1. OBJETIVO

Establecer los lineamientos institucionales para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, fortaleciendo la resiliencia y capacidad de respuesta ante incidentes, garantizando la protección de la información, la continuidad operativa y el cumplimiento de la normatividad vigente, en armonía con la Política Nacional de Seguridad Digital (CONPES 3854 de 2016) y el Modelo Integrado de Planeación y Gestión – MIPG.

2. ALCANCE

Esta Política de Seguridad Digital aplica a todas las dependencias, procesos, servidores públicos, contratistas y terceros que utilicen o gestionen información institucional. Abarca la infraestructura tecnológica, plataformas, aplicaciones, redes, servicios en la nube y todos los activos de información físicos o digitales.

3. RESPONSABLES

LÍNEA ESTRATÉGICA: Conformada por la Alta Dirección y el Comité Institucional de Gestión y Desempeño – CIGD. Define los lineamientos, metas y objetivos de la Política de Seguridad Digital; garantiza su articulación con el MIPG vigente, asigna los recursos necesarios, aprueba la política y realiza seguimiento a su implementación, fortaleciendo la gestión institucional y la generación de valor público.

PRIMERA LÍNEA – Gestión Operativa: Integrada por todos los servidores públicos y contratistas que utilizan, administran o gestionan información y activos digitales de la entidad. Son responsables de aplicar la Política de Seguridad Digital en sus actividades diarias, cumpliendo los lineamientos, controles, procedimientos y buenas prácticas establecidas.

El Auxiliar Administrativo – Analista de Sistemas apoya esta línea mediante la orientación técnica, el soporte operativo y el acompañamiento en la implementación de controles de seguridad digital.

SEGUNDA LÍNEA – Supervisión: El Líder de TIC supervisa la implementación de la Política de Seguridad Digital, verificando el cumplimiento de controles, evaluando riesgos tecnológicos y proponiendo acciones correctivas. Garantiza la alineación de la política con la planeación institucional y el MIPG, promoviendo la mejora continua y la protección de los activos de información.

TERCERA LÍNEA – Aseguramiento Independiente: El Jefe de Control Interno y el Comité Coordinador de Control Interno (CCCI) evalúan de forma independiente la eficacia, cumplimiento y madurez de la Política de Seguridad Digital. Identifican riesgos, debilidades y oportunidades de mejora, y emiten recomendaciones a la Alta Dirección para fortalecer la transparencia, legalidad, protección de la información y sostenibilidad del sistema de seguridad digital, contribuyendo a la mejora continua y a la alineación con el MIPG.

4. DEFINICIONES

ACTIVO DE INFORMACIÓN: Recurso que contiene información que la entidad pública genera, obtiene, adquiere, transforma o controla, incluyendo datos, documentos, sistemas, aplicaciones y cualquier soporte físico o digital.

AMENAZA: Causa potencial de un incidente no deseado que puede afectar la confidencialidad, integridad o disponibilidad de los activos de información. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: Proceso para identificar, evaluar y comprender los riesgos sobre los activos de información y determinar su nivel, con el fin de definir controles adecuados. (ISO/IEC 27000).

ARQUITECTURA: Marco de referencia conceptual que aplica el enfoque de Arquitectura Empresarial para fortalecer las capacidades institucionales y de gestión de TI, según el Marco de Referencia de Arquitectura Empresarial del Estado.

CIBERSEGURIDAD: Conjunto de medidas técnicas y administrativas destinadas a proteger sistemas informáticos y redes frente a accesos no autorizados, ataques o incidentes.

INCIDENTE DE SEGURIDAD DIGITAL: Evento que compromete la confidencialidad, integridad o disponibilidad de la información, los sistemas o los servicios digitales.

LINEAMIENTOS: Directrices establecidas por el Ministerio TIC para la implementación de la Política de Gobierno Digital, incluyendo estándares, guías, buenas prácticas y recomendaciones.

RIESGO DE SEGURIDAD DIGITAL: Probabilidad de que una amenaza explote una vulnerabilidad, afectando los activos de información o servicios digitales.

SEGURIDAD DIGITAL: Conjunto de acciones, medidas y controles destinados a proteger la información, los servicios digitales y la infraestructura tecnológica frente a riesgos y amenazas.

SEGURIDAD DE LA INFORMACIÓN: Habilitador de la Política de Gobierno Digital que asegura la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información y de los datos personales, incorporando controles según el Modelo de Seguridad y Privacidad de la Información (MSPI).

SGSI: (Sistema de Gestión de Seguridad de la Información): Sistema institucional de gestión basado en la NTC ISO 27001, destinado a implementar, mantener y mejorar la seguridad de la información.

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el MinTIC y se basa en los requisitos y controles definidos en la Norma NTC ISO 27001.

