1. OBJETIVO

Establecer los lineamientos para la protección de la información de la UPME, garantizando la confidencialidad, integridad y disponibilidad de los activos de información. Esta política se fundamenta en el Modelo de Seguridad y Privacidad de la Información (MSPI) el cuál se encuentra regulado según la Resolución 02277 de 2025 y su anexo y la ISO/IEC 27001:2022; asegurando el cumplimiento normativo y la mitigación de riesgos de seguridad digital.

1.2. OBJETIVO ESPECÍFICOS

- Fortalecer la gobernanza y la eficacia del SGSI con su cumplimiento normativo.
- Asegurar la resiliencia y continuidad de la seguridad de la información.
- Promover una cultura de seguridad y privacidad de la información.
- Fortalecer la gestión y tratamiento de riesgos de seguridad de la información.

2. ALCANCE

La presente política define el marco de referencia para la gestión de la seguridad y privacidad de la información de la UPME, asegurando su implementación en todos los niveles de la organización. Se orienta a proteger la información, minimizar riesgos y garantizar la continuidad de las operaciones mediante la implementación de controles de ciberseguridad, seguridad y privacidad de la información. Se aplica a todas las actividades donde la información sea creada, procesada, almacenada o compartida, asegurando que los controles de seguridad sean adecuados y alineados con los principios de confidencialidad, integridad y disponibilidad.

Esta política aplica a:

- Todos los funcionarios, contratistas y proveedores que manejen información de la UPME.
- Toda la información generada, procesada, almacenada y transmitida en el marco de las funciones de la UPME.
- Infraestructura tecnológica y plataformas digitales utilizadas en la gestión de la información institucional.

3. GLOSARIO

Activo de Información: Cualquier dato, sistema, proceso o infraestructura tecnológica que tenga valor para la UPME. (Fuente: ISO/IEC 27001:2022)

Confidencialidad: Propiedad que garantiza que la información solo sea accesible para quienes estén autorizados. (Fuente: ISO/IEC 27001:2022)

Disponibilidad: Garantía de que la información esté accesible y utilizable cuando sea requerida por usuarios autorizados. (Fuente: ISO/IEC 27001:2022)

Incidente de Seguridad de la Información: Evento que puede comprometer la seguridad de la información y afectar la confidencialidad, integridad o disponibilidad de los activos de información. (Fuente: ISO/IEC 27001:2022)

Integridad: Propiedad de la información que asegura su exactitud y completitud. (Fuente: ISO/IEC 27001:2022)

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad, causando impacto en la organización. (Fuente: ISO/IEC 27001:2022)

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de políticas, procedimientos y controles implementados para gestionar la seguridad de la información en la organización. (Fuente: ISO/IEC 27001:2022)

4. RESPONSABILIDADES

Alta Dirección: Liderar la implementación del SGSI y asegurar su integración con la estrategia organizacional.

Oficial de Seguridad de la Información: Coordinar la gestión de seguridad, supervisar el cumplimiento y hacer seguimiento a la aplicación de controles de seguridad.

Funcionarios y Contratistas: Cumplir con las políticas de seguridad documentadas en el Manual de Políticas de Seguridad y Privacidad de la Información el cual hace parte integral de este documento, y reportar cualquier incidente asociado.

Administradores de TI: Implementar y mantener las medidas de seguridad en los sistemas y redes.

Proveedores: Cumplir con los requerimientos de seguridad definidos por la UPME.

5. POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

En la Unidad de Planeación Minero Energética (UPME), la información es un activo estratégico fundamental para la toma de decisiones y la prestación de servicios eficientes. La entidad se compromete con la protección y gestión rigurosa de la información, adhiriéndose a marcos regulatorios y alineándose con las mejores prácticas internacionales en seguridad de la información y ciberseguridad, en cumplimiento de la ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI) el cuál se encuentra regulado según la Resolución 02277 de 2025 y su anexo.

La Alta Dirección, al aprobar esta Política, reafirma su compromiso con la seguridad de la información y ciberseguridad en la UPME, estableciendo un entorno que garantiza la Confidencialidad, Integridad y Disponibilidad (CID) de los activos de información. Este entorno se fundamenta en la aplicación de medidas preventivas, el análisis de riesgos y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Las directrices clave para la gestión y operación del SGSI en la UPME incluyen:

- Adoptar un enfoque basado en gestión de riesgos, asegurando la identificación, mitigación y monitoreo continuo de amenazas a la seguridad de la información.
- Garantizar la adherencia a los principios de seguridad de la información (CID) en todos los procesos y sistemas de la organización.
- Mantener la imparcialidad y la equidad en todas las actividades relacionadas con la seguridad de la información.
- Fomentar la innovación tecnológica y la resiliencia digital, fortaleciendo la infraestructura de seguridad de la UPME.
- Desarrollar y mantener políticas y procedimientos alineados con los estándares internacionales y regulaciones nacionales.

- Promover una cultura de seguridad y concienciación en ciberseguridad para funcionarios, contratistas y demás partes interesadas.
- Asegurar la continuidad del negocio y la respuesta efectiva a incidentes, implementando planes de contingencia y recuperación ante desastres.

Este compromiso permitirá a la UPME fortalecer su capacidad de prevención y respuesta ante riesgos cibernéticos, garantizando la protección de los activos de información y la confianza de las partes interesadas.

6. REVISIÓN Y MEJORA CONTINUA

El SGSI será revisado y auditado de manera periódica, garantizando su eficacia en la protección de la información. Se realizarán auditorías internas y externas conforme a los lineamientos del MSPI y la ISO/IEC 27001:2022, promoviendo la mejora continua.

La política será revisada anualmente para adaptarse a nuevas regulaciones y posibles amenazas.

Se promoverá la innovación tecnológica en seguridad y protección de la información.

Se evaluará el desempeño del SGSI a través de auditorías y monitoreo de controles.

7. ANEXOS

- Manual de Políticas de Seguridad y Privacidad de la Información.
- Normas de Seguridad de las Tecnologías de Información y las Comunicaciones (TIC)

8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción de los cambios**
14/07/2025	1	Actualización de la política general de seguridad de la información acorde al MSPI Versión 5 y la norma ISO/IEC 27001:2022.

1. INTRODUCCIÓN

La Unidad de Planeación Minero Energética (UPME), consciente del valor estratégico de la información y la necesidad de protegerla frente a amenazas internas y externas, ha establecido este manual como complemento técnico de su Política General de Seguridad y Privacidad de la Información.

Este manual consolida las políticas específicas y las normas operativas necesarias para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) el cuál se encuentra regulado según la Resolución 02277 de 2025 y su anexo; y con la Norma Técnica Colombiana ISO/IEC 27001:2022.

