Información Pública

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CENTRO NACIONAL DE MEMORIA HISTÓRICA

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
2025

	NOMBRE	CARGO	FECHA
ELABORÓ	Jair Caicedo Angélica María Ángel	Contratista Gestión de TIC	28/09/2025
REVISÓ	Ronal Alexis Martínez Cerón	Profesional Especializado	28/09/2025
	María Camila Pardo Reyes	Oficina Asesora jurídica	20/11/2025
REVISÓ	Yeraldine Nope León	Contratista - Planeación	18/12/2025
REVISÓ	Luz Dary Patricia Pardo Muñoz	Profesional Universitario - Planeación	26/12/2025
APROBÓ	Ana María Trujillo Coronado	Directora Administrativa y Financiera	20/11/2025
APROBÓ	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	12/18/2025

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección del **Centro Nacional de Memoria Histórica** (en adelante la Entidad), 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.

En concordancia con este propósito, la política busca garantizar que la gestión de la seguridad y privacidad de la información sea transversal a todos los procesos institucionales, asegurando que la información se preserve bajo los principios de confidencialidad, integridad, disponibilidad y trazabilidad. Así mismo, el objetivo se orienta a fortalecer la resiliencia de la Entidad frente a amenazas internas y externas, a promover el cumplimiento de la normatividad nacional e internacional, y a consolidar un entorno de gestión de la información que respalde la toma de decisiones estratégicas, la continuidad del servicio público y la confianza ciudadana en el cumplimiento de la misión institucional.

De igual manera, este objetivo se complementa con la definición de un marco de acción que permita a la Entidad implementar de forma efectiva controles, políticas, procedimientos y prácticas alineadas con estándares internacionales como la ISO/IEC 27001:2022, garantizando un enfoque de mejora continua en la gestión de la seguridad de la información. En este sentido, la política no solo constituye un instrumento normativo, sino también un compromiso estratégico de la Alta Dirección para proteger los activos de información, gestionar los riesgos asociados a su uso y asegurar que la Entidad cumpla su función pública de manera responsable, transparente y segura.

2. DEFINICIONES/GLOSARIO

- **ACCESO LÓGICO:** Restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como id.
- **ACTIVO CRÍTICO**: Son aquellos elementos o componentes que hacen parte de la infraestructura crítica.
- **ACTIVO DE INFORMACIÓN:** Conocimiento o información que tiene valor para 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.
- **AMENAZA:** Causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o de la Entidad.

- **AUDITORÍA DE SEGURIDAD:** Proceso formal de evaluación del cumplimiento de controles, políticas y procedimientos relacionados con la seguridad de la información.
- **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.
- **AUTORIZACIÓN:** Proceso que determina los recursos a los que un usuario o sistema puede acceder, según sus permisos asignados.
- **BACKUP (COPIA DE SEGURIDAD):** Copia de los datos originales realizada con el fin de recuperarlos en caso de pérdida, eliminación o corrupción.
- **BRECHA DE SEGURIDAD:** Acceso, uso, divulgación, modificación o destrucción no autorizada de información, ya sea accidental o intencional.
- **CIBERSEGURIDAD:** Conjunto de prácticas, procesos, herramientas y medidas técnicas, organizativas y legales orientadas a proteger los sistemas de información, redes, aplicaciones y datos frente a accesos no autorizados, ataques, daños, alteraciones o interrupciones, ya sean deliberados o accidentales. La ciberseguridad busca garantizar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, así como la resiliencia de los servicios digitales frente a amenazas internas o externas.
- **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 DE ACCESO:** Mecanismo que restringe el acceso a sistemas o información sólo a personas o procesos autorizados.
- **CONTROLES:** Medida preventiva, detectiva o correctiva que permite reducir o mitigar los riesgos de seguridad.
- **CRIPTOGRAFÍA:** Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
- **DATOS PERSONALES:** Información personal que afecta la intimidad del titular o cuyo uso indebido puede vulnerar el derecho fundamental de una persona.
- **DISPONIBILIDAD:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información.

