**GESTIÓN ESTRATEGICA DE TECNOLOGÍA**

# DOCUMENTO TÉCNICO POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**GEST-DT-04**

**V.1**

**2026-07-29**

**Unidad Administrativa Especial de Catastro Distrital -UAECD-**
AV. Carrera 30 N0. 25 90, Torre B Piso 2
+57 (601) 2347600
Código postal: 111311

# TABLA DE CONTENIDO



**ÍNDICE DE TABLAS**

## 1. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección de la Unidad Administrativa Especial de Catastro Distrital, en adelante la UAECD para la seguridad y privacidad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

## 2. DESARROLLO

### 2.1. DEFINICIONES/GLOSARIO

- **Acceso Lógico:** Restricción de acceso a los datos mediante técnicas de ciberseguridad como identificación, autenticación y autorización, incluyendo control de privilegios, gestión de contraseñas, autenticación multifactor y principio de mínimo privilegio.
- **Activo De Información:** Conocimiento o información que tiene valor para la organización.
- **Activo Crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura critica.
- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Ciberseguridad:** El conjunto de actividades y procesos cuyo propósito es proteger los activos de información, los sistemas de información, los activos de la red, los programas y la infraestructura en el ciberespacio, por medio del tratamiento de las amenazas a la información que es procesada, almacenada o transportada a través de sistemas de información interconectados.
- **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Criptografía:** Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
- **CSIRT:** Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)

- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **SGSPI Sistema de Gestión de Seguridad y Privacidad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

Estas definiciones han sido tomadas principalmente de:

- Glosario de la ISO27000
- Consejo Nacional de política y economía social

## 2.2. INTRODUCCIÓN

La Unidad Administrativa Especial de Catastro Distrital (UAECD), en el desarrollo de su misión, recolecta, procesa, modifica, almacena y transfiere información en formatos físico y digital. Esta información constituye un activo fundamental para la UAECD y proviene de diversas fuentes, tales como funcionarios, contratistas, proveedores, así como entidades públicas y privadas ciudadanos y propietarios; esta información es recolectada y tratada conforme a los lineamientos establecidos en la normatividad vigente y en la Política y gestión de datos personales. Por lo anterior, su gestión requiere un manejo responsable y seguro que permita hacer un buen uso de esta y mitigar los riesgos sobre su confidencialidad, disponibilidad e integridad.

Para lograr este propósito, la UAECD mantiene un Sistema de Gestión de Seguridad de la Información (SGSI), entendido como un conjunto integrado de controles, políticas, procesos, procedimientos, estructuras organizacionales y componentes de software y hardware. Dicho sistema abarca desde la identificación de los activos de información y el análisis de riesgos, hasta el establecimiento, implementación y seguimiento continuo de los controles y su efectividad. Por esta razón, el SGSI ha sido incorporado al Sistema Integrado de Gestión de la Unidad.

Alineada con la política de Gobierno Digital y con el estándar internacional ISO 27001:2022 —norma emitida por la Organización Internacional de Normalización que describe cómo gestionar la seguridad de la información en una organización—, la UAECD determina que la implementación de su SGSI se realice en el marco de dicha norma. Sobre esta base se desarrolla la Política de Seguridad y Privacidad de la Información.

La Política de Seguridad y Privacidad de la Información constituye la declaración formal mediante la cual la UAECD establece su compromiso y enfoque respecto a la gestión de la seguridad y privacidad de la información. En ella se indican las responsabilidades y la conducta aceptada para funcionarios,

contratistas, proveedores y terceros que, debido al cumplimiento de sus funciones u obligaciones, tengan acceso a la información de la Entidad.

Adicionalmente, la UAECD se compromete con la gobernanza de la seguridad digital conforme al Decreto 338 de 2022. Para ello, identifica sus activos como Infraestructura Crítica Cibernética (ICC) cuando corresponde, y se vincula al CSIRT Distrital y al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) para la gestión de incidentes de seguridad digital.

En consecuencia, se adopta la presente Política de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Catastro Distrital (UAECD).