El contenido aquí descrito orienta la gestión de la seguridad de la información en todos los niveles y procesos institucionales, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la UPME. Estas políticas reflejan el compromiso de la Alta Dirección y se articulan con el Sistema Integrado de Gestión de la entidad.

El cumplimiento de este manual es obligatorio para todos los funcionarios, contratistas y terceros que acceden, procesen, transmiten o almacenen información institucional. Asimismo, este documento será revisado anualmente para garantizar su vigencia y pertinencia frente a los cambios en el contexto tecnológico, normativo y de riesgos.

2. OBJETIVO.

El presente manual tiene como objetivo establecer las políticas y normas específicas de seguridad y privacidad de la información diseñadas para la Unidad de Planeación Minero Energética (UPME), con el fin de facilitar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Estas políticas permiten asegurar la confidencialidad, integridad y disponibilidad de la información institucional, así como la gestión adecuada de los riesgos mediante la aplicación de controles alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la Norma ISO/IEC 27001:2022.

2. ALCANCE

El presente manual de políticas y normas de seguridad y privacidad de la información aplica como anexo técnico a la Política General de Seguridad y Privacidad de la Información de la Unidad de Planeación Minero Energética (UPME).

Su contenido abarca la definición, despliegue y gestión de las políticas específicas que soportan el Sistema de Gestión de Seguridad de la Información (SGSI), alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma ISO/IEC 27001:2022.

4. GLOSARIO

Aceptación del riesgo: Decisión de asumir un riesgo sin aplicar medidas adicionales de mitigación. *Fuente: ISO/IEC 27005:2018*

Activo de información: Cualquier cosa que tenga valor para la organización, incluyendo datos, personas, dispositivos, sistemas, servicios e infraestructura. *Fuente: ISO/IEC 27000:2018*

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar su nivel. *Fuente: ISO/IEC 27005:2018*

Autenticidad: Propiedad que asegura que una entidad es quien dice ser. *Fuente: ISO/IEC 27000:2018*

Clasificación de la información: Proceso de asignación de niveles de sensibilidad o criticidad a la información, según su valor y riesgos asociados. *Fuente: MSPI – MinTIC*

Confidencialidad: Propiedad que garantiza que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. *Fuente: ISO/IEC 27000:2018*

Confiabilidad de la información: Cualidad de que la información provenga de una fuente válida y sea útil para la toma de decisiones. *Fuente: MSPI – MinTIC*

Control de seguridad: Medida implementada para modificar o mantener un riesgo dentro de niveles aceptables. *Fuente: ISO/IEC 27000:2018*

Declaración de aplicabilidad (SoA): Documento que justifica los controles seleccionados y excluidos del Anexo A de la ISO/IEC 27001. *Fuente: ISO/IEC 27001:2022*

Disponibilidad: Propiedad que garantiza que la información esté accesible y utilizable por las personas autorizadas cuando se requiera. *Fuente: ISO/IEC 27000:2018*

Evaluación del riesgo: Comparación entre los niveles de riesgo estimados y los criterios establecidos, para determinar su aceptabilidad. *Fuente: ISO/IEC 27005:2018*

Evento de seguridad de la información: Ocurrencia identificada en un sistema o servicio que indica una posible violación de la política o fallo de control. *Fuente: ISO/IEC 27035-1:2016*

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización respecto al riesgo. *Fuente: ISO/IEC 27000:2018, ISO 31000:2018*

Incidente de seguridad de la información: Evento o serie de eventos inesperados o no deseados que comprometen la seguridad de la información. *Fuente: ISO/IEC 27035-1:2016*

Integridad: Propiedad que asegura que la información no ha sido modificada de manera no autorizada y mantiene su exactitud y completitud. *Fuente: ISO/IEC 27000:2018*

Oficial de Seguridad de la Información (OSI): Persona encargada de liderar y coordinar el SGSI en la entidad. *Fuente: MSPI – MinTIC*

Protección contra duplicación: Medida que evita la repetición no autorizada de transacciones o acciones para prevenir fraudes. *Fuente: MSPI – MinTIC*

Recursos informáticos: Infraestructura, hardware, software y redes utilizadas para procesar, almacenar y transmitir información. *Fuente: MSPI – MinTIC*

Riesgo: Efecto de la incertidumbre sobre los objetivos. *Fuente: ISO 31000:2018*

Riesgo inherente: Nivel de riesgo existente en ausencia de controles. *Fuente: ISO/IEC 27005:2018*

Riesgo residual: Nivel de riesgo que permanece después de aplicar controles o tratamientos.
Fuente: ISO/IEC 27005:2018

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. *Fuente: ISO/IEC 27000:2018*

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados que establecen políticas, objetivos y procesos para proteger la información. *Fuente: ISO/IEC 27001:2022*

Sistema de información: Conjunto de elementos organizados para la recolección, procesamiento, almacenamiento y distribución de información. *Fuente: MSPI – MinTIC*

Tecnología de la información: Hardware, software y servicios que permiten el tratamiento automático de la información. *Fuente: MSPI – MinTIC*

Tratamiento del riesgo: Proceso para seleccionar e implementar acciones dirigidas a modificar el riesgo. *Fuente: ISO/IEC 27005:2018*

Valoración del riesgo: Proceso compuesto por el análisis y la evaluación del riesgo. *Fuente: ISO/IEC 27005:2018*

5. Políticas específicas de seguridad y privacidad de la información

Esta sección consolida las políticas específicas que soportan técnicamente la implementación de la Política General de Seguridad y Privacidad de la Información y del Sistema de Gestión de Seguridad de la Información (SGSI) de la UPME. Cada política está alineada con los controles y dominios establecidos en la norma ISO/IEC 27001:2022 y con los componentes definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

Las políticas aquí descritas tienen como objetivo orientar la aplicación de controles operativos y estratégicos que aseguren la confidencialidad, integridad y disponibilidad de los activos de información, y establecer responsabilidades claras para su cumplimiento.

5.1 Controles organizacionales

Incluye políticas relacionadas con la estructura de gestión, roles, gobierno, riesgos, relaciones externas, concienciación y cumplimiento normativo.

PA01 – Política General de Seguridad y Privacidad de la Información

Definición:
Establece los lineamientos generales para proteger la información institucional de la UPME, garantizar su confidencialidad, integridad y disponibilidad, y cumplir con los marcos normativos aplicables, incluyendo la ISO/IEC 27001:2022 y el MSPI del MinTIC.

Alcance:
Aplica a todos los funcionarios, contratistas y terceros que gestionen activos de información en el marco de los procesos de la entidad.