- **INFORMACIÓN:** Conjunto de datos organizados, procesados y contextualizados que poseen valor y significado para la entidad, y que requieren protección en cuanto a su confidencialidad, integridad y disponibilidad.
- **INTEGRIDAD:** Propiedad de la información que busca preservar su exactitud y completitud.
- **ISO/IEC 27001**: Norma internacional que establece los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- **MITIGACIÓN DE RIESGOS:** Acciones orientadas a reducir el impacto o la probabilidad de ocurrencia de un riesgo.
- **RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021:** Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital.
- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza explote una vulnerabilidad y afecte la información o los activos asociados.
- **SEGURIDAD DE LA INFORMACIÓN:** Conjunto de medidas, políticas, procedimientos y controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información frente a amenazas internas o externas, garantizando su uso adecuado y reduciendo riesgos que comprometan a la entidad.
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI**): Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan o se gestionan dentro de una entidad.
- **TRATAMIENTO DE LA INFORMACIÓN:** Procedimiento que permite decidir sobre el tratamiento de los datos personales.
- **VULNERABILIDAD:** Debilidad que puede ser explotada por una amenaza para causar un incidente.

3. MARCO NORMATIVO

La entidad como establecimiento público del orden nacional, en el marco de sus funciones deberá velar por el cumplimiento de la normativa relacionada con la seguridad y privacidad de la información, entre las que se encuentra:

- **Constitución Política de Colombia de 1991**, artículos 15 y 20, que consagran el derecho fundamental al habeas data, a la intimidad y a la información.
- **Ley 1581 de 2012** y sus decretos reglamentarios, por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014** – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Decreto 1377 de 2013**, reglamentario de la Ley 1581 de 2012, sobre autorización y tratamiento de datos personales.
- **Ley 1273 de 2009**, que tipifica delitos informáticos y protege la información y los datos.
- **Decreto 2106 de 2019**, que establece lineamientos de simplificación de trámites y la gestión digital en las entidades públicas.
- **Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC),** que incluye lineamientos sobre seguridad y privacidad de la información en entidades públicas.
- **Modelo de Seguridad y Privacidad de la Información (MSPI)** expedido por el MINTIC, como referente obligatorio para las entidades del Estado en la gestión y protección de la información.
- **Norma Técnica Colombiana NTC ISO/IEC 27001 y 27002**, sobre gestión de seguridad de la información y controles de seguridad, como referencia de buenas prácticas internacionales.
- **Decreto 1078 de 2015, Decreto Único Reglamentario del sector TIC**, que compila normas en materia de seguridad digital y gobierno electrónico.
- **Ley 594 de 2000** – Ley General de Archivos, que regula la organización, conservación y disposición de documentos, incluyendo criterios de seguridad.
- **Circular 001 de 2021 de la Superintendencia de Industria y Comercio (SIC),** sobre medidas mínimas para la implementación del programa de gestión de datos personales.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La **Entidad**, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad 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.

La Entidad reconoce que la información constituye un recurso estratégico esencial para el cumplimiento de su misión, visión y objetivos institucionales. En consecuencia, se establece la presente Política de Seguridad y Privacidad de la Información, orientada a garantizar la protección, confidencialidad, integridad, disponibilidad y trazabilidad de la información que se genera, administra, procesa, comparte, almacena, consulta o elimina, sin importar su formato, medio, ubicación o canal de transmisión. Esta política aplica a todos los funcionarios, contratistas, proveedores y terceros que, en desarrollo de sus funciones o actividades, tengan acceso a activos de información de la Entidad, y define las directrices necesarias para su gestión segura, en concordancia con la normatividad vigente, las buenas prácticas internacionales y el compromiso institucional con la transparencia, la confianza ciudadana y la mejora continua.

La Política de Seguridad y Privacidad de la Información de la Entidad se formaliza en el presente documento como marco rector para la gestión segura de la información institucional. Su definición se fundamenta en los lineamientos de la norma ISO/IEC 27001:2022, en la Resolución 00500 del 10 de marzo de 2021, mediante la cual se adoptan los estándares de seguridad digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital, así como en la normativa nacional e internacional aplicable.

De esta manera, la Entidad asegura la adopción de buenas prácticas reconocidas globalmente, alineadas con los objetivos estratégicos institucionales, el fortalecimiento de la confianza ciudadana y la consolidación de un entorno digital seguro, resiliente y transparente.

La presente política constituye un eje fundamental del Sistema de Gestión de Seguridad y Privacidad de la Información de la Entidad, y se establece como el marco orientador para la definición, implementación y fortalecimiento de los controles, procedimientos y lineamientos institucionales. En este sentido, se convierte en un instrumento estratégico que asegura la adecuada protección de los activos de información, facilita el cumplimiento normativo y promueve la mejora continua en la gestión de la seguridad y privacidad de la información.

