Revisión de documentación, Recopilación de información, lista de chequeo | 5 | Marzo | | | 2 | 2 | 1 |
| 2.4 | Presentación para aprobación de actualización del inventario de Activos de Información al Comité MIPG | Gerencia TICs y Oficina de Gestión Documental | Gerencia TICs y Oficina de Gestión Documental | Acta de reunión | Lista de chequeo, Juicio de expertos, Plan de Comunicaciones | 1 | Abril | 1 | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.5 | Revisar y aprobar inventario de Activos de Información | Comité MIPG | Comité MIPG | Acta de reunión | Lista de chequeo, Juicio de expertos, Plan de Comunicaciones | 1 | Abril | 1 | | | | |
| 2.6 | Establecer el plan de revisión de la herramienta para el levantamiento de activos y la actualización del inventario de activos | Gerencia TICs y Oficina de Gestión Documental | Gerencia TICs y Oficina de Gestión Documental | Acta de reunión | Recopilación de información, revisión de documentación | 1 | Abril | 1 | | | | |
| 2.7 | Actualización e Identificación y clasificación de la Información pública, clasificada y reservada de la Alcaldía Distrital de Barranquilla | Oficina de Gestión Documental | Oficina de Gestión Documental | Índice de información clasificada y reservada | Microsoft Excel | 120 | Abril a junio | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.8 | Definir lineamientos de la protección de los documentos electrónicos, sistemas de información y dispositivos asociados a los procesos de gestión documental | Oficina de Gestión Documental | Oficina de Gestión Documental | PGD ajustado | Microsoft Word | 25 | Agosto | 5 | 5 | 5 | 5 | 5 |
| 2.9 | Seguimiento y capacitación en el manejo y aplicación Tablas de Retención Documental | Oficina de Gestión Documental | Oficina de Gestión Documental | Informe aplicación TRD | Microsoft Word | 90 | Julio-septiembre | | | | | |
| 2.10 | Establecer niveles de protección y privacidad de los archivos de gestión y archivo central de la Alcaldía Distrital de Barranquilla | Oficina de Gestión Documental | Oficina de Gestión Documental | Niveles de acceso definidos | Microsoft Word | 25 | abril | 5 | 5 | 5 | 5 | 5 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.11 | Verificación de seguridad en las Transferencias documentales de acuerdo a las Tablas de Retención Documental | Oficina de Gestión Documental | Oficina de Gestión Documental | Informe de verificación | Microsoft Word | 25 | abril | 5 | 5 | 5 | 5 | 5 |
| **3** | **FASE III: GESTIÓN DE RIESGOS** | | | | | | | | | | | |
| 3.1 | Revisar metodología de gestión de riesgo | Comité técnico de seguridad | Agente de Cambio | Documento de metodología | Herramienta MSPI, ISO 27005<br>ISO 31000 | 5 | Mayo | 5 | | | | |
| 3.2 | Identificar Riesgos de Seguridad y Privacidad de la Información de la entidad | Comité técnico de seguridad | Agente de Cambio | Registro de Riesgos | Herramienta MSPI, Revisión de documentación, Recopilación de información, lista de chequeo, análisis de supuestos | 5 | Mayo | | 5 | | | |
| 3.3 | Realizar el análisis de riesgos de seguridad y privacidad de la información | Comité técnico de seguridad | Agente de Cambio | Documento Plan de tratamiento de riesgos | Evaluación de probabilidad e impacto<br>Categorización de riesgos | 5 | Mayo | | | 5 | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3.4 | Elaborar plan de tratamiento de riesgos | Comité técnico de seguridad | Agente de Cambio | Documento Plan de tratamiento de riesgos | Estrategias de respuesta a riesgos | 5 | Mayo | | | | 5 | |
| 3.5 | Socializar Plan de tratamiento de riesgos | Comité técnico de seguridad | Profesional Gobierno Digital | Acta de reunión | Plan de Comunicaciones | 5 | Junio | | | 5 | | |
| 3.6 | Establecer el seguimiento a la implementación del plan de tratamiento de riesgos | Comité técnico de seguridad | Líder Gobierno Digital | Informe de seguimiento, solicitudes de cambio y actualizaciones | Reevaluación, Análisis de variación y tendencias, medición del desempeño técnico, reuniones de estado | 12 | Mensual | | | | 1 | |
| **4** | **FASE IV : PLANES, POLÍTICAS Y PROCEDIMIENTOS** | | | | | | | | | | | |
| 4.1 | Revisar y actualizar políticas de seguridad y privacidad digital | Comité técnico de seguridad | Líder de Proceso | Políticas Actualizadas | Revisión de documentación, Recopilación de información, lista de chequeo | 60 | Junio - julio | 5 | 5 | 5 | 5 | 5 |
| 4.2 | Crear y aprobar políticas de seguridad de la información y privacidad. | Líder de Proceso | Líder Gobierno Digital | Políticas de Seguridad y Privacidad | Revisión de documentación, Recopilación de información, lista de chequeo | 30 | Agosto | 5 | 5 | 5 | 5 | 5 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.3 | Socializar (sensibilizar) políticas de seguridad de la información y privacidad. | Profesional Gobierno Digital | Líder Gobierno Digital | Acta de reunión | Plan de comunicaciones | 5 | Septiembre | | | 5 | | |
| 4.4 | Establecer el plan de seguimiento a la implementación de políticas | Comité técnico de seguridad | Líder Gobierno Digital | Informe de seguimiento, solicitudes de cambio y actualizaciones | Reuniones de estado | 10 | Septiembre | | | 5 | 5 | |