OTSI: (Oficina de Tecnología y Sistemas de Información): Unidad responsable de la gestión, operación y mantenimiento de los sistemas y servicios tecnológicos de la entidad.

MINTIC: (Ministerio de Tecnologías de la Información y las Comunicaciones): Entidad gubernamental encargada de formular y coordinar la política de tecnologías de la información, comunicación y seguridad digital en Colombia.

1. MARCO NORMATIVO

NORMATIVIDAD	DESCRIPCIÓN
Conpes 3854 de 2016	Política Nacional de Seguridad Digital.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC.
Ley 1712 de 2014	Transparencia y acceso a la información pública.
Ley 1581 de 2012	Protección de datos personales.
Ley 1273 de 2009	Delitos informáticos.
Ley 1928 de 2018	Convenio de Budapest (ciberdelitos).
Acuerdo 02 de 2018	Gobierno Digital.
Acuerdo 08 de 2019	Seguridad Digital en entidades públicas.
Artículo 39 de la Ley 489 de 1998	Ámbito de la administración pública.

2. DESARROLLO

6.1 DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL.

"La EDESO se compromete a proteger la información y los recursos tecnológicos, garantizando su confidencialidad, integridad y disponibilidad, mediante medidas que prevengan, detecten y respondan a riesgos digitales.

Promueve una cultura de seguridad y el uso responsable de tecnologías, salvaguardando la privacidad de los datos y la continuidad de los procesos en todas las áreas de la Entidad".

6.2 POLÍTICA DE SEGURIDAD DIGITAL.

La Política Nacional de Seguridad Digital, establecida en el Documento CONPES 3854 de 2016 y coordinada por la Presidencia de la República, tiene como propósito orientar y proporcionar lineamientos claros a las entidades públicas.

Esta política busca fortalecer las capacidades de las distintas partes interesadas para identificar, gestionar, tratar y mitigar los riesgos asociados al entorno digital en sus actividades socioeconómicas. Además, promueve la creación e implementación de mecanismos de resiliencia, recuperación y respuesta frente a incidentes de seguridad digital, dentro de un marco de cooperación, colaboración y asistencia entre las entidades.

El objetivo final es contribuir al crecimiento de la economía digital nacional, fomentando la innovación tecnológica y garantizando la seguridad de la información, lo que a su vez impulsa la prosperidad económica y social del país.

6.3 LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL.

La Política de Seguridad Digital constituye un pilar fundamental para garantizar la protección de la información y la infraestructura tecnológica en las entidades públicas y privadas, en cumplimiento de los lineamientos establecidos por el CONPES 3854 de 2016, el Decreto 1078 de 2015 y las directrices del Ministerio TIC.

Su implementación busca fortalecer la confidencialidad, integridad y disponibilidad de los datos, reducir riesgos asociados al entorno digital y asegurar la continuidad de los procesos misionales y administrativos.

Los presentes Lineamientos para la Implementación de la Política de Seguridad Digital definen las acciones, responsabilidades y mecanismos de articulación necesarios para garantizar una gestión integral de riesgos, promover una cultura de seguridad y cumplir con los estándares nacionales, integrando el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) y el Plan de Acción de Seguimiento (PAS).

Gobernanza y Responsabilidades: El Comité Institucional de Gestión y Desempeño será la instancia encargada de articular esfuerzos, recursos y metodologías para la implementación de la política.

Se designará un Responsable de Seguridad Digital, quien también asumirá la función de Seguridad de la Información, con dependencia directa de la Alta Dirección.

Las responsabilidades frente a la seguridad de la información serán definidas, publicadas y aceptadas por funcionarios, contratistas, proveedores y terceros.

Integración Normativa y Modelos: Alinear la política con el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) del MinTIC y el Plan de Acción de Seguimiento (PAS) del CONPES 3854.

Emitir resoluciones y actos administrativos internos que regulen el entorno digital y fortalezcan la gestión de riesgos.

Protección de la Información y Activos: Garantizar la seguridad como un activo primordial en el ciclo de vida de los sistemas de información; establecer lineamientos para asegurar la integridad de la información histórica, generada, transmitida o resguardada; implementar controles para el análisis de información externa, utilizando herramientas de detección de amenazas (antivirus, filtros).

Uso Responsable de Recursos TIC: Prohibir el acceso a sitios no autorizados (pornografía, juegos, redes sociales no permitidas) desde la infraestructura institucional; restringir el uso de dispositivos extraíbles para compartir información, promoviendo plataformas colaborativas seguras; establecer parámetros para contraseñas seguras y autenticación en equipos, redes y sistemas.

Seguridad Física y Control de Accesos: Garantizar el uso de elementos de identificación y protocolos de acceso físico y lógico para evitar el ingreso no autorizado; informar oportunamente a Tics sobre cualquier vulnerabilidad o incumplimiento detectado.

