ACUERDO NÚMERO **019** **DE**

(**20 de mayo de 2026**)

Por cual se actualiza y aprueba la Política de Seguridad y Privacidad de la Información, de la Escuela Tecnológica Instituto Técnico Central

EL CONSEJO DIRECTIVO DE LA ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL – ETITC.

En uso de sus facultades legales, estatutarias y en especial la conferida en el artículo 14, literal "a" del Acuerdo 05 de 2013 del Consejo Directivo "Estatuto General", y

C O N S I D E R A N D O:

Que la Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones define los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso de la información pública, accesibilidad web, seguridad digital y datos abiertos.

Que, la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones establece 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.

Que, la Resolución 1951 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones establece los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.

Que, el Decreto 529 de 2024 modifica parcialmente el Capítulo 2 del Título 3 de la Parte 5 del Libro 2 del Decreto1075 de 2015 - Único Reglamentario del Sector Educación.

Que, la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".

Que, en la sesión del 5 de mayo de 2026 el Comité Institucional de Gestión y Desempeño validó propuesta presentada por la Rectoría de la Política de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central.

Que, en sesión ordinaria del 20 de mayo de 2026 el Consejo Directivo discutió y aprobó la propuesta presentada por la Rectoría de la Política de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central.

En mérito de lo anteriormente expuesto,

ACUERDA:

Artículo 1°-. Actualización. Se actualiza y aprueba la Política de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central, conforme a lo establecido en el artículo 14 literal a) del acuerdo 05 de 2013. Estatuto General vigente.

Artículo 2°-. Alcance. La Política de Seguridad y Privacidad de la Información es de obligatorio cumplimiento para todos los servidores públicos, personal administrativo, docentes, contratistas, proveedores, estudiantes y terceros que, en el ejercicio de sus funciones, actividades o relaciones contractuales, tengan acceso, administren, recolecten, procesen, almacenen, transmitan, intercambien, hagan tratamiento en nombre de la ETITC o gestionen activos de información, incluyendo datos personales. Así mismo la implementación del Modelo de Seguridad y Privacidad de la Información, conforme a los requisitos normativos, comprende a todos los procesos de la ETITC en sus distintas sedes.

Su aplicación se extiende a todos los procesos misionales, estratégicos, de apoyo y de evaluación; a los sistemas de información, infraestructura tecnológica, plataformas académicas, servicios en la nube, dispositivos institucionales o personales usados para fines laborales (cuando aplique), y cualquier otro medio físico o digital que soporte información de la ETITC, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información.

Ninguna persona o proceso está exento del cumplimiento de esta política, y su observancia deberá integrarse en la operación diaria, en la gestión de riesgos, gestión de proyectos, en la contratación y en la adopción de controles técnicos, administrativos, físicos y humanos que fortalezcan la protección de la información y de los datos personales.

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

Artículo 3°-. Anexo Único. El cuerpo de la Política de Seguridad y Privacidad de la Información forma parte integral del presente acto administrativo

Artículo 4°-. Socialización. Socializar el contenido del presente Acuerdo a través de los medios institucionales de la ETITC.

Artículo 5°-. Vigencia. El presente Acuerdo rige a partir de la fecha de su publicación y deroga el Acuerdo 12 de 2024.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dado en Bogotá, D.C., a los 20 días de mayo de 2026.

El Presidente Ad hoc del Consejo Directivo,

HNO. EDGAR FIGUEROA ABRAJIM

El Secretario del Consejo Directivo

EDGAR MAURICIO LÓPEZ LIZARAZO

Proyectó: Yaneth Jimena Pimiento Cortés, Profesional Aseguramiento de la Calidad.
Revisó: Edgar Mauricio López Lizarazo, Secretario General
Aprobó: Consejo Directivo

ANEXO ÚNICO

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer los lineamientos, principios y directrices de la Alta Dirección de la ETITC que permitan proteger adecuadamente los activos de información institucionales, incluyendo las bases de datos personales, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

2. Alcance

La Política de Seguridad y Privacidad de la Información es de obligatorio cumplimiento para todos los servidores públicos, personal administrativo, docentes, contratistas, proveedores, estudiantes y terceros que, en el ejercicio de sus funciones, actividades o relaciones contractuales, tengan acceso, administren, recolecten, procesen, almacenen, transmitan, intercambien, hagan tratamiento en nombre de la ETITC o gestionen activos de información, incluyendo datos personales. Así mismo la implementación del Modelo de Seguridad y Privacidad de la Información, conforme a los requisitos normativos, comprende a todos los procesos de la ETITC en sus distintas sedes.