Lineamientos clave:

- Implementar controles de seguridad acordes al nivel de riesgo.
- Integrar el SGSI con la gestión institucional.
- Promover la mejora continua del sistema.
- Sensibilizar y formar a los usuarios en seguridad y privacidad de la información.
- Cumplir con las leyes y normas aplicables.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.1 Políticas para la seguridad de la información
A.5.35 Revisión independiente de la seguridad de la información

PA02 – Roles y responsabilidades

Definición:
Establece la asignación de responsabilidades y funciones específicas para la gestión de la seguridad y privacidad de la información en la UPME.

Alcance:
Aplica a todos los funcionarios, contratistas y terceros que participen en la creación, gestión o soporte de activos de información institucional.

Lineamientos clave:

- La Alta Dirección lidera y apoya la implementación del SGSI.
- El Oficial de Seguridad coordina la aplicación de controles.
- Cada responsable de proceso gestiona los riesgos de su área.
- Todo el personal debe cumplir las políticas y reportar incidentes.
- Los proveedores deben cumplir requisitos contractuales de seguridad.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.2 Roles y responsabilidades de seguridad de la información
A.5.3 Segregación de funciones
A.5.4 Responsabilidades de la dirección
A.5.5 Contacto con las autoridades
A.5.6 Contacto con grupos de interés especial

A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

PA03 – Gestión del riesgo de seguridad de la información

Definición:
Establece los lineamientos para identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la seguridad y privacidad de la información de la UPME.

Alcance:
Aplica a todos los procesos, activos y servicios de la entidad que manejan información, tanto a nivel interno como en interacción con terceros.

Lineamientos clave:
- Aplicar una metodología formal y sistemática de análisis y valoración de riesgos.
- Documentar y mantener actualizada la matriz de riesgos de seguridad de la información.
- Alinear el tratamiento del riesgo con la capacidad institucional y el apetito al riesgo.
- Incluir a los responsables de proceso en la identificación y seguimiento de riesgos.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
ISO/IEC 27001:2022 – Cláusula 6.1 Acciones para abordar riesgos y oportunidades
A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)
A.5.37 Procedimientos operacionales documentados

PA04 – Concientización y formación en seguridad de la información

Definición:
Establece las directrices para sensibilizar, capacitar y mantener informados a los funcionarios, contratistas y terceros sobre sus responsabilidades frente a la seguridad y privacidad de la información.

Alcance:
Aplica a todas las personas que accedan, procesen o gestionen información institucional de la UPME.

Lineamientos clave:
- Realizar actividades periódicas de sensibilización en ciberseguridad y protección de datos.
- Incluir temas de seguridad de la información en procesos de inducción y reinducción.
- Fortalecer capacidades técnicas en los equipos que gestionan TI, datos y riesgos.
- Evaluar la efectividad de las acciones de formación implementadas.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.6.3 Concientización, educación y entrenamiento en seguridad de la información

PA05 – Seguridad con proveedores y terceros

Definición:
Establece los lineamientos para asegurar que los proveedores y terceros que tengan acceso a información o recursos tecnológicos de la UPME cumplan con los requisitos de seguridad y privacidad establecidos por la entidad.

Alcance:
Aplica a todos los contratos, convenios o acuerdos con terceros que impliquen acceso, tratamiento o soporte a activos de información institucional.

Lineamientos clave:
- Incluir cláusulas de seguridad y confidencialidad en los contratos.
- Evaluar riesgos de seguridad asociados a proveedores y servicios externos.
- Supervisar el cumplimiento de los requisitos de seguridad durante la relación contractual.
- Definir medidas de control para el acceso remoto o compartido con terceros.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.14 Transferencia de información
A.5.15 Control de Acceso
A.5.16 Gestión de la identidad
A.5.17 Información de autenticación
A.5.19 Seguridad de la información en la relación con proveedores
A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores
A.5.22 Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores
A.5.37 Procedimientos operacionales documentados

PA06 – Cumplimiento legal, normativo y contractual

Definición:
Establece los lineamientos para garantizar que la gestión de la información en la UPME cumpla con la legislación vigente, regulaciones aplicables y obligaciones contractuales en materia de seguridad y privacidad.

Alcance:
Aplica a todos los procesos, sistemas y relaciones contractuales que involucren tratamiento de información institucional.

Lineamientos clave:
- Identificar y aplicar la normativa vigente sobre protección de datos personales, acceso a la información y hábeas data.
- Asegurar el cumplimiento de requisitos legales en el manejo de registros, evidencia digital y contratación.

- Incorporar requisitos legales y contractuales en la operación de los sistemas de información.
- Mantener evidencia del cumplimiento normativo y apoyar auditorías externas o requerimientos legales.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.31 Requisitos legales, estatutarios, regulatorios y contractuales
A.5.32 Derechos de propiedad intelectual
A.5.33 Protección de registros
A.5.34 Privacidad y protección de la PII (Información Identificable Personal)
A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

PA07 – Clasificación, etiquetado y uso aceptable de la información

Definición:

Establece las directrices para clasificar, etiquetar y manejar adecuadamente la información institucional de acuerdo con su nivel de sensibilidad, así como definir las condiciones para su uso aceptable.

Alcance:

Aplica a todos los documentos, datos y sistemas que contengan información institucional, sin importar su formato o medio de almacenamiento.

Lineamientos clave:

- Clasificar la información como confidencial, restringida, de uso interno o pública, según criterios definidos.
- Etiquetar los activos de información conforme a su clasificación.
- Garantizar que el tratamiento de la información se realice de acuerdo con su nivel de sensibilidad.
- Definir y divulgar reglas claras de uso aceptable para el acceso, almacenamiento y transmisión de información.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.10 Uso aceptable de activos de información y otros asociados a la misma
A.5.11 Devolución de activos
A.5.12 Clasificación de la información
A.5.13 Etiquetado de la información

PA08 – Política de trabajo remoto y dispositivos móviles

Definición:

Establece los lineamientos para proteger la información institucional cuando es accedida o procesada mediante dispositivos móviles o fuera de las instalaciones de la UPME.

Alcance:

Aplica al personal, contratistas y terceros que utilicen equipos móviles o accedan a

los sistemas de la entidad desde ubicaciones remotas.

Lineamientos clave:

- Autorizar previamente el acceso remoto y uso de dispositivos móviles.
- Aplicar cifrado, autenticación y control de acceso en conexiones remotas.
- Definir condiciones y restricciones para el uso institucional de equipos personales (BYOD).
- Supervisar y limitar el almacenamiento de información en dispositivos móviles.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.18 Derechos de acceso
A.5.37 Procedimientos operacionales documentados
A.6.7 Trabajo remoto
A.7.6 Trabajar en áreas seguras

5.2 Controles de personas

Controles relacionados con la seguridad antes, durante y después del vínculo laboral o contractual.

