1. OBJETIVOS

1.1 Objetivo General:

Diseñar la Política de Seguridad Digital en la Veeduría Distrital, en un marco de gestión de los riesgos de Seguridad Digital en el que la Entidad pueda estar expuesta desde la perspectiva de entorno cibernético y siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información MSPI.

1.2 Objetivos Específicos:

Establecer articulación con las autoridades definidas por el gobierno nacional en la identificación, prevención y gestión de incidentes de seguridad digital que afecten a la Veeduría Distrital.

Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en la Veeduría Distrital siguiendo la metodología del Departamento Administrativo de la Función Pública - DAFP y del Ministerio de Tecnología de Comunicaciones – MinTIC establecida para ello.

Desarrollar el Modelo de Seguridad y Privacidad de la Información MSPI, en concordancia con la Política de Gobierno Digital.

Promover en los usuarios internos el uso y comportamiento responsable, en el entorno digital, que pueda afectar la seguridad de los activos digitales/información de la Entidad.

2. ANTECEDENTES Y JUSTIFICACIÓN

DIMENSIONES DE LA POLÍTICA DE SEGURIDAD DIGITAL

Con el fin de adoptar un enfoque multidimensional, que garantice la seguridad digital y atienda las necesidades y expectativas de todas las partes interesadas, se definen cinco dimensiones estratégicas (DE). Estas dimensiones determinan los campos de acción de la política nacional de seguridad digital.

Gobernanza de la seguridad digital: articulación y armonización de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno nacional.

Marco legal y regulatorio de la seguridad digital: marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la política.

Gestión sistemática y cíclica del riesgo de seguridad digital: conjunto de iniciativas, procedimientos o metodologías coordinadas con el fin de abordar, de manera cíclica y holística, los riesgos de seguridad digital en el país.

Cultura ciudadana para la seguridad digital: sensibilización de las múltiples partes interesadas, para crear y fomentar una cultura ciudadana responsable en la seguridad digital.

Capacidades para la gestión del riesgo de seguridad digital: fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y

administrativas en las múltiples partes interesadas, para adelantar la gestión de riesgos de la seguridad digital.

(Tomado de documento CONPES 3854).

ESTRATEGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La estrategia de gestión de riesgos para abordar la seguridad digital debe tener un enfoque flexible y ágil para abordar las incertidumbres digitales. Lo anterior, con el fin de alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales, y proteger a las personas frente a las amenazas de seguridad digital (Organización para la Cooperación y Desarrollo Económico OCDE, 2015a).

De acuerdo con las recomendaciones de la OCDE, la estrategia nacional debe ser consistente con el conjunto de principios formulados, debe crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe fomentar la confianza en el entorno digital y, además, debe: (i) estar apoyada desde el más alto nivel de gobierno; (ii) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social; (iii) estar dirigida a todas las partes interesadas; y (iv) ser el resultado de un enfoque intra-gubernamental, coordinado, abierto y transparente, donde participen las múltiples partes interesadas.

La política nacional de seguridad digital: (i) adoptará la gestión sistemática y cíclica del riesgo; (ii) será liderada desde el alto nivel del gobierno; (iii) asegurará la defensa y seguridad nacional; (iv) estimulará la prosperidad económica y social; (v) adoptará un enfoque multidimensional, es decir, la seguridad digital será abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social; (vi) tendrá en cuenta a las múltiples partes interesadas; (vii) promoverá la responsabilidad compartida; (viii) salvaguardará los derechos humanos; (ix) protegerá los valores nacionales; y (x) concientizará y educará.

(Tomado de documento CONPES 3854).

3. BASE LEGAL

Norma	Descripción
Constitución Política	Artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre. Artículo 20 en donde 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 masivos de comunicación. Artículo 76 que establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado. Artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano.
Ley 1928 de 24 de 2018	Por la cual se aprueba el convenio sobre la ciberdelincuencia.

