Plan de Seguridad y Privacidad de la Información

Versión 3

TABLA DE CONTENIDO

Contenido

Plan de seguridad y privacidad de la información

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. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.

La nueva 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. Estos se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos para alcanzar los logros de la política.

Este habilitador se soporta en 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 del mismo, 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 una actividad obligatoria como lo establece el decreto 612 de 2018 en el artículo 1, el cual debe ser integrado y planificado a los planes institucionales en el ámbito de aplicación del modelo integrado de planeación y gestión.

Así mismo, la resolución 0500 de marzo 10 del 2021 precisa la necesidad de que los sujetos obligados deban adoptar las 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 e incidentes de seguridad digital. La 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

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, el marco de ciberseguridad NIST y la NTC ISO 27001.

1.1 Objetivos Específicos

- 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.

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. 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. "

4. Situación Actual

La Alcaldía Distrital de Barranquilla ha realizado actividades tendientes a la implementación del modelo de seguridad y privacidad de la información, para lo cual se cuenta con una política aprobada por la alta dirección obteniendo los siguientes resultados:

Ámbito	Situación Actual
Diagnostico	Se cuenta con diagnóstico inicial y las respectivas actualizaciones de las vigencias
Plan de seguridad y privacidad	En la vigencia 2021 se crea y formaliza el plan para las vigencias 2021-2023. Así mismo, se han ejecutado las actividades correspondientes a cada vigencia, alcanzando un porcentaje de avance del 76.1%
Cronograma de implementación	El plan de seguridad y privacidad de la información, contienen cronograma de actividades por vigencias, el cual se actualiza y realiza seguimiento trimestral y anual según los requerimientos de la primera y segunda línea de defensa de la entidad.

5. Tratamiento de Riesgos de seguridad de la Información

La entidad definió las directrices para el tratamiento de riesgos de seguridad digital en la Guía para la administración de riesgos de procesos de la Alcaldía Distrital de Barranquilla, adoptada en el año 2022 para la gestión de los riesgos en cada una de las etapas.

En el cronograma adjunto en el presente documento en el ítem 3 se definen las actividades de: identificación, análisis, valoración y tratamientos de riesgos, para la gestión de riesgos de seguridad de la información en la entidad.

6. Roles y responsabilidades

La seguridad y privacidad de la información debe ser una cultura, en la cual se deben involucrar todos los colaboradores, tantos servidores públicos, usuarios y contratistas pues son los directamente 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 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. • 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 con el fin de prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y servicios que presta 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 TIC cualquier incidencia respecto a la seguridad de la información.

7. 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.

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)

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.

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:

2. CRONOGRAMA								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	Año	Trimestres			
					1	2	3	4
1	**FASE I: DEFINIR MARCO DE SEGURIDAD Y PRIVACIDAD**							
1,1	Crear el comité de Seguridad y Privacidad de la información	Gerencia TIC	Líder de Proceso	2021				
1,2	Definir los roles y responsabilidades en el comité de seguridad y privacidad de la información digital por áreas de la Gerencia TIC	Gerencia TIC	Líder de Proceso	2021				
1,3	Definir y documentar las funciones del comité de Seguridad y Privacidad de la información	Gerencia TIC	Líder de Proceso	2021				
1,4	Crear el equipo de repuesta a incidentes	Gerencia TIC	Líder de Proceso	2022				
1,5	Definir y documentar las funciones del equipo de respuesta a incidentes	Gerencia TIC (Administrativa)	Líder de Proceso	2022				
1,6	Identificar el marco legal, requisitos técnicos normativos, documentos, lineamientos y herramientas asociadas a la seguridad y privacidad de la información.	Gerencia TIC	Asesor Jurídico	2021				
1,7	Actualizar Matriz de verificación de Requisitos Legales y normativo de Seguridad de la Información y privacidad	Administrativa	Asesor Jurídico	2022				
1,8	Identificar estado actual de la gestión de seguridad y privacidad de la información.	Gerencia TIC (Administrativa)	Agente de Cambio	2022				
1,9	Identificar nivel de madurez en la gestión de la seguridad y privacidad de la información	Gerencia TIC (Administrativa)	Agente de Cambio	2022				
1,1	Identificar vulnerabilidades técnicas y administrativas (Insight fases siguientes)	Gerencia TIC (Administrativa)	Agente de Cambio	2021				

