ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de
Servicios Públicos

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Unidad Administrativa Especial de Servicios Públicos

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de
Servicios Públicos

CONTENIDO

1. INTRODUCCIÓN

La Unidad Administrativa Especial de Servicios Públicos - UAESP, en respeto de los Derechos Humanos y de los principios constitucionales y legales, entiende la información, como uno de los activos más importantes para el cumplimiento de su misionalidad y la toma de decisiones, por esta razón y como parte del proceso de mejora continua, se ha comprometido a definir, implementar, operar y actualizar la Política General de Seguridad y Privacidad de la Información, con el fin de establecer un marco de confianza en el ejercicio de sus deberes, alineados a las necesidades del negocio y los requerimientos legales, reglamentarios, regulatorios y de normas colombianas en materia de seguridad y privacidad de la información.

De acuerdo con lo anterior, el presente documento, establece el compromiso, los principios y lineamientos generales que buscan proteger y mantener la integridad, confidencialidad y disponibilidad de la información, implementando controles para el desarrollo de todas las actividades relacionadas con el tratamiento de la información en la Entidad, con el fin de mitigar los riesgos e incidentes de seguridad de la información; Así mismo, define los deberes, obligaciones y responsabilidades de los sujetos aplicables.

Esta política es desarrolla de manera proactiva, confiable, articulada, colaborativa y estará complementada de manera detallada en el Manual de Políticas de Seguridad y Privacidad de la Información, el cual será publicado y consultado en el Sistema Integrado de Gestión – SIG.

2. TÉRMINOS Y DEFINICIONES

Activos de información: Toda información o elemento relacionado con el tratamiento de esta (Documentos, hardware, software, servicios, edificios, personas, entre otros) que tenga valor para la organización y por lo tanto se debe proteger. Se puede considerar un activo de información los datos creados o utilizados por un proceso, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, equipos de cómputo relacionados al tratamiento o almacenamiento de información, software del sistema, servicios utilizados para la transmisión, recepción y control de la información, entre otros.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños o afectaciones aun activo de información.

Autoridad competente: Es la autoridad apta e idónea para tratar de un determinado procedimiento o proceso de acuerdo con la ley.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27000]

DAFP: Departamento Administrativo de la Función Pública (DAFP), es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Disponibilidad: La propiedad de tener la información cuando es requerida. Se relaciona con la facilidad y oportunidad de acceso a la información.

Estándar informático: todo aquel patrón o parámetro que permite establecer uniformidad en características de equipos, sistemas de cómputo y procedimientos de operación, con el cual se pretende garantizar la integridad, compatibilidad y racionalidad para los procesos tecnológicos de la institución.

Evento de seguridad de la información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la Política de Seguridad de la Información o falla en los controles.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la Entidad y de amenazar la seguridad y privacidad de la información

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO 27000]

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.

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 en cualquier medio: impreso o digital. (ISO/IEC 27000).

Es pertinente señalar que "seguridad de la información" no solo corresponde a Seguridad Informática, sino que su alcance se complementa con ciberseguridad, seguridad física, ambiental y del recurso humano entre otras, buscando mantener la confidencialidad, la disponibilidad e integridad de la información. [Directiva 002 de 2021 – Alcaldía Mayor de Bogotá]

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Terceros: Para efectos de esta política, el termino hace referencia a proveedores, practicantes o cualquier persona natural o jurídica que tenga un vínculo laboral con la Entidad y preste un servicio de forma directa o indirecta bien sea en las instalaciones de la Entidad o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones de la Entidad.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3)

Usuario: Cualquier persona que tiene acceso a la plataforma y a los activos de información, sea en calidad de usuario final, tercero o administrador de la plataforma.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. OBJETIVOS

3.1 Objetivo General

Establecer los lineamientos orientados a proteger y preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información gestionados por la Entidad, mediante una gestión integral de riesgos y la implementación de controles que prevengan la materialización de incidentes de seguridad y privacidad de la información, cumpliendo los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua, el uso efectivo y la apropiación de seguridad y privacidad de la Información.

3.2 Objetivos específicos

1. Definir las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.

2. Mitigar el impacto de los incidentes de seguridad y privacidad de la información.

3. Establecer mecanismos de control que permitan fortalecer la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la Información.

4. Fortalecer la cultura organizacional, a través de la concienciación, participación y apropiación de la seguridad y privacidad de la información, orientados a la mejora continua.

5. Cumplir los principios, requisitos legales, reglamentarios y regulatorios en materia de seguridad y privacidad de la información.