Su aplicación se extiende a todos los procesos misionales, estratégicos, de apoyo y de evaluación; a los sistemas de información, infraestructura tecnológica, plataformas académicas, servicios en la nube, dispositivos institucionales o personales usados para fines laborales (cuando aplique), y cualquier otro medio físico o digital que soporte información de la ETITC, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información.

Ninguna persona o proceso está exento del cumplimiento de esta política, y su observancia deberá integrarse en la operación diaria, en la gestión de riesgos, gestión de proyectos, en la contratación y en la adopción de controles técnicos, administrativos, físicos y humanos que fortalezcan la protección de la información y de los datos personales.

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

3. Responsables

La ETITC, define los roles y responsabilidades para la organización de la seguridad de la información, la implementación del Modelo de Seguridad y Privacidad de la Información, MSPI, el cumplimiento de la norma NTC ISO/IEC 27001:2022, los lineamientos de seguridad y privacidad de la información y los demás documentos derivados (Manuales, Procedimientos, Guías, Planes, Formatos y otros documentos relacionados):

Área, proceso o instancia responsable	Descripción de responsabilidades o funciones
Alta Dirección	• Aprobar la política de seguridad y privacidad de la información y el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la asignación de los recursos necesarios para su implementación, operación y mejora continua (recursos económicos, tecnológicos y de talento humano). • Integrar la seguridad de la información en la estrategia institucional, realizar seguimiento periódico al desempeño del SGSI y promover una cultura organizacional orientada a la protección de la información.

Área, proceso o instancia responsable	Descripción de responsabilidades o funciones
Comité Institucional de Gestión y Desempeño	• Evaluar y aprobar los planes, indicadores e informes estratégicos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su articulación con la planeación institucional, la gestión del riesgo y las políticas del Modelo Integrado de Planeación y Gestión (MIPG). • Coordinar y articular entre las vicerrectorías, procesos, roles y recursos necesarios para garantizar la implementación operación, mejora continua y cumplimiento de la Política de Seguridad y Privacidad de la Información, en coherencia con el Modelo Integrado de Planeación y Gestión. • Aprobar, desde el nivel estratégico, los recursos, acciones y estrategias necesarios para la mitigación de los riesgos de seguridad y privacidad de la información, realizando especial seguimiento a los riesgos críticos garantizando su articulación con la planeación institucional, la gestión del riesgo y las políticas del MIPG. • Supervisar, desde el nivel estratégico, el cumplimiento del marco normativo institucional relacionado con la seguridad y la privacidad de la información. • Liderar la gestión de crisis de seguridad de la información y los procesos de continuidad del servicio. • Hacer seguimiento a la implementen de los controles y acciones establecidos en las políticas de gestión, incluidos los relacionados con seguridad y privacidad de la información por parte de los procesos y sus líderes. • Promover la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.
Gestión de Informática y Telecomunicaciones	• Implementar y administrarlos controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información y seguridad digital. • Gestionar la infraestructura tecnológica asegurando su disponibilidad, integridad y confidencialidad. • Administrar los accesos a sistemas de información y recursos tecnológicos. • Apoyar la gestión de incidentes de seguridad desde el componente tecnológico. • Identificar y gestionar los activos de información tecnológicos bajo su responsabilidad. • Aplicar controles de ciberseguridad de acuerdo con los lineamientos institucionales.
Profesional de Seguridad de la Información	• Liderar la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Sistema de Gestión de Seguridad de la Información (SGSI). • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Políticas, Manuales, Guías, instructivos, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la ETITC. • Asegurar la gestión para que los procesos y líderes de proceso identifiquen, analicen y gestionen los riesgos que afectan los activos de información bajo su responsabilidad, garantizando la actualización periódica del análisis de riesgos y la implementación de los controles definidos en el MSPI y la norma NTC ISO/IEC 27001:2022. • Asegurar que los activos de información sean identificados, gestionados y protegidos adecuadamente por sus responsables.