PA09 – Seguridad en la gestión del personal

Definición:
Establece los lineamientos para asegurar que el personal que tenga acceso a información institucional conozca y cumpla con las responsabilidades de seguridad durante todo el ciclo del vínculo laboral o contractual.

Alcance:
Aplica a funcionarios, contratistas y demás personas con acceso a los sistemas o activos de información de la UPME.

Lineamientos clave:

- Verificar antecedentes y compromisos de confidencialidad antes del ingreso.
- Incluir responsabilidades de seguridad en los perfiles de cargo y contratos.
- Realizar procesos de inducción en seguridad de la información.
- Definir procedimientos para el retiro o cambio de funciones, garantizando el retiro de accesos y activos.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.37 Procedimientos operacionales documentados
A.6.1 Revisión de antecedentes
A.6.2 Términos y condiciones de empleo
A.6.4 Proceso Disciplinario
A.6.5 Responsabilidades después de la finalización o cambio de empleo

PA10 – Compromisos de confidencialidad y conducta esperada

Definición:
Establece los compromisos que deben asumir funcionarios, contratistas y terceros respecto al uso responsable de la información y el cumplimiento de normas de conducta relacionadas con la seguridad de la información.

Alcance:
Aplica a toda persona que tenga acceso a activos de información de la UPME, de forma directa o indirecta.

Lineamientos clave:

- Firmar compromisos de confidencialidad como parte de la vinculación contractual o laboral.
- Incluir cláusulas de uso adecuado de la información en contratos y acuerdos.
- Establecer consecuencias por el incumplimiento de las normas de seguridad.
- Reforzar principios éticos en la gestión de la información institucional.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.6.2 Términos y condiciones de empleo
A.6.6 Acuerdos de confidencialidad o no divulgación

5.3 Controles físicos

Políticas relacionadas con el entorno físico y protección de instalaciones, equipos y medios.

PA11 – Seguridad física y del entorno

Definición:
Establece las medidas para proteger las instalaciones, equipos y áreas donde se maneja información institucional, frente a accesos no autorizados, daños o interferencias.

Alcance:
Aplica a todos los espacios físicos bajo responsabilidad de la UPME donde se ubiquen sistemas de información o se almacene información institucional.

Lineamientos clave:

- Restringir el acceso físico a zonas críticas como salas de servidores y archivos confidenciales.
- Implementar mecanismos de control de acceso físico (cerraduras, tarjetas, registros).
- Proteger los equipos contra daños por fuego, agua o fallas eléctricas.
- Asegurar la continuidad de los servicios ante cortes de energía o eventos físicos.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.7.1 Perímetros de seguridad física
A.7.2 Entrada física

A.7.4 Supervisión de la seguridad física
A.7.12 Seguridad del cableado
A.7.13 Mantenimiento de equipos

PA12 – Control de acceso físico

Definición:
Establece los mecanismos para gestionar y restringir el acceso físico a las instalaciones y recursos donde se almacena o procesa información de la UPME.

Alcance:
Aplica a todas las sedes, zonas restringidas, centros de datos, cuartos de comunicaciones y demás espacios físicos relacionados con el manejo de información institucional.

Lineamientos clave:
- Implementar controles de acceso físico diferenciados por niveles de criticidad.
- Registrar ingresos y salidas del personal y visitantes en zonas sensibles.
- Revocar el acceso físico inmediatamente al finalizar la relación contractual o laboral.
- Inspeccionar periódicamente el estado de los controles de acceso físico.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.7.3 Aseguramiento de oficinas, salas e instalaciones
A.7.4 Supervisión de la seguridad física

PA13 – Protección de activos físicos y medios de almacenamiento

Definición:
Establece las medidas para proteger los activos físicos y los medios que contienen información institucional, asegurando su uso adecuado, almacenamiento seguro y disposición controlada.

Alcance:
Aplica a todos los equipos, dispositivos, documentos impresos y medios digitales utilizados o almacenados en las instalaciones de la UPME o por terceros autorizados.

Lineamientos clave:
- Mantener inventario actualizado de los activos físicos y medios de almacenamiento.
- Prevenir accesos no autorizados, daños o pérdidas de medios físicos.
- Aplicar controles de almacenamiento seguro para medios removibles.
- Establecer procesos de destrucción segura de medios que contengan información sensible.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.7.5 Protección contra amenazas físicas y ambientales.
A.7.6 Trabajar en áreas seguras
A.7.7 Escritorio despejado y pantalla despejada
A.7.8 Ubicación y Protección del equipo
A.7.9 Seguridad de los activos fuera de las instalaciones
A.7.10 Medios de almacenamiento
A.7.11 Servicios de apoyo

5.4 Controles tecnológicos

Incluye políticas orientadas a la gestión segura de tecnologías de la información, sistemas, redes y datos.

PA14 – Control de acceso lógico

Definición:
Establece los lineamientos para controlar el acceso a sistemas, redes, aplicaciones y datos institucionales, asegurando que solo usuarios autorizados puedan acceder a los recursos de información según su rol.

Alcance:
Aplica a todos los sistemas de información, plataformas, aplicaciones y servicios tecnológicos utilizados en la UPME.

Lineamientos clave:

- Asignar accesos de acuerdo con principios de mínima autoridad y necesidad de conocer.
- Gestionar credenciales de forma segura, incluyendo autenticación fuerte cuando aplique.
- Establecer procedimientos para altas, modificaciones y bajas de usuarios.
- Monitorear y revisar periódicamente los permisos y cuentas activas.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.15 Control de Acceso
A.5.16 Gestión de la identidad
A.5.17 Información de autenticación
A.5.37 Procedimientos operacionales documentados
A.8.2 Derechos de acceso privilegiado
A.8.3 Restricción de acceso a la información
A.8.5 Autenticación segura
A.8.11 Enmascaramiento de datos

PA15 – Gestión de activos de información

Definición:
Establece los lineamientos para identificar, clasificar, mantener y proteger los activos de información de la UPME a lo largo de su ciclo de vida.

Alcance:
Aplica a todos los activos relacionados con la información, incluyendo datos, aplicaciones, infraestructura tecnológica, documentación y servicios de la entidad.