### 2.3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La **UAECD**, entendiendo la importancia de sus activos de información y la importancia de la seguridad de la información como actividad estratégica para el cumplimiento de su misión institucional, se ha comprometido a mantener un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) buscando proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

### 2.4. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

La **UAECD** en su propósito de dar cumplimiento a la Política de Seguridad y Privacidad de la Información, establece los objetivos del sistema, los cuales se detallan en el Documento Técnico Manual del Sistema de Gestión Integral de la **UAECD**.

### 2.5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la **UAECD** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI); así mismo, se compromete a revisar el avance de la implementación del SGSPI, con una periodicidad mínima anual o cuando se considere pertinente y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información y continuidad de negocio.

## 2.6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos aplica a:

- Todas las personas vinculadas con la UAECD, funcionarios, contratistas, personal que labora en las instalaciones vinculado con un proveedor de la Unidad, los stakeholders (o grupos de interés) y ciudadanía en general;
- Todos los recursos y activos de información de la Unidad;
- Todos los procesos y procedimientos de la Unidad;
- Toda la infraestructura tecnológica y sistemas de información que soportan la misionalidad de la Entidad;
- Todas las sedes físicas de la Unidad.

El detalle del alcance se describe en el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 2.7. PRINCIPIOS

Los siguientes principios de seguridad de la información soportan el SGSI:

a. **Gestión continua del SGSI:** La UAECD ha decidido definir, implementar, operar y mejorar de forma continua el Subsistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a sus necesidades y a los requerimientos regulatorios que le aplican a su naturaleza, mediante la formulación de procedimientos, controles y políticas de seguridad que deben ser adoptados por funcionarios, contratistas y terceros.
b. **Responsabilidad universal:** La responsabilidad frente a la seguridad de la información es de todos los funcionarios, contratistas, personal que labora en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad) con el fin de minimizar impactos financieros, operativos o legales por uso incorrecto, alteración o borrado no autorizado de la información.
c. **Controles de acceso**: La UAECD protegerá la información generada, transmitida, procesada o resguardada por los procesos de la Unidad, su infraestructura tecnológica y sus activos, del riesgo que se genera por los accesos otorgados a funcionarios, contratistas y terceros (ej.: proveedores, entidades externas), o como resultado de un servicio de la UAECD suministrado a través de uno de sus proveedores, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, su alteración o borrado no autorizados.
d. **Protección de infraestructura:** La UAECD velará por la protección de las instalaciones de procesamiento de información (centro de cómputo, centro alterno e infraestructura en la nube) y de los recursos tecnológicos que soportan sus procesos críticos.
e. **Control de operaciones:** La UAECD controlará la operación de sus procesos, garantizando la

seguridad de la información en cada uno de ellos.

f. **Continuidad operacional:** La UAECD garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos que afecten su seguridad.
g. **Seguridad en el ciclo de vida del software:** La UAECD garantizará que la seguridad sea parte integral del ciclo de vida de sus soluciones de software.
h. **Gestión de riesgos:** El Comité Institucional de Gestión y Desempeño aprobará las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información y continuidad del negocio
i. **Inteligencia artificial (IA)**: La UAECD establecerá los requisitos obligatorios de seguridad de la información, privacidad, ciberseguridad y ética que rigen el ciclo de vida completo (adquisición, desarrollo, entrenamiento, implementación, operación y disposición) de cualquier sistema de IA
j. **Seguridad por defecto y por diseño:** La UAECD incorporará medidas de seguridad desde el diseño y por defecto en el desarrollo, adquisición y operación de sistemas de información, servicios y productos tecnológicos, conforme a la Estrategia Nacional Digital 2023-2026.
k. **Gestión de incidentes y respuesta:** La UAECD establecerá procesos para la detección, reporte, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información, con notificación al ColCERT cuando corresponda, conforme al Decreto 338 de 2022.
l. **Trazabilidad y no repudio:** La UAECD garantizará la trazabilidad de las operaciones sobre activos de información críticos y la capacidad de demostrar la realización de acciones por parte de usuarios identificados.
m. **Protección de datos personales:** La UAECD implementará el principio de responsabilidad demostrada en el tratamiento de datos personales, garantizando los derechos de los titulares conforme a la Ley 1581 de 2012 y el SGSPI
n. **Seguridad en la cadena de suministro digital:** La UAECD evaluará y gestionará los riesgos de seguridad asociados a proveedores, contratistas, entidades productoras, consumidoras de información geográfica y terceros que tengan acceso a sus activos de información.