6. Garantizar la continuidad del negocio frente a posibles incidentes de seguridad y privacidad de la información.

7. Incrementar la confianza y la seguridad digital de los grupos de interés, mediante la implementación de un sistema de gestión de seguridad de la información -SGSI.

4. ALCANCE

El alcance de esta Política General de Seguridad y Privacidad de la Información aplica para todos los servidores (as) públicos (as), contratistas, proveedores, operadores, así como aquellas personas o terceros que utilicen, recolecten, procesen, intercambien, consulten y accedan a los activos de información de la Unidad Administrativa Especial de Servicios Públicos – UAESP.

De igual manera, la presente política está orientada a todos los procesos de la entidad, bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión - MIPG propuesto por el DAFP y el Modelo de Seguridad y Privacidad de la Información - MSPI.

5. MARCO NORMATIVO

Teniendo en cuenta las disposiciones legales sobre seguridad de la información, el marco normativo en la materia, sin ser restringido, corresponde a:

CONSTITUCIÓN POLITICA: Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…).

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Ley 23 de 1989: Sobre derechos de autor.

Ley 527 de 1999: Por medio de 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 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 603 DE 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 962 de 2005: Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

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 1341 de 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro 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 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.

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.

Decreto 2106 DE 2019: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Decreto 2364 de 2012: Firma electrónica. Decreto 2609 de 2012 Expediente electrónico.

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".

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, derogado parcialmente por el Decreto 1081 de 2015.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Compilado en el Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo." 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 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Reglamenta parcialmente la ley 1581 de 2012 y compila el Decreto 103 de 2015.

Decreto 1008 de 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Resolución 2710 del 2017: Por la cual se establecen lineamientos para la adopción del protocolo IPV6.

Directiva 002 de 2018 - Secretaría Jurídica Distrital: Tratamiento de Datos Personales.

Directiva 005 de 2018 - Secretaría Jurídica Distrital: Tratamiento de datos personales – Autorizaciones, datos sensibles, datos de niños, niñas y adolescentes, cámaras y videos de seguridad, sanciones y recomendaciones.

Resolución 1519 de 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 materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

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 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".

CONPES 3854 de 2016: Política Nacional de Seguridad Digital.

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

6. COMPROMISO DE LA DIRECCIÓN

La Dirección de la Unidad Administrativa Especial de Servicios Públicos, entendiendo la importancia de una adecuada gestión de los activos de información, se compromete con la implementación, seguimiento y medición del Modelo de Seguridad y Privacidad de la Información MSPI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de los requerimientos legales, reglamentarios, regulatorios y de normas colombianas en materia de seguridad y privacidad de la información y en concordancia con la misión, visión, los objetivos y planes estratégicos de la Entidad.

7. PRINCIPIOS

Los principios están orientados a proteger los tres pilares de seguridad de la información, confidencialidad, integridad y disponibilidad, para garantizar que la información recibe los niveles de protección adecuados.

Principio de cumplimiento normativo:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, se ajustará a la normativa de aplicación legal vigente con relación a la seguridad y privacidad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

Principio de Gestión de Riesgos:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los riesgos hasta niveles aceptables implementando controles de seguridad adecuados y pertinentes.

Principio de concienciación y formación:

La Unidad Administrativa Especial de Servicios Públicos – UAESP, articulará programas de formación, sensibilización y campañas de concienciación para todos los servidores (as) públicos (as), contratistas y terceros que tengan acceso a los activos de información de la entidad en materia de seguridad de la información.

Principios de continuidad del negocio:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, asegurará la continuidad del negocio mediante planes de contingencia para los servicios de la información críticos y de procesos misionales, velando por la confidencialidad, integridad y disponibilidad de la información.

Principio de responsabilidad:

Todos los servidores (as) públicos (as), contratistas y terceros en relación con la Unidad Administrativa Especial de Servicios Públicos – UAESP, deben ser responsables de los activos de información y sus acciones relacionadas a la seguridad de la información, cumpliendo con las normas y controles establecidos.

Principio de gestión de incidentes:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los incidentes de seguridad digital articulando las capacidades que permitan atender de forma oportuna y adecuada la materialización de riesgos.

Principio de mejora continua:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, revisará de manera periódica el grado de eficacia de los controles de seguridad implementados en la Entidad y velará por la disponibilidad de sus procesos estratégicos, misionales, de apoyo y de evaluación y la continuidad de su operación basada en la prevención de incidentes de seguridad de la información.

Lo anterior, con el fin de aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico.