Lineamientos clave:

- Mantener un inventario actualizado de activos de información.
- Asignar responsables a cada activo para su custodia y gestión.
- Aplicar controles adecuados según la clasificación del activo.
- Garantizar la protección de los activos durante cambios, traslado o baja.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.9 Inventario de activos de información y otros asociados a la misma
A.5.10 Uso aceptable de activos de información y otros asociados a la misma
A.5.37 Procedimientos operacionales documentados
A.8.1 Dispositivos de punto final de usuario

PA16 – Seguridad en redes y comunicaciones

Definición:
Establece los controles para proteger la infraestructura de red y las comunicaciones de datos institucionales contra accesos no autorizados, alteraciones o pérdidas.

Alcance:
Aplica a todas las redes internas, conexiones remotas, canales de comunicación, servicios en la nube y medios utilizados para la transmisión de información en la UPME.

Lineamientos clave:

- Segmentar la red y aplicar controles de acceso a nivel de red y dispositivos.
- Proteger las comunicaciones mediante cifrado y autenticación cuando sea requerido.
- Monitorear el tráfico y los eventos de red para detectar actividades anómalas.
- Asegurar las configuraciones de routers, switches y puntos de acceso inalámbricos.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.8.6 Gestión de la capacidad
A.8.14 Redundancia de las instalaciones de procesamiento de información
A.8.20 Seguridad en redes
A.8.21 Seguridad de los servicios de red
A.8.22 Segregación de redes

PA17 – Protección contra software malicioso

Definición:
Establece las medidas para prevenir, detectar y responder ante la presencia de software malicioso que pueda comprometer la seguridad de los sistemas y la información de la UPME.

Alcance:
Aplica a todos los dispositivos, servidores, estaciones de trabajo, sistemas de información y redes de la entidad.

Lineamientos clave:

- Implementar soluciones antimalware actualizadas en todos los equipos.
- Restringir la ejecución de software no autorizado o proveniente de fuentes no confiables.
- Configurar políticas de protección en correo electrónico y navegación web.
- Monitorear eventos y alertas para responder a infecciones o intentos de ataque.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.8.7 Protección contra malware
A.8.8 Gestión de vulnerabilidades técnicas

PA18 – Copias de seguridad y restauración

Definición:
Establece los lineamientos para realizar y gestionar copias de seguridad de la información crítica, asegurando su disponibilidad y recuperación ante pérdida o incidente.

Alcance:
Aplica a todos los sistemas, bases de datos, archivos y configuraciones relevantes para la operación de la UPME.

Lineamientos clave:

- Definir y aplicar una política de respaldos con periodicidad adecuada.
- Verificar regularmente la integridad y restauración de las copias.
- Almacenar respaldos en ubicaciones seguras, preferiblemente fuera del sitio principal.
- Proteger las copias mediante cifrado y control de acceso.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.8.13 Copia de seguridad de la información

PA19 – Desarrollo seguro y control de cambios

Definición:
Establece los lineamientos para asegurar que el desarrollo, adquisición y mantenimiento de sistemas de información se realice bajo prácticas seguras y con gestión controlada de los cambios.

Alcance:
Aplica a todo el ciclo de vida de desarrollo de software, implementación de soluciones tecnológicas, y procesos de cambio en sistemas existentes de la UPME.

Lineamientos clave:

- Aplicar principios de codificación segura y revisión de vulnerabilidades.
- Controlar los cambios mediante procesos documentados y autorizados.
- Validar la funcionalidad y seguridad antes de pasar a producción.
- Segregar ambientes de desarrollo, pruebas y producción.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.29 Seguridad de la información durante interrupciones
A.5.37 Procedimientos operacionales documentados
A.8.4 Acceso al código fuente
A.8.25 Ciclo de vida de desarrollo seguro
A.8.26 Requisitos de seguridad de la aplicación
A.8.27 Arquitectura del sistema seguro y principios de ingeniería
A.8.28 Codificación segura
A.8.29 Pruebas de seguridad en desarrollo y aceptación
A.8.30 Desarrollo subcontratado
A.8.31 Separación de los entornos de desarrollo, prueba y producción
A.8.32 Gestión de cambios

PA20 – Uso de criptografía y autenticación

Definición:
Establece los lineamientos para proteger la información mediante el uso adecuado de técnicas criptográficas y mecanismos de autenticación, garantizando la confidencialidad, integridad y control de acceso.

Alcance:
Aplica a todos los sistemas, servicios, plataformas y dispositivos de la UPME que gestionen información sensible o realicen intercambio de datos.

Lineamientos clave:

- Utilizar algoritmos criptográficos robustos y actualizados para cifrado de datos.
- Proteger las claves criptográficas mediante almacenamiento seguro y controles de acceso.
- Establecer autenticación multifactor en servicios críticos.
- Documentar y revisar periódicamente las políticas de cifrado y autenticación.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.37 Procedimientos operacionales documentados
A.8.3 Restricción de acceso a la información
A.8.24 Uso de criptografía

PA21 – Inteligencia de amenazas

Definición:
Establece los lineamientos para identificar, recopilar, analizar y utilizar información relevante sobre amenazas de seguridad que puedan afectar la organización, con el fin de anticiparse y fortalecer la postura defensiva.

Alcance:
Aplica a todas las áreas encargadas de la seguridad de la información, incluyendo monitoreo, análisis, respuesta y gestión del riesgo.

Lineamientos clave:

- Obtener inteligencia de amenazas de fuentes internas y externas confiables.
- Establecer procesos para analizar y filtrar indicadores de compromiso.
- Incorporar la inteligencia de amenazas en la evaluación de riesgos.
- Actualizar y compartir información relevante con las partes interesadas pertinentes.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.7 Inteligencia de amenazas
A.5.25 Evaluación y decisión sobre los eventos de seguridad de la información
A.5.37 Procedimientos operacionales documentados

PA22 – Seguridad en la gestión de proyectos

Definición:
Define los principios que aseguran la incorporación de requisitos de seguridad de la información en todas las fases del ciclo de vida de los proyectos institucionales.

Alcance:
Aplica a todos los proyectos institucionales que involucren sistemas, servicios o procesos que usen información de la organización.

Lineamientos clave:

- Identificar requisitos de seguridad desde la planificación del proyecto.
- Evaluar riesgos de seguridad en cada etapa del proyecto.
- Asignar responsables de la seguridad dentro del equipo del proyecto.
- Validar el cumplimiento de medidas de seguridad antes del cierre del proyecto.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.8 Seguridad de la información en la gestión de proyectos

PA23 – Filtrado web y uso aceptable de Internet

Definición:
Regula el acceso a contenidos web a través de mecanismos de filtrado y establece criterios de uso aceptable de Internet en los equipos de la organización.

Alcance:
Aplica a todos los usuarios, dispositivos y redes que utilicen acceso a Internet desde los sistemas institucionales.