### 2.8. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios para establecer mucho más la aplicabilidad de la política de seguridad de la UAECD se aplica a: funcionarios, contratistas, terceros, proveedores, así como a aquellas personas que en razón del cumplimiento de sus funciones y las de la **UAECD**, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información".

El incumplimiento de la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen según la normativa vigente de la Entidad.

## 2.9. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La **UAECD**, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, procedimientos, formatos entre otros):

| ROL / INSTANCIA / DEPENDENCIA | RESPONSABILIDADES (Deberes respecto a la SEGURIDAD DE LA INFORMACIÓN) |
|---|---|
| **Alta Dirección** | • Proporcionar los recursos necesarios para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (Recursos económicos, talento humano, formación y recursos tecnológicos). |
| **Comité Institucional de Gestión y Desempeño** | • Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información. |
| **Gerencia TI** | • Implementar los controles de tipo tecnológico diseñados para mitigar los riesgos de seguridad de la información. |
| **Subgerencia de Talento Humano** | • Asegurar que se cumplan los espacios de capacitaciones, inducciones y charlas a los colaboradores en seguridad de la información además de validar la firma de compromisos de confidencialidad para el manejo y buen uso de la información y la tecnología de la UAECD de acuerdo con las políticas y procedimientos establecidos.<br>• Realizar la gestión integral del talento humano con el enfoque y cumplimiento de las políticas de seguridad. |
| **Oficina de Control Interno** | • Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.<br>• Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información, en el acompañamiento, identificación de la causa, las implicaciones y la introducción de los correctivos necesarios para el cumplimiento de las metas y objetivos propuestos. |
| **Comunicaciones** | • Apoyar en las labores de comunicación y sensibilización en seguridad de la información, en todos los niveles de la entidad. |
| **Subgerencia de Contratación** | • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad.<br>• Procurar la protección de todos los activos de la información que puedan verse involucrados en procesos o contratos. |

| ROL / INSTANCIA / DEPENDENCIA | RESPONSABILIDADES (Deberes respecto a la SEGURIDAD DE LA INFORMACIÓN) |
|---|---|
| **Oficina Asesora de Planeación y aseguramiento de procesos** | • Direccionar la formulación, ejecución, seguimiento y actualización de la planeación institucional a nivel estratégico, táctico y operativo. |
| **Gerencia Jurídica** | • Proveer apoyo integral a la UAECD mediante la atención de las actuaciones administrativas, la asesoría en asuntos normativos y el ejercicio de la defensa judicial y extrajudicial, contribuyendo a la adecuada toma de decisiones y a la prevención del daño antijurídico, en los términos y condiciones legales aplicables. Lo anterior, incorporando de manera transversal criterios de seguridad y privacidad de la información, garantizando la protección, confidencialidad, integridad y disponibilidad de los datos gestionados, conforme a la normativa vigente en materia de protección de datos personales y seguridad de la información. |
| **Oficina de control disciplinario interno** | • Desarrollar la gestión disciplinaria cumpliendo los principios constitucionales y legales del debido proceso, garantizando la confidencialidad, seguridad y privacidad de la información y los datos personales involucrados. |
| **Subgerencia Administrativa y Financiera** | • Administrar los recursos financieros y proveer información presupuestal, contable y de tesorería para apoyar el cumplimiento de la misión de la UAECD.<br>• Administrar la gestión documental de la UAECD mediante la creación y actualización de políticas, planes, programas e instrumentos archivísticos. |
| **Líderes de Proceso** | • Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (por ejemplo: gestión de activos, gestión de riesgos, entre otros).<br>• Incentivar que los colaboradores participen en la transferencia de conocimiento y en las actividades que se propongan para la seguridad de la información. |
| **Todos los colaboradores.** | • Apoyar a los líderes de proceso en el desarrollo de tareas como la gestión de activos y la gestión de riesgos.<br>• Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.<br>• Participar activamente en los programas de transferencia de |