En este contexto, la Entidad, mediante la implementación del Manual de Políticas de Seguridad y Privacidad de la Información, establece las directrices necesarias para la adecuada aplicación de la política aquí definida.

Dicho manual orienta el cumplimiento de requisitos normativos y regulatorios, promueve el manejo responsable y seguro de la información, y fortalece la gestión de los riesgos asociados a su uso, así como a la adopción de nuevas tecnologías de información y comunicaciones. Con ello, la Entidad garantiza a sus usuarios y a la

ciudadanía en general la custodia, el control y la protección integral de la información procesada internamente o suministrada por terceros, consolidando un entorno de confianza y transparencia.

La **Entidad,** en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, proveedores, aprendices, practicantes y personas interesadas de la Entidad.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar los riesgos de seguridad y privacidad de la información de todos los procesos de la entidad.
- Mejorar continuamente el sistema de gestión de seguridad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de información de la entidad y para la reducción de los riesgos.
- Asegurar el cumplimiento normativo y regulatorio en materia de seguridad y privacidad de la información, en concordancia con la legislación nacional e internacional aplicable.
- Promover la confidencialidad, integridad, disponibilidad y trazabilidad de la información como principios rectores de la gestión institucional.
- Fomentar la resiliencia organizacional frente a incidentes de seguridad, garantizando la continuidad de los servicios y procesos críticos de la Entidad.
- Consolidar la confianza de los usuarios y la ciudadanía, garantizando un manejo responsable, transparente y seguro de la información institucional y de terceros.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la **Entidad** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica 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. lo anterior, conforme lo previsto en el artículo 5 de la Resolución

00500 de 10 de marzo de 2021, expedida por MINTIC, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Así mismo manifiesta la importancia de la implantación, sostenibilidad y mejora continua de la Política de Seguridad y Privacidad de la Información, reconociendo que la protección de los activos de información es un pilar fundamental para el cumplimiento de la misión institucional, la generación de confianza ciudadana y la consolidación de un estado transparente y eficiente.

En este sentido, la Alta Dirección propende por asignar los recursos humanos, tecnológicos, financieros y logísticos necesarios para garantizar la adecuada implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como el cumplimiento de la normativa vigente, los estándares internacionales y los lineamientos de la Política de Gobierno Digital. Adicionalmente, promueve la participación activa de todos los funcionarios, contratistas y terceros vinculados, fomentando una cultura organizacional basada en la confidencialidad, la integridad, la disponibilidad y la trazabilidad de la información. De esta manera, la Entidad reafirma que la seguridad de la información no solo es un requisito normativo, sino un compromiso estratégico para la continuidad del servicio público y la resiliencia institucional.

Para la Entidad, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Entidad con respecto a la protección de los activos de información (los servidores públicos, contratistas, terceros, la información, los procesos, uso de hardware y el software), que soportan los procesos de la Entidad y sobre los cuales se basa la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) abarca el conjunto de procesos, recursos, tecnologías, personas y activos de información que intervienen en el tratamiento y protección de la información institucional, garantizando su confidencialidad, integridad y disponibilidad. Su alcance incluye todas las áreas organizacionales que gestionan información crítica o sensible, así como los servicios tecnológicos, plataformas, redes y sistemas de información utilizados para el cumplimiento de los objetivos misionales y administrativos.

El SGSI cubre tanto el entorno físico como digital, considerando los riesgos internos y externos que puedan afectar la seguridad de la información. Asimismo, incorpora controles técnicos, administrativos y legales, alineados con los lineamientos de la Norma ISO/IEC 27001, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normatividad vigente en materia de protección de datos, toda vez que se ampara con la Política de Tratamiento de la Información y datos personales SIP-PC-015. Este sistema aplica a funcionarios, contratistas, proveedores y demás partes interesadas que interactúan con los activos de información de la entidad.

7. APLICABILIDAD

La presente Política de Seguridad y Privacidad de la Información aplica de manera integral a todos los funcionarios, contratistas, terceros, proveedores y demás partes interesadas que, en el ejercicio de sus funciones o en el marco de una relación contractual con la Entidad, accedan, gestionen, procesen, consulten, almacenen, transmitan o compartan información institucional. Esta aplicabilidad también se extiende a las entidades de control y a cualquier organismo externo que, por su naturaleza o relación con la Entidad, interactúe con sus activos de información.