Lineamientos clave:

- Bloquear sitios maliciosos o que representen riesgos.
- Establecer categorías de contenido permitidas y restringidas.
- Monitorear el uso de Internet para detectar abusos o incidentes.
- Sensibilizar a los usuarios sobre las consecuencias del uso indebido.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.8.23 Filtrado web

PA24 – Supervisión y monitoreo de actividades

Definición:
Establece los mecanismos para registrar, supervisar y analizar las actividades que afectan la seguridad de la información dentro de los sistemas institucionales.

Alcance:
Aplica a todos los sistemas, procesos y usuarios que interactúan con activos de información.

Lineamientos clave:

- Implementar registros de auditoría en sistemas críticos.
- Establecer herramientas y procedimientos de monitoreo continuo.
- Definir alertas e indicadores para detectar eventos anómalos.
- Revisar los registros periódicamente para mejorar la detección de incidentes.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.25 Evaluación y decisión sobre los eventos de seguridad de la información
A.5.26 Respuesta a los incidentes de seguridad de la información
A.5.28 Recopilación de pruebas
A.5.33 Protección de registros
A.5.37 Procedimientos operacionales documentados
A.6.8 Reportes de eventos de seguridad de la información
A.8.12 Prevención de fuga de datos

PA25 – Seguridad en servicios en la nube

Definición:
Define los lineamientos para garantizar la protección de la información institucional

cuando se adquieren o utilizan servicios de computación en la nube.

Alcance:
Aplica a todos los servicios contratados o utilizados por la organización que se ejecuten en plataformas de nube pública, privada o híbrida.

Lineamientos clave:

- Establecer cláusulas contractuales que aseguren la protección de la información.
- Asegurar que el proveedor implemente controles alineados a normas internacionales.
- Cifrar la información almacenada o procesada en la nube.
- Evaluar la seguridad y cumplimiento del proveedor antes de la contratación.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.23 Seguridad de la información para el uso de servicios en la nube (cloud)
A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
A.5.37 Procedimientos operacionales documentados

PA26 – Eliminación y destrucción segura de información

Definición:
Establece los mecanismos para eliminar o destruir de forma segura información y medios de almacenamiento cuando ya no sean necesarios.

Alcance:
Aplica a todos los dispositivos, documentos y medios que contengan información sensible o institucional.

Lineamientos clave:

- Utilizar herramientas y procedimientos certificados para la eliminación de datos.
- Documentar la destrucción de medios críticos.
- Asegurar que terceros contratados para destrucción cumplan con requisitos de seguridad.
- Capacitar al personal en las prácticas seguras de eliminación de información.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.7.14 Eliminación segura o reutilización de equipos
A.8.10 Eliminación de información

PA27 – Pruebas de seguridad técnica y validación de cambios

Definición:
Define los criterios para realizar pruebas técnicas de seguridad en sistemas y para validar que los cambios no introduzcan nuevas vulnerabilidades.

Alcance:
Aplica a todos los sistemas, aplicaciones e infraestructuras sujetas a mantenimiento, desarrollo o mejora.

Lineamientos clave:

- Ejecutar pruebas de penetración y escaneo de vulnerabilidades regularmente.
- Realizar pruebas después de cambios mayores.
- Documentar y mitigar los hallazgos de seguridad.
- Asegurar que el entorno de pruebas esté separado del de producción.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.29 Seguridad de la información durante interrupciones
A.5.37 Procedimientos operacionales documentados
A.8.31 Separación de los entornos de desarrollo, prueba y producción
A.8.33 Información de prueba
A.8.34 Protección de sistemas de información durante pruebas de auditoría

PA28 – Gestión de configuraciones y control de software

Definición:
Establece los lineamientos para mantener configuraciones seguras y controlar la instalación de software en los sistemas institucionales.

Alcance:
Aplica a todos los equipos, servidores, redes y sistemas operativos de la Entidad.

Lineamientos clave:

- Establecer configuraciones base seguras para cada tipo de sistema.
- Controlar la instalación de software con listas blancas o sistemas de aprobación.
- Prohibir el uso de software no autorizado o sin licenciamiento.
- Revisar y actualizar las configuraciones regularmente.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:
A.5.37 Procedimientos operacionales documentados
A.8.9 Gestión de la configuración

PA29 – Gestión de configuraciones en TI

Definición:
Establece los lineamientos para la generación, gestión, monitoreo y protección de registros técnicos asociados a eventos de seguridad, actividades de usuario, sincronización de sistemas y control del uso de software y programas privilegiados.

Alcance:
Aplica a todos los sistemas, servidores, estaciones de trabajo y dispositivos que hagan parte de la infraestructura tecnológica de la Entidad.

Lineamientos clave:

- Elaborar, conservar y revisar periódicamente los registros que documenten actividades de los usuarios, eventos de seguridad, fallas y excepciones.
- Generar y analizar registros que incluyan actividades relevantes para la seguridad, incluyendo fallas, excepciones y eventos operativos.
- En lo posible todos los sistemas deben mantener sincronización con una fuente única y confiable de tiempo.
- El uso de programas con privilegios elevados debe estar estrictamente restringido y controlado.
- La instalación de software en sistemas operativos debe estar sujeta a procedimientos definidos y autorizaciones formales.

Controles relacionados del Anexo A – ISO/IEC 27001:2022:

A.5.27 Aprendizaje sobre los incidentes de seguridad de la información
A.5.30 Preparación de las TIC para la continuidad de negocio
A.5.37 Procedimientos operacionales documentados
A.8.6 Gestión de la capacidad
A.8.15 Registro
A.8.16 Actividades de seguimiento
A.8.17 Sincronización del reloj (clock)
A.8.18 Uso de programas de utilidad privilegiados
A.8.19 Instalación de software en sistemas operativos
A.8.34 Protección de sistemas de información durante pruebas de auditoría

6. VIGENCIA, REVISIÓN Y MEJORA

El presente manual de políticas y normas de seguridad y privacidad de la información entra en vigencia a partir de su aprobación por el Comité Institucional de Gestión y Desempeño de la UPME.

El contenido será revisado al menos una vez al año o cuando ocurran cambios significativos en los riesgos, procesos, tecnologías, estructura organizacional o normatividad aplicable.

Las políticas contenidas en este manual podrán ser ajustadas por recomendación del Oficial de Seguridad de la Información y deberán conservar su alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma ISO/IEC 27001:2022.

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción de los cambios**
14/07/2025	1	Creación del documento acorde al MSPI Versión 5 y la norma ISO/IEC 27001:2022.