Capacitación y Cultura Digital: Generar espacios de formación para líderes y personal, orientados a la prevención, detección y respuesta ante riesgos digitales; incluir contenidos de seguridad digital en procesos de inducción y reinducción.

Plan de Contingencia y Continuidad: Definir y mantener actualizado un plan de contingencia para la materialización de riesgos identificados; asegurar el respaldo y recuperación de la información crítica para minimizar impactos financieros, operativos y legales.

6.4 IMPLEMENTAR LAS ACCIONES PARA LA POLÍTICA DE SEGURIDAD DIGITAL.

La implementación de la Política se desarrollará conforme a los lineamientos, guías y principios del Manual Operativo del MIPG vigente, así como a los planes de acción y mejora definidos por la entidad y aprobados por el Comité Institucional de Gestión y Desempeño de la EDESO.

Para garantizar su efectividad, la EDESO integrará esta política con los siguientes instrumentos institucionales:

- ✓ Plan Estratégico de Tecnologías de la Información (PETI)
- ✓ Modelo de Seguridad y Privacidad de la Información (MSPI)

Esta fase comprende la ejecución de las acciones planificadas, orientadas a:

- ✓ Corregir las debilidades identificadas en el diagnóstico inicial.
- ✓ Fortalecer los controles y procesos críticos relacionados con la seguridad digital.
- ✓ Asegurar la mejora continua en la gestión de riesgos y protección de la información.

La implementación incluirá:

- ✓ Monitoreo permanente del avance de las acciones.
- ✓ Evaluación periódica de resultados en el Comité Institucional de Gestión y Desempeño.

6.5 EVALUAR Y SEGUIMIENTO POLÍTICA SEGURIDAD DIGITAL.

La evaluación de la Política de Seguridad Digital tiene como objetivo dar seguimiento a las acciones implementadas, medir su impacto, eficacia y contribución al fortalecimiento institucional, asegurando la mejora continua.

El seguimiento estará a cargo de la Subgerencia Administrativa y Financiera, con el apoyo del Auxiliar Administrativo – Analista de Sistemas, quienes verificarán el cumplimiento de las actividades y evaluarán los resultados frente a los objetivos establecidos.

La evaluación se fundamenta en:

- ✓ Autodiagnóstico de la Gestión Estratégica del Talento Humano (GETH).
- ✓ Formulario Único de Reporte y Avance de Gestión (FURAG) para monitoreo y control del desempeño institucional.
- ✓ Plan de Acción (PETI).

Se elaborará un informe anual de desempeño, que será presentado al Comité Institucional de Gestión y Desempeño, garantizando transparencia y rendición de cuentas.

Instrumentos de planeación y seguimiento:

- ✓ Plan Estratégico de Tecnologías de la Información (PETI).
- ✓ Modelo de Seguridad y Privacidad de la Información (MSPI).

Estos instrumentos permiten una gestión basada en evidencia, orientada a resultados y alineada con los principios del MIPG, fortaleciendo la implementación de la Política de Seguridad Digital y la generación de valor público.

6.6 APROBACIÓN EN EL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO.

La Política de Seguridad Digital será aprobada por el Comité Institucional de Gestión y Desempeño, garantizando su alineación con los objetivos estratégicos, la normativa vigente y los principios del MIPG.

Se realizará una revisión anual de sus lineamientos, o antes si se presentan cambios normativos, tecnológicos o de riesgos, para asegurar su pertinencia, vigencia y coherencia con los estándares nacionales y las necesidades institucionales.

6.7 DIVULGACIÓN Y SENSIBILIZACIÓN.

Para asegurar la apropiación y aplicación efectiva de la Política de Seguridad Digital por parte de todos los servidores públicos y contratistas, se implementarán acciones de divulgación y sensibilización mediante los siguientes canales:

- ✓ Página web institucional (publicación oficial y acceso público).
- ✓ Correo electrónico corporativo (circulares y boletines informativos).
- ✓ Grupos oficiales de mensajería (WhatsApp u otros autorizados).
- ✓ Reuniones informativas, carteleras y medios digitales internos.
- ✓ Procesos de inducción y reinducción, integrando la política en la formación inicial y continua.

Estas acciones buscan garantizar que la política sea conocida, comprendida y aplicada correctamente, fomentando una cultura de seguridad digital en toda la entidad.

7. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA DE APROBACIÓN
01	Creación del documento de la Política Seguridad Digital alineada al Manual Operativo MIPG Versión 6	30/12/2025

….

8. CONTROL DE FORMALIZACIÓN

ELABORÓ	REVISÓ	APROBÓ
Auxiliar Administrativo Analista de sistemas	Subgerente Administrativo y Financiero	Comité Institucional de Gestión y Desempeño
FECHA: 15/12/2025	FECHA: 22/12/2025	FECHA: 30/12/2025