La política abarca no solo los lineamientos generales, sino también los manuales, procedimientos, instructivos y documentos complementarios que establecen el marco normativo y operativo necesario para garantizar la seguridad de la información en todos los niveles.

El incumplimiento de esta política o de cualquiera de sus disposiciones asociadas dará lugar a las sanciones y consecuencias legales contempladas en la normativa vigente de la Entidad, sin perjuicio de otras acciones administrativas o contractuales a que haya lugar. Esta política constituye un compromiso institucional para salvaguardar los derechos sobre la información, garantizar la continuidad del negocio y mitigar los riesgos que puedan afectar la operación y la confianza pública.

La aplicabilidad de esta política abarca todas las fases del ciclo de vida de la información, sin importar el medio, formato o tecnología utilizada para su gestión. En este sentido, incluye la información en estado físico, digital, en tránsito o almacenada, asegurando que se garantice su protección desde el momento de su creación o recolección, hasta su disposición final o eliminación segura. La Entidad establece que toda información, independientemente de su nivel de clasificación, debe ser tratada bajo los principios de confidencialidad, integridad, disponibilidad, de acuerdo con la normatividad nacional, las disposiciones internacionales aplicables y las mejores prácticas reconocidas en materia de seguridad de la información.

De igual forma, la política es aplicable a todos los procesos, proyectos, servicios y procedimientos desarrollados por la Entidad, tanto de carácter misional como de apoyo, garantizando que la seguridad de la información sea un componente transversal en la planeación, ejecución, seguimiento y mejora de cada actividad institucional. Esta aplicabilidad se extiende también a las tecnologías de información y comunicaciones, plataformas digitales, sistemas de información, aplicaciones, infraestructuras críticas, redes y dispositivos que soportan la operación de la Entidad, asegurando que la protección de la información esté alineada con los objetivos estratégicos y con la Política de Gobierno Digital.

Finalmente, la aplicabilidad de la presente política se fortalece con el compromiso de la Alta Dirección y con la corresponsabilidad de todos los servidores públicos, contratistas y terceros vinculados a la Entidad. La implementación efectiva de la misma exige el cumplimiento de las responsabilidades asignadas en materia de seguridad y privacidad de la información, la observancia de los lineamientos y protocolos establecidos, y la participación activa en actividades de sensibilización y capacitación. De esta manera, la Entidad asegura que la gestión de la seguridad de la información no sea vista únicamente como un requisito normativo, sino como un factor clave para la confianza institucional, la continuidad de los servicios y la transparencia en la gestión pública.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La Entidad, define los roles y responsabilidades para la implementación operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), como mecanismo institucional para la adopción del Modelo de Seguridad y Privacidad de la Información MSPI y el cumplimiento de los lineamientos de seguridad descritos en el manual de políticas y los demás documentos asociados.

ROLES / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos). • Recibir y revisar los resultados del seguimiento y evaluación del SGSI, y disponer las decisiones estratégicas necesarias para su mejora continua.
Comité de Gestión y Desempeño	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información. • Conocer, analizar y realizar seguimiento a los resultados del monitoreo y evaluación del SGSI, y definir las acciones de mejora correspondientes.
Proceso de Gestión TIC	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Seguridad Digital: Profesional Especializado de Gestión TIC y Dirección Administrativa y Financiera	• Estructurar, orientar, liderar la implementación de la política • Acompañar a las dependencias y/o procesos en la identificación y gestión de los riesgos de seguridad de la información. • Realizar seguimiento o monitoreo a la ejecución de los controles, lo anterior alineado a la Guía para la gestión integral del riesgo en entidades públicas. • Prestar asistencia técnica en el análisis de resultados • Establecer indicadores de gestión de calidad relacionados con seguridad de la información. • Atender los incidentes de Seguridad de la Información y ejecutar actividades de seguimiento. • Asesorar en materia de Seguridad de la Información a la entidad. • Planificar, coordinar y realizar el seguimiento, medición, análisis y evaluación periódica del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo la revisión de indicadores, el avance en la implementación del MSPI y el cumplimiento de la Política de Seguridad Digital, y presentar los resultados a la Alta Dirección y al Comité de Gestión y Desempeño para la toma de decisiones y mejora continua.