2. CRONOGRAMA								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	Año	Trimestres			
					1	2	3	4
1,11	Actualizar vulnerabilidades técnicas y administrativas (mapa de riesgos)	Gerencia TIC (Administrativa)	Agente de Cambio	2022				
1,11	Plan de diagnóstico de IPv4 a IPv6	Gerencia TIC Infraestructura	Líder de Proceso	2022-2023				
2	**FASE II : ACTIVOS DE INFORMACIÓN**							
2,1	Definir lineamientos para la actualización y levantamiento del inventario de activos de información	Gerencia TIC; Gestión Documental	Líder de Proceso	2021				
2,2	Socializar Herramienta para el levantamiento de información	Gerencia TIC; Gestión Documental	Líder de Proceso	2022				
2,3	Revisar la información suministrada para actualizar el Inventario de Activos de Información	Gerencia TIC; Gestión Documental	Líder de Proceso	2021				
2,4	Establecer el plan de revisión de la herramienta para el levantamiento de activos y la actualización del inventario de activos	Gerencia TIC y Oficina de Gestión Documental	Líder de Proceso	2022				
2,5	Actualización e Identificación y clasificación de la Información pública, clasificada y reservada de la Alcaldía Distrital de Barranquilla	Gerencia TIC; Gestión Documental	Líder de Proceso	2021-2023				
2,6	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	2021-2022				
2,7	Seguimiento y capacitación en el manejo y aplicación Tablas de Retención Documental	Oficina de Gestión Documental	Oficina de Gestión Documental	2021				
2,8	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	2021				
2,9	Verificación de seguridad en las Transferencias documentales de acuerdo a las Tablas de Retención Documental	Oficina de Gestión Documental	Oficina de Gestión Documental	2021				
3	**FASE III: GESTIÓN DE RIESGOS**							

2. CRONOGRAMA								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	Año	Trimestres			
					1	2	3	4
3,1	Revisar metodología de gestión de riesgo	Planeación y áreas convocadas	Agente de Cambio	2021				
3,2	Identificar Riesgos de Seguridad y Privacidad de la Información	Todas las áreas	Agente de Cambio	2022-2023				
3,3	Realizar el análisis de riesgos de seguridad y privacidad de la información	Todas las áreas	Agente de Cambio	2022-2023				
3,4	Elaborar plan de tratamiento de riesgos	Todas las áreas	Agente de Cambio	2022-2023				
3,5	Socializar Plan de tratamiento de riesgos	Todas las áreas	Agente de Cambio	2022-2023				
3,6	Establecer el seguimiento a la implementación del plan de tratamiento de riesgos	Gerencia TIC (Administrativa)	Agente de Cambio	2022-2023				
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	2021				
4,2	Aprobar políticas de seguridad de la información y privacidad.	Gerencia TIC	Líder de Proceso	2021				
4,3	Socializar políticas de seguridad de la información y privacidad.	Gerencia TIC (Administrativa)	Líder de Proceso	2022				
4,4	Establecer el plan de seguimiento a la implementación de políticas	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2022				
4,5	Revisar y actualizar procedimientos para gestionar la seguridad y privacidad	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				

2. CRONOGRAMA								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	Año	Trimestres			
					1	2	3	4
4,6	Crear y aprobar procedimientos para gestionar la seguridad y privacidad de la información	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				
4,7	Socializar procedimientos de seguridad de la información y privacidad.	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				
4,8	Establecer el plan de seguimiento a la implementación de procedimientos	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				
4,9	Crear y aprobar acuerdos para gestionar la seguridad y privacidad de la información	Gerencia TIC	Agente de Cambio	2022-2023				
4,1	Socializar acuerdos para gestionar la seguridad de la información y privacidad.	Gerencia TIC (Administrativa)	Agente de Cambio	2022-2023				
4,11	Establecer el seguimiento a la implementación de acuerdos	Gerencia TIC (Administrativa)	Agente de Cambio	2022-2023				
4,12	Crear y aprobar plan de continuidad (BCP)	Gerencia TIC (Administrativa)	Líder de Proceso	2021-2023				
4,13	Socializar plan de continuidad de negocios	Gerencia TIC (Administrativa)	Líder de Proceso	2021-2023				
4,14	Crear y aprobar el Plan de Transición de IPv4 a IPv6	Gerencia TIC (Infraestructura)	Líder de Proceso	2021-2023				
4,15	Socializar plan Transición IPV4 a IPV6	Gerencia TIC (Infraestructura)	Líder de Proceso	2021-2023				
4,16	Establecer el seguimiento a la implementación del plan de transición	Gerencia TIC (Infraestructura)	Agente de Cambio	2021-2023				
4,17	Definir y presentar indicadores de gestión de la seguridad de la información y privacidad	Gerencia TIC (Administrativa)	Agente de Cambio	2022-2023				
5	**FASE V : NIVEL DE MADUREZ**							

2. CRONOGRAMA								
CÓDIGO	ACTIVIDAD	AREAS QUE INTERVIENEN	RESPONSABLE DE LA ACTIVIDAD	Año	Trimestres			
					1	2	3	4
5,1	Revisar estado de la gestión de seguridad y privacidad de la información.	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				
5,2	Revisar nivel de madurez en la gestión de la seguridad y privacidad de la información	Gerencia TIC (Administrativa)	Agente de Cambio	2021-2023				

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 genal, 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.
- Decreto 767 de mayo de 2022, Actualización política Colombiana de Gobierno Digital
- 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
28-01-2022	Versión 2	Actualización de las actividades del plan.
25-01-2023	Versión 3	Actualización del plan