Área, proceso o instancia responsable	Descripción de responsabilidades o funciones
	• Liderar el proceso de atención de incidentes, incluyendo la identificación, reporte, análisis, respuesta y cierre; coordinar las actividades de los procesos involucrados (TI, Jurídica, Control Interno, etc.) y asegurar la definición e implementación de acciones correctivas y de mejora. • Asesorar a los procesos en la implementación de controles, gestión de riesgos y buenas prácticas de seguridad de la información. • Promover, coordinar y ejecutar las acciones necesarias para fortalecer la cultura institucional de seguridad y privacidad de la información en la ETITC. • Reportar el estado, desempeño y nivel de madurez del SGSI y del MSPI a la alta dirección y al Comité Institucional de Gestión y Desempeño.
Profesional de Protección de Datos Personales y de Continuidad	• Garantizar cumplimiento de la Ley 1581. • Administrar y supervisar los lineamientos en términos de tratamiento de datos. • Coordinar gestión de riesgos de privacidad. • Atender requerimientos de la SIC. • Registrar bases de datos. • Integrar privacidad con el SGSI. • Adelantar las gestiones necesarias para mantener y/o reanudar las actividades críticas durante y después de una interrupción.
Gestión de Talento Humano	• Programar los planes de concientización y sensibilización de seguridad de la información en el Plan Institucional de Capacitación. • Dar aplicación a los controles relacionados al recurso humano en seguridad de la información, de acuerdo con los lineamientos y procedimientos establecidos. • Gestionar la suscripción de acuerdos de confidencialidad y compromisos de protección de la información. • Incluir la seguridad de la información en los procesos de inducción, reinducción y formación institucional. • Aplicar los controles de seguridad asociados al recurso humano, de acuerdo con los lineamientos y procedimientos definidos en el SGSI. • Gestionar la desvinculación segura del personal, solicitando la revocación de accesos y la protección de la información institucional.
Oficina Asesora Jurídica	• Asesorar a la entidad en el cumplimiento del marco legal y normativo aplicable en materia de seguridad y privacidad de la información, protección de datos personales y acceso a la información pública. • Apoyar la gestión de incidentes de seguridad de la información que tengan implicaciones legales o regulatorias.
Gestión de Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Evaluar la efectividad de los controles del Sistema de Gestión de Seguridad de la Información (SGSI) y del Modelo de Seguridad y Privacidad de la Información (MSPI). • Emitir informes de auditoría sobre el estado de la seguridad de la información en la entidad. • Realizar seguimiento a los planes de mejora derivados de auditorías y evaluaciones. • Apoyar la verificación del cumplimiento normativo en materia de seguridad y privacidad de la información. • Apoyar en situaciones de posibles violaciones a la política o lineamientos de seguridad de la información.
Gestión de Comunicaciones	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la ETITC.

Área, proceso o instancia responsable	Descripción de responsabilidades o funciones
Gestión de Adquisiciones	• Incluir requisitos de seguridad de la información, confidencialidad y protección de datos en los contratos, convenios y procesos de adquisición. • 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.
Profesional de Aseguramiento de la Calidad	• Adelantar gestiones para que el Sistema de Gestión de Seguridad de la Información (SGSI) opere de forma coherente y articulada con los sistemas de gestión, con gestión documental, con la gestión de riesgo, promoviendo su interoperabilidad y evitando duplicidad de esfuerzos. • Recopilar, verificar y analizar la información estratégica generada por el SGSI, asegurando su incorporación en los informes institucionales y en los procesos de evaluación y mejora continua del SIACET. • Adelantar la gestión necesaria para que el SGSI cuente con los medios requeridos para su operación, gestión de riesgos, atención de auditorías, implementación de controles y programas de sensibilización, promoviendo su inclusión en los planes de acción del SIACET.
Líderes de Proceso (Propietarios de Activos)	• Implementar los lineamientos y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de riesgos, implementación de controles entre otros).
Todos los funcionarios y contratistas	• Cumplir a cabalidad con la política, lineamientos, manuales, guías y procedimientos de seguridad de la información definidos y aprobados. • Proteger la confidencialidad, integridad y disponibilidad de la información y los activos a los que tengan acceso. • Apoyar a los líderes de proceso en el desarrollo de tareas como implementación de controles para los activos de información y gestión de riesgos. • Reportar de manera oportuna incidentes o eventos de seguridad de la información. • Participar en programas de capacitación, formación y sensibilización en seguridad de la información. • Usar de manera adecuada y responsable los recursos tecnológicos y activos de información de la entidad.
Proveedores y Terceros	• Cumplir con la política de seguridad y privacidad de la información y los lineamientos establecidos por la entidad. • Proteger la confidencialidad, integridad y disponibilidad de la información y los activos a los que tengan acceso. • Implementar los controles de seguridad de la información acordados contractualmente. • Notificar de manera oportuna cualquier incidente o evento de seguridad de la información. • Permitir y facilitar la realización de auditorías, revisiones o verificaciones relacionadas con seguridad de la información. • Garantizar la devolución, eliminación o transferencia segura de la información y activos al finalizar la relación contractual.