Norma	Descripción
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 1581 de 2012	Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
Ley 1437 de 2011 (Uso de medios electrónicos procedimiento administrativo)	Consagra la utilización de medios electrónicos en el procedimiento administrativo y permite adelantar los trámites y procedimientos administrativos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria. Especialmente los artículos 59 al 64.
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.
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 594 de 2000 (Ley general de archivos)	Habilita el uso de nuevas tecnologías de manera general, lo cual viabiliza el uso de firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código penal)	En particular las materias atinentes a: i) violación a los derechos patrimoniales de autor y derechos conexos (modificación introducida por la Ley 1032 de 2006); ii) protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC (modificación introducida por la Ley 1273 de 2009)
Ley 527 de 1999 Comercio electrónico	Se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establece certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6, 8, 7, 28, 12 y 13), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del decreto ley 019 de 2012).
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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Norma	Descripción
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Decreto Nacional 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Decreto 2758 de 2012 (Modifica la estructura del Ministerio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
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 316 de 2008	Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Decreto 1151 de 2008, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	Lineamientos generales de la Estrategia de Gobierno en línea.
Decreto 619 de 2007	Se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.
Acuerdo 702 de 2018	Por el cual se adoptan lineamientos para la definición de estrategias de prevención frente a la ocurrencia de crímenes cibernéticos que amenazan o vulneran los derechos de las niñas, niños, adolescentes y jóvenes del distrito capital.
Acuerdo 003 de 2015.	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.
Resolución 166 de 2017 de la Veeduría Distrital	Por medio de la cual se adopta la Política de Seguridad de la Información de la Veeduría Distrital.
Resolución 3564 de 2015 – Alcaldía Mayor	Por la cual se reglamentan algunos artículos del Decreto 1081 de 2015.Ley de transparencia.

Norma	Descripción
Resolución 318 de 2016 de la Veeduría Distrital	Por medio de la cual se adopta la Política de Tratamiento y Protección de Datos Personales de la Información de la Veeduría Distrital.
Resolución 305 de 2008 - Alcaldía Mayor	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Resolución 004 de 2017	Por la cual se modifica la Resolución 305de 2008 de la Comisión Distrital de Sistemas.
Directiva 002 de 2018	Tratamiento de datos personales.
Directiva 5 de 2005	Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital.
Concepto 133 de 2017 Secretaría General Alcaldía Mayor de Bogotá D.C	Concepto Jurídico Habeas Data-Correos masivos-Transferencia de información entre entidades públicas
Norma Técnica NTC 5854 5854 de 2011	Accesibilidad a páginas web
Norma Técnica ISO/IEC 27002	Señala los requisitos del Sistema de Gestión de Seguridad de la Información.
Manual Gobierno Digital	Define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de la Política de Gobierno Digital.
CONPES 3854 de 2016	Por la cual se define la Política Nacional de Seguridad Digital.
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y ciberdefensa.
Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP – Min TIC	Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital
Modelo Nacional de Gestión de Riesgos de Seguridad Digital	Modelo Nacional de Gestión de Riesgos de Seguridad Digital

4. GLOSARIO

Amenaza cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Documento CONPES 3854)

Ataque cibernético: acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Documento Modelo Nacional Riesgo de Seguridad Digital)

Ciberdefensa: es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (Documento CONPES 3854).

Ciberespionaje: es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas. (Documento CONPES 3854).

Ciberterrorismo: es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo. (Documento CONPES 3854).

Cibercrímen (delito cibernético): conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (Documento CONPES 3854).

Ciberlavado: es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades. (Documento CONPES 3854).

Ciberseguridad: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (Documento CONPES 3854).

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (Documento CONPES 3854).

Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (Documento CONPES 3854).

Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (Documento CONPES 3854).

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos. (Documento CONPES 3854).

Infraestructura crítica cibernética nacional: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (Documento CONPES 3854).

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas. (Documento CONPES 3854).

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. (Documento CONPES 3854).

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).

