OBJETIVO

Diseñar la Política de Seguridad Digital en la Entidad descentralizada Distriseguridad, 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.

ALCANCE

Es aplicable a todos los Empleados de Distriseguridad (Directores, Funcionarios y Contratistas) que actúan en representación (legal o fáctica) de la Entidad en relaciones contractuales con Particulares, Servidores Públicos, Contratistas o cualquier tercero.

OBJETIVOS ESPECIFICOS

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 Entidad descentralizada Distriseguridad.

Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en Distriseguridad 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.

DEFINICIONES:

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

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).

MARCO DE REFERENCIA

NORMA	DESCRIPCIÓN
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.
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.
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.
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

POLÍTICA

La Entidad descentralizada Distriseguridad 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.

APLICABILIDAD

La política de Seguridad Digital será aplicable a todos los servidores y Contratistas de Distriseguridad, con un enfoque pedagógico y preventivo, que sirva de guía de cómo deben ser y obrar los servidores públicos, por el hecho mismo de servir a la ciudadanía. La responsabilidad de los servidores públicos y demás colaboradores es llevar a cabo las directrices planteadas en esta política, dando a conocer la aplicación e implementación de los valores institucionales aquí definidos. Es un compromiso y responsabilidad de todos conocer la Política y es su deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta.

NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% a la política. La política será objeto de evaluación aplicando mecanismos de mejoramiento continuo que involucren participación, compromiso, cooperación, adaptación e inversión. La Política de Seguridad Digital de Distriseguridad será de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas, practicantes, proveedores y terceros. La política abarca clientes internos que son las dependencias que componen la estructura de la administración.

ESTRATEGIAS A IMPLEMENTAR

A continuación se presentan las estrategias a implementar para dar cumplimiento a esta política:

La Seguridad Digital establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, liderada por 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.

COMUNICACIÓN

La divulgación de la Política se realizará a través de todos los canales institucionales como son página web, correo electrónico y socialización. De igual forma y transmitida e implementada en las diferentes dependencias que conforman la estructura organizacional y jerarquía de la Entidad.

EVALUACION Y SEGUIMIENTO

Es necesario realizar seguimiento a las gestiones, planes y programas adelantados para la divulgación e interiorización de los valores, principios, políticas y directrices contenidos en la Política de Seguridad Digital.

La Entidad descentralizada Distriseguridad 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 Entidad descentralizada Distriseguridad 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.

RESPONSABILIDADES

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

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

Oficina Asesora de Planeación de de Distriseguridad 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.

RECOMENDACIONES

Implementar la política de Seguridad Digital con el fin de generar resultados que atiendan planes de desarrollo, garanticen derechos, resuelvan necesidades y problemas de los ciudadanos con calidad.
Es necesario que todos los funcionarios de esta entidad puedan entender la importancia de su labor en función de los propósitos misionales de la entidad, conozcan y se apropien de las herramientas e instrumentos de la entidad y se genere cultura de Seguridad Digital.

Se requiere implementar pedagogía y acciones orientadoras a la implementación de la Política de Seguridad Digital de manera permanente.

DOCUMENTO DE APROBACIÓN

Esta Política Institucional fue aprobada mediante resolución No.100 del 18 de Noviembre del 2021.

PEDRO RODELO ASFORA
Director General Distriseguridad