| ROL / INSTANCIA / DEPENDENCIA | RESPONSABILIDADES (Deberes respecto a la SEGURIDAD DE LA INFORMACIÓN) |
|---|---|
| | conocimiento y en las actividades de seguridad de la información. |
| **Oficial de Seguridad de la información** | • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidos y aprobados por la Entidad.<br>• Apoyar en la generación de los lineamientos (manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad. |
| **Oficial de continuidad del negocio** | • Liderar la implementación, mantenimiento y mejora del modelo de continuidad del negocio, asegurando la resiliencia de los procesos críticos de la organización |
| **Oficial de Protección de Datos Personales (OPD)** | • Es la persona encargada de velar por el cumplimiento de los deberes consagrados en la Ley 1581 de 2012 y las normas relacionadas con la privacidad y garantizar la protección de la información que reposa en las bases de datos de la UAECD.<br>• Fomentar una cultura de protección de datos, gestionar y dar trámite a las consultas, quejas y solicitudes relacionadas con los datos personales en las bases de datos de la UAECD y actuar como el punto de contacto oficial con la Superintendencia de Industria y Comercio. |

*Tabla 1: Roles y Responsabilidades*

Para mayor detalle de los roles y responsabilidades consultar el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN en el cual se Encuentra en el sistema de gestión de calidad de la UAECD.

### 2.10. POLITICAS Y CONTROLES

La **UAECD,** de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Norma ISO 27001:2022, establece el “Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información”, en el cual se encuentran los lineamientos detallados para el cumplimiento de la implementación y monitoreo del Sistema de Gestión de Seguridad y Privacidad de la Información.

## 2.11. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Todos los líderes de proceso de la UAECD, acompañados por el Oficial de Seguridad de la Información, deben realizar la identificación, clasificación y tratamiento de los riesgos de seguridad digital, que puedan comprometer las operaciones de la UAECD y amenazar la seguridad de la información de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad.

La UAECD gestionará los riesgos de seguridad de la información basándose en la identificación de activos de información con criticidad alta y aquellos identificados como Infraestructura Crítica Cibernética (ICC).

El reporte, gestión y conservación de las evidencias de los controles definidos para la mitigación de los riesgos será responsabilidad de cada dependencia como parte de la operación de sus procesos, quienes deberán garantizar la trazabilidad, integridad y disponibilidad de los soportes, manteniéndolos en repositorios definidos y entregándolos oportunamente cuando sean requeridos para auditorías, seguimientos o instancias de control.

Para los riesgos de seguridad de la información, las evidencias deberán gestionarse y reportarse atendiendo los lineamientos definidos por la Gerencia de Tecnología y el Oficial de Seguridad de la Información, en concordancia con el modelo de seguridad y privacidad de la información, garantizando la protección, confidencialidad, integridad y disponibilidad de los activos de información asociados.

## 2.12. SOPORTE LEGAL

El SGSPI de la **UAECD** se encuentra soportado en el siguiente marco normativo:

- **Constitución Política de Colombia (Artículo 15):** se establece que *"todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar"*
- **Ley 1273 de 2009**: crea un nuevo bien jurídico tutelado denominado "*De la protección de la información y los datos*", preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **Ley Estatutaria 1581 de 2012**: por la cual se dictan disposiciones generales para la protección de datos personales, tiene como objeto *"(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales*", estableciendo, además, las disposiciones generales para la protección de datos personales.