Seguridad de la información: Entendida como el “conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información” (ISO/IEC 27000). (Guía de ajuste del Sistema Integrado de Gestión Distrital. Tomo II)

Seguridad informática: comprende los métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información contenida en formato digital en estos medios. (Guía de ajuste del Sistema Integrado de Gestión Distrital. Tomo II)

Seguridad digital o ciberseguridad: Conjunto de medidas de “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.A diferencia de la seguridad de la información, en la ciberseguridad se aplican medidas ofensivas y no solo de defensa. (Guía de ajuste del Sistema Integrado de Gestión Distrital. Tomo II)

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Documento CONPES 3854).

5. PRINCIPIOS

5.1 Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los

datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. (Documento CONPES 3854).

5.2. Adoptar un enfoque incluyente y colaborativo que involucre activamente a las múltiples partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital. (Documento CONPES 3854).

5.3. Asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital. (Documento CONPES 3854).

5.4. Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. Lo anterior, fomentará la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía. (Documento CONPES 3854).

6. ÁREAS O EJES TEMÁTICOS DE LA POLÍTICA INTERNA DE OPERACIÓN CON SUS RESPONSABLES

6.1 RESPONSABLES

Comité Institucional de Gestión y Desempeño de la Veeduría Distrital: Responsables de aprobar la Política de Seguridad Digital de la Entidad.

Líder del El Equipo de Gestión TIC de la Veeduría Distrital: Responsable en liderar la implementación la Política de Seguridad Digital en la Entidad.

Oficina Asesora de Planeación de la Veeduría Distrital: Responsable de asesorar en la aplicación de la herramienta para la administración de los riesgos de seguridad digital.

Equipo de Control Interno: Responsable de hacer seguimiento al cumplimiento de la Política de Seguridad Digital en la Entidad.

6.2 POLÍTICA DE SEGURIDAD DIGITAL INSTITUCIONAL

La Viceveeduría Distrital establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, liderada por el El Equipo de Gestión TIC.

La Oficina Asesora de Planeación, el Equipo de Gestión Documental y El Equipo de Gestión TIC, revisará y actualizará los activos de información y en ello tendrá en cuenta la clasificación según su naturaleza, como por ejemplo, información, software, hardware y/o componentes de red.

El Equipo de Gestión TIC, hará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

El Equipo de Gestión TIC, actualizará los riesgos de seguridad digital, siguiendo la metodología dispuesta por el DAFP y el Ministerio de TIC.

El Equipo de Gestión TIC implementará el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital.

El Equipo de Gestión TIC establecerá los controles definidos en el Anexo A de la ISO 27001:2013, que en el MSPI se define como la Declaración de Aplicabilidad.

El Equipo de Gestión TIC evaluará el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, a través de la aplicación de la política de seguridad y privacidad de la información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

El Equipo de Gestión TIC desarrollará el Procedimiento de Gestión de Incidentes de Seguridad de la Información y en él se establecerá como actividad el reporte de los incidentes a las autoridades como el CSIRT o COLCERT.

El Equipo de Talento Humano, brindará capacitación técnica, tecnológica para atender riesgos de seguridad digital y fortalecerá la capacidad humana.

El Equipo de Gestión TIC sensibilizará a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la Entidad.

7. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

La Veeduría Distrital realizará seguimiento a través de las tres líneas de defensa definidas en el MIPG en la dimensión 7, control Interno mediante el componente de actividades de control.

La Veeduría Distrital realizará seguimiento al avance de la política, a través de la definición de indicadores en el Plan Estratégico de TI –PETI- y en el Plan de Seguridad y Privacidad de la Información.

Se realizará el seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, con la herramienta dispuesta por el Ministerio de Tecnologías y Comunicaciones.

La medición de la política se realizará a través del reporte de la herramienta en línea dispuesta por el DAFP, FURAG.

Elaboró	Reviso	Aprobó
Angela María Restrepo Profesional Especializado **Andrea E. Escalante** Profesional Universitario	**Daniel Andrés García Cañón** Viceveedor Distrital	**Jairo Tirado Martínez** Jefe de la Oficina Asesora de Planeación