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
RESOLUCIÓN	002277 DE 2025	RESOLUCIÓN 002277 DE JUNIO DE 2025	Externo	Actualización del Modelo de Seguridad y Privacidad de la Información (MSPI), contenido en el Anexo 1 de la Resolución 500 de 2021, y se derogan disposiciones anteriores	Se fortalece la estrategia de seguridad digital del Estado colombiano, al adoptar los lineamientos de la norma ISO/IEC 27001:2022.	MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	03/06/2025
CONPES	3854 de 2016	CONPES 3854 de 2016	Externo	Lineamientos de Política Nacional de Seguridad Digital	El objetivo general de esta política es que los ciudadanos, las entidades del Gobierno y los empresarios conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.	DEPARTAMENTO NACIONAL DE PLANEACIÓN	11/04/2016
DECRETO	1524 de 2002	Decreto 1524 de 2002 – Pornografía Infantil	Externo	Por el cual se reglamenta el artículo 5 de la Ley 679 de 2001.	Establece las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad a cualquier modalidad de información pornográfica contenida en internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.	MINISTERIO DE COMUNICACIONES	24/07/2002
DECRETO	1377 de 2013	Decreto 1377 de 2013	Externo	Por el cual se reglamenta parcialmente la Ley 1581 de 2012	Autorización para el tratamiento de datos personales y establece obligaciones específicas para el tratamiento de datos sensibles.	MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO DE COLOMBIA	27/06/2013
DECRETO	1499 de 2017	Decreto 1499 de 2017	Externo	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015	El objetivo principal de esta actualización es consolidar, en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente. MIPG.	DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA DE COLOMBIA	11/09/2017
DECRETO	1082 de 2015	Decreto1082 de Julio 17 de 2015	Externo	Por el cual se reglamenta el sistema de compras y contratación pública	Las entidades estatales deben procurar por el logro de los objetivos del sistema de compras y contratación pública definidos por Colombia Compra Eficiente	EL CONGRESO DE LA REPÚBLICA	17/07/2013

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
DIRECTIVA PRESIDENCIAL	01 de 1999	Directiva Presidencial 01 de 1999	Externo	Respecto al Derecho de autor y a los Derechos Conexos	Obligaciones de los Servidores Públicos respecto al Derecho de autor y a los Derechos Conexos	PRESIDENTE DE LA REPÚBLICA	25/02/1999
DIRECTIVA PRESIDENCIAL	02 de 2000	Directiva Presidencial 02 de agosto 28 de 2000:	Externo	Respecto a las tecnologías de información y la Agenda de Conectividad como política del Estado	Para garantizar la modernización del Estado, eficiente y transparente, que haga uso intensivo de las TIC, para prestar servicios al ciudadano a través de un óptimo desempeño de sus funciones.	PRESIDENTE DE LA REPÚBLICA	28/08/2000
DIRECTIVA PRESIDENCIAL	02 de 2002	Directiva Presidencial 02 de 2002	Externo	Respecto al autor y a los Derechos Conexos en lo referente a utilización de programas de Ordenador (Software)	Instruir a las personas encargadas en cada entidad de la adquisición de Software para que los programas de computador que se adquieran estén respaldados por los documentos de licenciamiento o transferencia de propiedad respectivos.	PRESIDENTE DE LA REPÚBLICA	02/02/2002
DIRECTIVA PRESIDENCIAL	4 de 2012	Directiva Presidencial 4 de 2012 – Cero Papel	Externo	Eficiencia Administrativa y lineamientos de la Política de Cero Papel	Directiva en la cual se establecen las condiciones para la implementación de la política de cero papeles mediante un plan de eficiencia administrativa	EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA	03/04/2012
LEY	23 de 1982	Ley 23 de 28 de enero de 1982 Autor	Externo	Por medio de la cual se introducen medidas para el reconocimiento de los derechos de autor	Reglamenta y reconoce los derechos de autor	EL CONGRESO DE LA REPÚBLICA	28/01/1982
LEY	80 de 1993	Ley 80 de 1993	Externo	Por la cual se expide el Estatuto General de Contratación de la Administración Pública	Dispone las reglas y principios que rigen los contratos de las entidades estatales.	EL CONGRESO DE LA REPÚBLICA	28/10/1993
LEY	527 de 1999	Ley 527 de agosto 18 de 1999	Externo	Por medio de la cual se define y reglamenta el comercio electrónico	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	EL CONGRESO DE LA REPÚBLICA	18/08/1999
LEY	1221 de 2008	Ley 1221 de 2008	Externo	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones	Regular el teletrabajo como un instrumento de generación de empleo y autoempleo.	EL CONGRESO DE LA REPÚBLICA	16/07/2008

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
DECRETO	2499 de 2012	Decreto 2499 de diciembre 6 de 2012	Externo	Por el cual se modifica el parágrafo del artículo 1 del Decreto 260 de 2001, adicionado por el Decreto 2521 de 2011.	Se les aplicará la nueva tarifa de retención en la fuente, a las empresas en actividades de análisis, diseño, desarrollo, implementación, mantenimiento, ajustes, pruebas, suministro y documentación, fases necesarias en la elaboración de programas de informática, sean o no personalizados, así como el diseño de páginas web y consultoría en programas de informática.	MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO	06/12/2012
DECRETO	2693 de 2012	Decreto 2693 de diciembre 21 de 2012	Externo	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones"	Lineamiento para entidades gubernamentales para el cumplimiento de la Estrategia de Gobierno en Línea	MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO DE COLOMBIA	21/12/2012
DECRETO	17 de 2013	Ley Estatutaria 1377 de 2013	Externo	Por el cual se reglamenta parcialmente la Ley 1581 de 2012	Regular el manejo de la información personal en bases de datos y los derechos de las personas respecto a sus datos personales	EL CONGRESO DE LA REPÚBLICA	19/12/2013
DECRETO	1510 de 2013	Decreto 1510 de Julio 17 de 2013	Externo	Por el cual se reglamenta el sistema de compras y contratación pública	Las entidades estatales deben procurar por el logro de los objetivos del sistema de compras y contratación pública definidos por Colombia Compra Eficiente	EL CONGRESO DE LA REPÚBLICA	17/07/2013
LEY	906 de 2004	Ley 906 de 2004	Externo	Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004)	LIBRO II TECNICAS DE INDAGACION E INVESTIGACION DE LA PRUEBA Y SISTEMA PROBATORIO.MEDIOS COGNOSCITIVOS EN LA INDAGACION E INVESTIGACION	EL CONGRESO DE LA REPÚBLICA	31/08/2004
LEY	1273 de 2009	Ley 1273 de 2009: delitos informáticos	–Externo	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	Dispone la normatividad referente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.	EL CONGRESO DE LA REPÚBLICA	05/01/2009