| 4.5 | Revisar y actualizar procedimientos para gestionar la seguridad y privacidad | Comité técnico de seguridad | Líder Gobierno Digital | Procedimientos Actualizados | Revisión de documentación, Recopilación de información, lista de chequeo | 10 | Septiembre | 5 | 5 | | | |
| 4.6 | Crear y aprobar procedimientos para gestionar la seguridad y privacidad de la información | Comité técnico de seguridad | Líder Gobierno Digital | Procedimientos para gestionar la seguridad y privacidad | Revisión de documentación, Recopilación de información, lista de chequeo | 5 | Octubre | 5 | | | | |
| 4.7 | Socializar procedimientos de seguridad de la información y privacidad. | Profesional Gobierno Digital | Líder Gobierno Digital | Acta | Plan de Comunicaciones | 5 | Octubre | | 5 | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.8 | Establecer el plan de seguimiento a la implementación de procedimientos | Comité técnico de seguridad | Líder Gobierno Digital | Informe de seguimiento, solicitudes de cambio y actualizaciones | Reuniones de estado | 5 | Octubre | | | 5 | | |
| 4.9 | Crear y aprobar acuerdos para gestionar la seguridad y privacidad de la información | Comité técnico de seguridad | Líder Gobierno Digital | Acuerdos de Seguridad y Privacidad | Revisión de documentación, Recopilación de información, lista de chequeo | 5 | Octubre | | | | 5 | |
| 4.10 | Socializar acuerdos para gestionar la seguridad de la información y privacidad. | Profesional Gobierno Digital | Líder Gobierno Digital | Acta | Plan de Comunicaciones | 5 | Octubre | | | | | 5 |
| 4.11 | Establecer el seguimiento a la implementación de acuerdos | Comité técnico de seguridad | Líder Gobierno Digital | Informe de seguimiento, solicitudes de cambio y actualizaciones | Reuniones de estado | 5 | Noviembre | 5 | | | | |
| 4.12 | Crear y aprobar plan de continuidad (BCP) | Comité técnico de seguridad | Líder Gobierno Digital | Plan de continuidad | Revisión de documentación, Recopilación de información, lista de chequeo | 5 | Noviembre | | 5 | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.13 | Socializar plan de continuidad de negocios | Profesional Gobierno Digital | Líder Gobierno Digital | Acta | Plan de Comunicaciones | 5 | Noviembre | | | 5 | | |
| 4.14 | Crear y aprobar el Plan de Transición de IPv4 a IPv6 | Comité técnico de seguridad | Líder Gobierno Digital | Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.<br><br>Guía No 20 - Transición de IPv4 a IPv6 para Colombia.<br><br>Guía No 19 – Aseguramiento del Protocolo IPv6. | 5 | Noviembre | | | | 5 | |
| 4.15 | Socializar plan Transición IPV4 a IPV6 | Profesional Gobierno Digital | Líder Gobierno Digital | | Plan de Comunicaciones | 5 | Noviembre | | | | | 5 |
| 4.16 | Asegurar la conservación y preservación a largo plazo de los documentos, mediante programas y planes en el marco del Sistema Integrado de Conservación | Oficina de Gestión Documental | Oficina de Gestión Documental | Plan de preservación a largo plazo | Microsoft Word | 25 | abril | 5 | 5 | 5 | 5 | 5 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.17 | Establecer el seguimiento a la implementación del plan de transición | Comité técnico de seguridad | Líder Gobierno Digital | Informe de seguimiento, solicitudes de cambio y actualizaciones | Reuniones de estado | 5 | Diciembre | 5 | | | | |
| 4.18 | Definir y presentar indicadores de gestión de la seguridad de la información y privacidad | Comité técnico de seguridad | Líder Gobierno Digital | Informe de indicadores | Recopilación de información, revisión de documentación | 5 | Diciembre | | 5 | | | |
| **5** | **FASE V : NIVEL DE MADUREZ** | | | | | | | | | | | |
| 5.1 | Revisar estado de la gestión de seguridad y privacidad de la información. | Comité técnico de seguridad | Líder Gobierno Digital | Diligenciamiento de Herramienta | Herramienta MSPI | 5 | Diciembre | | | 5 | | |
| 5.2 | Revisar nivel de madurez en la gestión de la seguridad y privacidad de la información | Comité técnico de seguridad | Líder Gobierno Digital | Diligenciamiento de Herramienta | Herramienta MSPI | 5 | Diciembre | | | | 5 | |

## 8. Seguimiento

En aras de mantener una buena gestión en el desarrollo de las actividades de la Entidad, una vez realizado el plan y cumplido los procedimientos, se realizará medición y seguimiento al cumplimiento de las actividades planeadas trimestralmente. Teniendo en cuenta que el Sistema de Gestión es un proceso que se realiza de manera permanente se deberá estar en continua revisión por parte de las áreas encargadas, es decir se crea un ciclo que permite 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.

## 9. Documentos de Referencia

- 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 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas 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.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1955 de 2019. por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”.
- Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- 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. Decreto 620 de 2020. por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- CONPES 3905 de 2020. Política Nacional de Confianza y

Seguridad Digital.

- NTC ISO 27001:2013
- MSPI – Modelo de Seguridad y Privacidad de la Información

## 10. Control de Cambios

| Fecha | Versión | Descripción del Cambio. |
|---|---|---|
| 07-01-2021 | Versión 1 | Elaboración del Plan |
| | | |