4. Glosario

- **Activo de Información:** Conocimiento o información que tiene valor para la institución.
- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel de la entidad. Es la máxima autoridad en la institución.

- **Confidencialidad:** Asegurar que la información institucional, independientemente de su formato o medio, y en aquellos casos exceptuados por la Ley 1712 de 2014 sobre transparencia y acceso a la información pública, sea accesible únicamente por personas, procesos o sistemas autorizados. Este principio se extiende tanto a datos administrativos como académicos, investigativos y de terceros.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Asegurar que la información, los sistemas y los servicios que la soportan estén accesibles y operativos cuando los usuarios autorizados los requieran para el cumplimiento de las funciones misionales, académicas, administrativas e investigativas.
- **Exención:** Autorizar la no aplicación de un control o lineamiento de seguridad de la información, siempre que se encuentre debidamente justificado, documentado, evaluado en términos de riesgo, aprobado por la instancia competente y sujeto a revisión periódica.
- **Excepción:** Autorizar el cumplimiento parcial o temporal de un control o lineamiento de seguridad de la información, ante una situación específica, debidamente justificada, documentada y evaluada en términos de riesgo, con aprobación de la instancia competente.
- **Gestión del Riesgo:** Tomar decisiones con base en la identificación, análisis, evaluación y tratamiento de riesgos conforme a la Guía Departamento Administrativo de la Función Pública (DAFP) y los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información, asegurando la priorización de controles.
- **Integridad:** Asegurar que la información sea precisa, completa, consistente y esté protegida contra modificaciones no autorizadas, manteniendo la confiabilidad necesaria para la toma de decisiones institucionales.
- **Legalidad y Cumplimiento Normativo:** Dar cumplimiento a las leyes, reglamentos, políticas y estándares técnicos aplicables a la seguridad y privacidad de la información, incorporando buenas prácticas nacionales e internacionales dictadas en el MSPI, la norma NTC ISO/IEC 27001:2022 y los lineamientos del MinTIC.
- **Privacidad:** Proteger los datos personales conforme a la normatividad vigente, asegurando su tratamiento adecuado, proporcional, informado y orientado a la protección de los derechos de los titulares.
- **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 dentro de una entidad.

5. Principios

En la Escuela Tecnológica Instituto Técnico Central, la Política de Seguridad y Privacidad de la Información se basa en los siguientes principios:

En concordancia con los principios del Estado Social de Derecho, la transparencia, la responsabilidad, la ETITC y su alta dirección entienden la importancia y su obligación de velar por la seguridad de sus activos de información para el cumplimiento de su misión institucional, es así como 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 estudiantes, egresados, profesores, funcionarios administrativos, contratistas y ciudadanos en general.

6. Considerandos

6.1. Externos

- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Resolución 1519 de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso de la información pública, accesibilidad web, seguridad digital y datos abiertos.
- Resolución 500 de 2021. "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”.