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
				integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.			
LEY	1341 de 2009	Ley 1341 de 2009	Externo	Por la cual se definen 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 de Espectro y se dictan otras disposiciones.	Esta ley establece el marco normativo para el desarrollo del sector de las TIC en Colombia, con el objetivo de promover su crecimiento y fortalecer su contribución al desarrollo económico y social del país	EL CONGRESO DE LA REPÚBLICA	30/07/2009
LEY	1437 de 2011	Ley 1437 de 2011	Externo	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	Está Ley es el marco general para 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.	EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA	06/03/2014
LEY	1581 de 2012	Ley Estatutaria 1581 de 17 de octubre de 2012	Externo	Por el cual se dictan disposiciones generales para la protección de Datos Personales.	Está Ley es el marco general de la protección de los datos personales en Colombia.	EL CONGRESO DE LA REPÚBLICA	17/10/2012
LEY	1712 de 2014	Ley 1712 de 2014 Transparencia de Información	Externo	Por la cual se dictan disposiciones para el acceso a la información pública.	Ley de transparencia de información pública	EL CONGRESO DE LA REPUBLICA	Marzo 2014
NORMA TÉCNICA	27001 de 2022	Norma Técnica 27001	Externo	Sistemas de gestión de la seguridad de la información	Permite a las organizaciones implementar un sistema de gestión de la seguridad de la información y aplicar un proceso de control de riesgos adaptado a sus necesidades, y ampliarlo según sea necesario a medida que evolucionen estos factores.	ICONTEC	25/10/2022
NORMA TÉCNICA	27002 de 2022	Norma Técnica 27002	Externo	Sistemas de gestión de la seguridad de la información	ISO 27002:2022 es un estándar de respaldo, complementario y accesorio de ISO 27001. Como tal, su función es de apoyo y respaldo	ICONTEC	25/10/2022

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
NORMA TÉCNICA	9001 de 2015	Norma Técnica ISO 9001 23 de Septiembre de 2015	Externo	Sistemas de gestión de la calidad	Gestión de la calidad; sistema de la calidad; gestión por procesos; administración de la calidad.	ICONTEC	23/09/2015
NORMA TÉCNICA	1000 de 2009	NTCGP 1000:2009	Externo	NORMA TÉCNICA DE CALIDAD EN LA GESTIÓN PÚBLICA que permite el cumplimiento de la norma internacional ISO 9001:2008, puesto que ajusta la terminología y los requisitos de ésta a la aplicación específica en las entidades.	Esta norma específica los requisitos para la implementación del Sistema de Gestión de la Calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de Servicios.	ICONTEC	15/12/2009
CONSTITUCIÓN	Artículo 15	CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991	Externo	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. La correspondencia y demás formas de comunicación privada son inviolables.	Presidente de la república	04/07/1991
CONSTITUCIÓN	Artículo 209	CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991	Externo	Métodos y procedimientos de control interno, de conformidad con lo que disponga la ley	Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.	Presidente de la república	04/07/1991
DECRETO	103 DE 2015	DECRETO 103 DE 2015	Externo	gestión de la información pública	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	Presidente de la república	20/01/2014
DECRETO	1074 de 2015	Decreto 1074 de 2015	Externo	Registro Nacional de Bases de Datos	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26	Presidente de la república	26/05/2015

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
DECRETO	1078 de 2015	Decreto 1078 de 2015	externo	Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones	Presidente de la república	26/05/2015
DECRETO	1081 de 2015	Decreto 1081 de 2015	Externo	Reglamentario del Sector Presidencia	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia	Presidente de la república	26/05/2015
DECRETO	1083 de 2015	Decreto 1083 de 2015	Externo	Reglamentario del Sector de la Función Pública	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".	Presidente de la república	26/05/2015
LEY	1915 de 2018	Ley 1915 de 2018	Externo	Disposiciones relativas al derecho de autor y los derechos conexos	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos	Presidente de la república	12/07/2018
DECRETO	612 de 2018	Decreto 612 de 2018	Externo	Reglamentario del Sector de Función Pública	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado	Presidente de la república	04/04/2018
DECRETO	2106 de 2019	Decreto 2106 de 2019	Externo	Estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.	establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.	Presidente de la república	22/11/2019
LEY	1952 de 2019	Ley 1952 de 2019	Externo	se expide el código general disciplinario	Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.	Congreso de Colombia	28/01/2019
LEY	Ley 2300 de 2023	Ley 2300 de 2023	Externo	Protección de usuarios frente al contacto digital no solicitado por entidades públicas o privadas.	Complementa el régimen de protección de datos personales regulado por la Ley 1581, enfocándose en comunicaciones digitales no autorizadas.	Congreso de la República	10/07/2023
LEY	Ley 2293 de 2023	Ley 2293 de 2023	Externo	Medidas para fortalecer la seguridad digital en entidades públicas y financieras,	Marco obligatorio para reforzar medidas técnicas, administrativas y operativas contra ciberataques.	Congreso de la República	22/05/2023

TIPO DE DOCUMENTO	NÚMERO	NOMBRE	ORIGEN	ASUNTO	ESPECIFICIDAD O USO	ENTIDAD EMISORA	FECHA DE ENTRADA EN VIGENCIA
				incluyendo la obligatoriedad de protocolos de ciberseguridad y reportes de incidentes.			
CONPES	4050 de 2021	Política de transformación digital e innovación pública	Externo	Política nacional que establece lineamientos para implementar la transformación digital en el sector público, integrando medidas de seguridad digital.	Define lineamientos estratégicos para mejorar servicios digitales institucionales con enfoque en seguridad.	Departamento Nacional de Planeación (DNP)	27/12/2021
Decreto	Decreto 1756 de 2020	Lineamientos de Arquitectura Empresarial Pública	Externo	Establece los lineamientos para adoptar e implementar Arquitectura Empresarial en las entidades públicas, incluyendo componentes de seguridad digital y gestión tecnológica.	Marco para la planeación tecnológica y gestión segura de información institucional.	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	23/12/2020
Circular	Circular Externa 003 de 2023	Actualización de políticas y avisos de privacidad de datos personales	Externo	Obliga a todas las entidades a revisar y actualizar sus políticas de tratamiento de datos personales y avisos de privacidad conforme a la Ley 1581 de 2012.	Directrices específicas para cumplir con requisitos normativos de protección de datos personales.	Superintendencia de Industria y Comercio (SIC)	16/01/2023

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción de los cambios**
25/07/2025	1	Creación del documento en el sistema de información acorde al MSPI Versión 5 y la norma ISO/IEC 27001:2022.