Principio de Confianza:

La unidad Administrativa Especial de Servicios Públicos, propenderá por la implementación, adecuación y uso de tecnologías, controles y lineamientos que permitan la protección de los activos de información.

8. POLÍTICA GENERAL

La Unidad Administrativa Especial de Servicios Públicos – UAESP protegerá y preservará la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información en todo su ciclo de vida, mediante la gestión de riesgos, fomentando una cultura de seguridad y privacidad de la información en los servidores (as) públicos (as), contratistas y terceros que permita establecer un marco de confianza en sus deberes acorde con las necesidades de las diferentes grupos de interés y el cumplimiento de los requisitos legales pertinentes.

9. OBLIGACIONES

Los servidores (as) públicos (as), contratistas y terceros que accedan a los activos de información de la Unidad Administrativa Especial de Servicios públicos – UAESP, son responsables del manejo adecuado de la información utilizada en el desarrollo de sus actividades u obligaciones contractuales.

Los sujetos de aplicabilidad de esta política deberán cumplir con los lineamientos, requisitos y buenas prácticas legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información que adopte la entidad y que se encuentran en el Manual de Políticas de Seguridad y Privacidad de la Información, en su última versión, previniendo, detectando y reportando cualquier incidente, contravención u omisión de la política aquí descrita.

10. REVISIÓN

La Política General de Seguridad y Privacidad de la Información será revisada anualmente, o cuando se requiera, para mantenerla oportuna, suficiente y eficaz.

El proceso de revisión será liderado por el Oficial de Seguridad y Privacidad de la Información, el Oficial de Protección de Datos Personales, la Oficina de Tecnologías de la Información y las Comunicaciones, de igual forma, la política será revisada y aprobada por el Comité Institucional de Gestión y Desempeño.

11. ROLES Y RESPONSABILIDADES

Para llevar a buen término el cumplimiento de las políticas y gestión de la seguridad y privacidad de la información, la Unidad Administrativa Especial de Servicios Públicos ha definido los siguientes roles:

ROL	PERFIL
Comité Institucional de Gestión y Desempeño	• Orientar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades: o Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información. o Promover la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad. o Aprobar acciones y mejores prácticas en la implementación del MSPI. o Adoptar las decisiones que permitan la gestión y mitigación de riesgos críticos de seguridad de la información. • Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

ROL	PERFIL
Jefe Oficina TIC	• Asesorar a la Dirección General y dependencias de la Unidad en materia de Seguridad y privacidad de la Información. • Planear y administrar los recursos informáticos y de telecomunicaciones para satisfacer las necesidades y requerimientos de los usuarios de la UAESP, de conformidad con las políticas, metodologías y normatividad vigente. • Adoptar e implementar buenas prácticas o estándares informáticos, de calidad y de seguridad y privacidad de la información. • Apoyar y aprobar estudios, investigación y análisis de tendencias tecnológicas para su posible aplicación en la Entidad. • Apoyar en la formulación del plan de capacitación en relación con seguridad y privacidad de la información. • Asumir el rol del Oficial de Seguridad de la Información, en ausencia de la persona designada en la Entidad para este fin.
Oficial de Seguridad de la Información	• Apoyar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información de conformidad con la regulación vigente. • Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad. • Realizar la planificación y cronograma de la implementación del MSPI. • Proponer, definir, elaborar o acompañar en la implementación las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI. • Realizar el acompañamiento a los procesos o proyectos en materia de seguridad y privacidad de la información. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y Contratistas. • Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Liderar la implementación el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. • Verificar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta dirección. • Convocar la participación de los servidores (as) públicos (as),