- **La Ley Estatutaria 1712 de 2014:** de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, define en su Artículo 1, que "el objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.".
- **Decreto Nacional 2573 de 2014:** establece los lineamientos generales de Gobierno en Línea e incorpora los requerimientos de la Ley 1581 de 2012 para la protección de datos personales y se diseñan en el marco de referencia a la norma ISO 27001 en cada uno de sus dominios.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes, el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

- **Decreto Único Reglamentario 1081 de 2015:** Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
- 
- **CONPES 3854 de 2016:** el cual contiene la "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL" se establecen los lineamientos y directrices de seguridad digital, incluyendo componentes tales como la gobernanza, educación, la regulación, la cooperación internacional y nacional, la investigación, el desarrollo y la innovación.
- **CONPES 3995 de 2020**: el cual contiene la "POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL" formula una política nacional que tiene como objetivo, establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.
- **Decreto Nacional 1008 de 2018**[1]: establece el habilitador transversal de seguridad de la información como elemento fundamental para el logro de los propósitos de esta.
- **Decreto 338 de 2022:** Por el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.
- **CONPES 4144 de 2025**: Política Nacional de Inteligencia Artificial, que establece lineamientos para el desarrollo, implementación y supervisión de sistemas de IA en Colombia.
- **Lineamientos de Seguridad y Privacidad de la Información para Sistemas de IA (MinTIC, 2026):** Directrices técnicas, organizativas y normativas para el diseño, desarrollo, implementación, operación y mantenimiento de sistemas de IA en entidades públicas.

[1] Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 9 de la parte 2 del libro del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012 en materia de protección de datos personales.
- **Resolución 500 de 2021 del MinTIC:** Por la cual se adopta el Marco de Interoperabilidad para Gobierno Digital (MIGD).
- **Resolución 2277 de 2025:** Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- Resolución 02277 de 2025: Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia
- **Decreto 767 de 2022:** Por el cual se reglamenta el artículo 148 de la Ley 1955 de 2019 sobre transformación digital pública.

### 2.13. SANCIONES

El incumplimiento de la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados por parte de los servidores públicos de la UAECD puede conllevar la adopción de las acciones disciplinarias, penales y/o administrativas según el caso. Asimismo, el incumplimiento de esta política por parte de los aprendices, practicantes, contratistas, proveedores, visitantes, organizaciones y miembros del público que accedan a información de la UAECD o utilicen los servicios de información proporcionados por la misma, puede generar la suspensión de los servicios, así como el inicio de las acciones administrativas, penales, contractuales y/o legales a que haya lugar.

### 2.14.SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

La **UAECD** realizará revisiones periódicas al SGSPI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por la herramienta definida para tal fin.

### 2.15.APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Alta Dirección/Comité institucional de gestión de desempeño. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la UAECD (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

## 3. DOCUMENTOS REFERENCIA

A continuación, se relacionan los documentos externos que se toman como de consulta y que pueden facilitar el entendimiento del presente documento:

- Documento Maestro de Lineamientos del MSPI (MinTIC, 2025).
- Lineamientos de Seguridad y Privacidad de la Información para Sistemas de IA (MinTIC, 2026).
- Decreto 338 de 2022, fortalecer la gestión de los riesgos de seguridad digital para los servicios esenciales e infraestructuras criticas cibernéticas.
- CONPES 4144 de 2025, establece la Política Nacional de Inteligencia Artificial (IA) en Colombia, con el fin de guiar el desarrollo, adopción y uso ético de esta tecnología entre 2025 y 2036.
- Estrategia Nacional Digital 2023-2026, es la hoja de ruta del Gobierno Nacional, coordinada por el MinTIC y el DNP, diseñada para convertir al país en una sociedad digital.
- Norma técnica colombiana NTC-ISO-IEC COLOMBIANA 27001 versión 2022. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
- Norma técnica colombiana NTC-ISO-IEC COLOMBIANA 27002 versión 2022. Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.
- Norma técnica colombiana NTC-ISO-IEC COLOMBIANA 27000 versión 2017. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.
- Guía técnica GTC-ISO/IEC COLOMBIANA 27003 versión 2017. Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de seguridad de la información.
- Modelo de seguridad y privacidad de la información – MSPI, del Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC.
- Guía N° 2 Elaboración de la política general de seguridad y privacidad de la información, del Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC versión 5.0.0 del 2025.
- Documentación del Modelo de Seguridad y Privacidad de la Información – MSPI – MINTIC. V5 2025.
- DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Definir y disponer para conocimiento y cumplimiento de todos los funcionarios, contratistas y terceros que acceden a los activos de información de la Unidad, los lineamientos y directrices del Modelo de Seguridad y Privacidad de la Información en la UAECD.