ROLES / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Talento Humano	• Promover y gestionar la toma de conciencia de los empleados y contratistas sobre sus responsabilidades en materia de seguridad de la información, verificando que estas sean formalmente comunicadas, aceptadas y cumplidas conforme a las políticas, lineamientos y procedimientos institucionales vigentes, en articulación con el proceso de Seguridad de la Información.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información. • Verificar, de manera independiente, la efectividad del SGSI y la correcta ejecución de los procesos de seguimiento y evaluación.
Comunicación	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
Dirección Administrativa y Financiera	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad y privacidad de la información definidos y aprobados.

9. REGLAMENTOS

a. Cualquier violación a las políticas de seguridad de la información de la **Entidad** debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. En el caso de contratistas, proveedores o terceros, se verificará el cumplimiento de sus obligaciones y adelantarán las acciones correspondientes, conforme lo acordado contractualmente y lo dispuesto en el ordenamiento jurídico.

c. Si se demuestra que el incumplimiento generó fuga, pérdida, alteración o uso indebido de información clasificada, reservada o personal, se podrá activar la correspondiente denuncia ante los órganos judiciales, en aplicación de la Ley 1273 de 2009 sobre delitos informáticos y otras normas que regulen la materia.

d. La Entidad se reserva el derecho de realizar auditorías, investigaciones internas o requerimientos de información a quienes hayan incumplido la política, como medida preventiva o correctiva, lo cual podría derivar en suspensión temporal del acceso a sistemas, redes o plataformas de información. Adicionalmente, en el caso de los servidores públicos, el jefe inmediato procederá a remitir el caso a la autoridad competente para lo de su competencia, de conformidad con lo establecido en la Ley 1952 de 2019 – Código General Disciplinario, y demás normas que regulen el régimen disciplinario de los empleados públicos.

10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

La Entidad, indica que realizará revisiones periódicas al SGSI. 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 FURAG o la herramienta definida para tal fin.

11. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Alta Dirección. 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 entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que conlleven a que la política requiera cambios.

4. Cuando se presenten actualizaciones o modificaciones en el marco normativo aplicable, con el fin de garantizar que la política se mantenga alineada con las disposiciones constitucionales, legales, reglamentarias y resolutivas, tanto externas como internas.

En este sentido, la política contará con un marco normativo de referencia, al cual podrán acudir quienes consulten el documento, que incluye la Constitución Política de Colombia, las leyes, decretos, resoluciones y lineamientos vigentes que regulan la seguridad y privacidad de la información en las entidades públicas:

Norma/Lineamiento	Descripción
Constitución Política de Colombia (1991)	Reconoce el derecho a la intimidad, al habeas data, y el acceso a la información (Artículos 15 y 20).
Ley 1581 de 2012	Regula la protección de datos personales y establece disposiciones generales para su tratamiento.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Ley 594 de 2000 (Ley General de Archivos)	Regula la organización, conservación y disposición de documentos públicos, asegurando su custodia y preservación.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC: incluye lineamientos de seguridad digital y gobierno electrónico.
Decreto 2106 de 2019	Establece disposiciones sobre la gestión digital y simplificación de trámites en el sector público.
Resolución 500 de 2021 (MinTIC)	Define lineamientos y estándares de la estrategia de seguridad digital y adopta el MSPI como habilitador del Gobierno Digital.
Política de Gobierno Digital (MinTIC)	Marco estratégico que establece directrices para la gestión de la información y seguridad digital en el sector público.
Modelo de Seguridad y Privacidad de la Información (MSPI)	Lineamientos de MinTIC que guían a las entidades públicas en la protección de la información.
ISO/IEC 27001 y 27002	Normas internacionales que definen los requisitos y buenas prácticas para la gestión de la seguridad de la información.

12. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	**CAMBIOS EFECTUADOS**	**FECHA DE CAMBIO**	**VERSIÓN**
Creación del documento	Creación del Documento	30/11/2017	001
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto a su estructura y contenido	25/09/2019	002
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto a su estructura y contenido, eliminando las acciones que no se ejecutan.	09/09/2021	003
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto al orden de numerales eliminando redundancias	27/11/2024	004
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se ajustaron el objetivo general y el alcance del documento; se incorporaron los objetivos específicos, el compromiso de la alta dirección, la aplicabilidad, los roles y responsabilidades. Asimismo, se eliminaron las políticas específicas, las cuales se encuentran documentadas en el Manual de Políticas de Seguridad.	19/06/2026	005