ROL	PERFIL
	contratistas o terceros cuando el incidente lo amerite. • Verificar el cumplimiento de los procedimientos y buenas prácticas en gestión de incidentes y recomendar, si lo amerita, la aplicación de planes de contingencia o continuidad. • Indagar todos los incidentes de seguridad de la información y apoyar el análisis forense, cuando se requiera.
Oficial de protección de Datos Personales	• Consolidar y reportar la información de Base de datos personales que maneja o tiene la entidad en conformidad con la normatividad vigente. • Fomentar la cultura de la protección y privacidad de datos personales que tiene a cargo la entidad y el cumplimiento de la normatividad aplicable. • Apoyar en la definición, implementación y seguimiento de los controles para el tratamiento de datos personales y privacidad de la información de acuerdo con la normatividad vigente. • Apoyar en la elaboración, comunicación y aplicación de la política de datos personales, con los criterios de calidad y oportunidad. • Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC o entes externos en temas de su competencia.
Líderes de Proceso	• Velar por el cumplimiento de las políticas de seguridad y privacidad en temas de su competencia, en sus equipos de trabajos o personal a cargo. • Identificar e inventariar los nuevos activos de información y los riesgos de seguridad y privacidad de la información asociados. • Apoyar la gestión de riesgos de seguridad digital o de la información conforme a la Política de Administración de Riesgos o la que haga sus veces. • Reportar cualquier evento o riesgo materializado, por medio de los canales dispuesto para ello.
Usuarios	• Conocer y cumplir las Políticas de Seguridad y Privacidad de la Información y la normatividad vigente relacionada en el desarrollo de sus funciones u obligaciones contractuales. • Reportar incidentes de seguridad que atenten contra la confidencialidad, disponibilidad o integridad de la información o cuando se evidencie un incumplimiento de las Políticas de Seguridad y Privacidad de la Información. • Participar en las campañas de sensibilización del MSPI. • Participar de las actividades para la identificación de activos de información y riesgos de seguridad y privacidad de la información. • Colaborar en el desarrollo de las auditorías internas y externas al MSPI.

11.1 Perfiles.

La designación del Oficial de Seguridad de la información y el Oficial de Datos Personales será a discreción de la Entidad, tomando en consideración los siguientes perfiles:

ROL	PERFIL
Oficial de Seguridad de la Información	Núcleos Básicos del Conocimiento (NBC): Ingeniería de Sistemas, informática, telemática, Ingeniería Electrónica, telecomunicaciones, Ingeniería Industrial, afines o cualquiera pertinente a la naturaleza de las responsabilidades descritas en el numeral 11. Conocimientos: Implementación y mantenimiento del estándar ISO 27001:2013 o versiones posteriores, si existieran, conocimientos en ISO 27032 o prácticas de seguridad del Instituto Nacional de Estándares y Tecnologías -NIST-, riesgos de seguridad de la información o seguridad digital, arquitecturas de seguridad informática, gestión de incidentes de seguridad de la información y capacidad para desarrollar políticas y procesos de Seguridad y Ciberseguridad. Deseable: • Postgrados en seguridad informática, seguridad de la información, ciberseguridad o afines. • Certificación en ISO 27001:2013 o posteriores. • Certificaciones en CISM, CISSP, CSX o GRISC.
Oficial de protección de Datos Personales	Núcleos Básicos del Conocimiento (NBC): Cualquiera pertinente a la naturaleza de las responsabilidades descritas en el numeral 11. Conocimientos: Legislación y buenas prácticas en materia de protección de datos personales, funcionamiento de la Entidad junto con sus normas y procedimientos administrativos.

12. INCUMPLIMIENTO

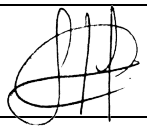
Cualquier contravención u omisión de la política aquí descrita, traerá consigo, las consecuencias legales que apliquen a la normatividad vigente y se sancionará por parte de la autoridad competente.

13. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01	15/10/2019	Se adopta la Política de Seguridad de la Información mediante resolución interna 0589 de 2019

02	28/09/2021	Se actualiza la normativa legal vigente aplicable en relación con la seguridad de la información. Se ajustan los objetivos y se definen objetivos específicos de acuerdo con los requerimientos de la ISO 27001, el MSPI y la Política del Sistema integrado de Gestión. Se elimina las menciones al Modelo de Transformación Organizacional – MTO. Se ajustan los principios básicos y se define de forma explícita el compromiso por la dirección. Se definen y ajustan la matriz de roles y responsabilidades en materia de seguridad de la información de acuerdo con la implementación del MSPI.
03	21/06/2022	Se actualiza y ajusta de conformidad al 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. Se adiciona el principio de confianza, el numeral 10 especificando la revisión de la política y responsables. Se ajustan los roles y responsabilidades para la implementación del MSPI, al igual que sus nombres, y se adiciona el perfil mínimo, para los Oficiales de Seguridad de la Información y el de Protección de Dato Personales y se especifica el incumplimiento a la política.

AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Jerce Aurora Sandoval Macias	Auxiliar Administrativo – Oficina TIC	
	Juan Sebastian Perdomo Mendez	Profesional Universitario – Oficina TIC	
Revisó	Cesar Mauricio Beltran Lopez	Jefe Oficina de Tecnologías de la Información y las Comunicaciones TIC.	
Aprobó	Comité Institucional de Gestión y Desempeño		Acta de comité Institucional de Gestión y Desempeño del 21/06/2022