- Norma NTC ISO 27001:2022: Sistema de Seguridad de la Información. Esta Norma Internacional proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.
- Directiva Presidencial No. 2 de 2022: "Reiteración de la Política Pública en Materia de Seguridad Digital".
- Decreto 767de 2022: "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo del Título 9 de la parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Resolución 1951 de 2022: "Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital".
- Ley 2294 de 2023: "Por el cual se expide el plan nacional de desarrollo 2022- 2026 Colombia potencia mundial de la vida".
- Decreto 0529 de 2024: "Por el cual se modifica parcialmente el Capítulo 2 del Título 3 de la Parte 5 del Libro 2 del Decreto1075 de 2015 - Único Reglamentario del Sector Educación".
- Resolución 02277 de 2025: "Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".

6.2. Internos

- Resolución 175 de 2018: "Por la cual se derogan las Resoluciones No. 581 del 28 de junio de 2011 y la 081 del 29 de febrero de 2017 y se crea el Comité Institucional de Gestión y Desempeño, en la Escuela Tecnológica Instituto Técnico Central".
- Resolución 169 del 29 de marzo de 2019: "Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión - MIPG en la Escuela Tecnológica Instituto Técnico Central y se definen otras políticas institucionales".
- Acuerdo 012 de 2024: "Por el cual se actualiza y aprueba la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, de la Escuela Tecnológica Instituto Técnico Central.

7. Desarrollo

7.1 Compromiso de la Alta Dirección

La Alta Dirección de la Escuela Tecnológica Instituto Técnico Central 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.

7.2 Objetivo del SGSI

Implementar, mantener y mejorar un sistema de gestión de seguridad de la información y privacidad de la información que permita cumplir con la obligación institucional de preservar la confidencialidad, integridad y disponibilidad de la información en todos sus procesos, servicios y sistemas, como parte de la estrategia de Gobierno Digital para proteger los derechos de los ciudadanos y fortalecer la confianza en la ETITC mediante la adecuada gestión de riesgos, el cumplimiento de los requisitos normativos, la implementación de controles y definición de responsabilidades.

7.2.1 Objetivos específicos del SGSI

- Gestionar los riesgos de seguridad y privacidad de la información de manera sistemática y documentada.
- Fortalecer la cultura en seguridad y privacidad de la información en la ETITC.
- Planear y proponer los controles y mecanismos tecnológicos, físicos, administrativos y humanos que protejan los activos de información, incluyendo bases de datos personales.
- Gestionar los incidentes de seguridad y privacidad de la información mediante una estrategia estructurada de identificación, reporte, análisis, respuesta y cierre, que permita mitigar su impacto.

7.3 Sanciones

Cualquier violación a la política de seguridad y privacidad de la información de la ETITC o de sus lineamientos, en el marco del debido proceso y demás garantías constitucionales, será objeto de las actuaciones legales que correspondan de conformidad con legislación y reglamentación vigente, que conduzcan a establecer la responsabilidad a que haya lugar.

7.4 Seguimiento, Medición, Análisis y Evaluación del SGSI

El Comité Institucional de Gestión y Desempeño 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 (MSPI) del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG.

Para la implementación de esta política se debe elaborar un plan de trabajo anual con responsables y cronograma. El seguimiento lo realiza la oficina Asesora de Planeación y Desarrollo Institucional.

7.5 Gestión de excepciones o exenciones

Esta política se articulada con el Manual de Lineamientos de Seguridad y Privacidad de la Información, el cual establece los principios, directrices, excepciones y controles generales que orientan la gestión de la seguridad de la información en la ETITC.

Toda excepción o exención a la aplicación de los controles definidos en dicho manual deberá estar debidamente justificada, documentada y autorizada por la instancia competente. Estas situaciones se evaluarán con base en un análisis de riesgos de seguridad de la información, requerirán la aprobación de la Alta Dirección cuando aplique y serán revisadas periódicamente, con el fin de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

8. Control de Cambios

Fecha	Versión	Cambios
8/07/2016	1	Adopción de la política.
14/09/2017	2	Se añade la fila Etiqueta en la página principal del documento.
19/04/2017	3	La Política General de Seguridad de la Información se alinea con los requisitos contenidos en las cláusulas de la 4 a la 10, de la norma ISO 27001:2013.
01/04/2019	4	Ingreso al Sistema de Gestión de Calidad Modificaciones en el contenido de la Política General de Seguridad de la Información, acorde al habilitador transversal de Seguridad de la Información de Gobierno Digital.
26/07/2024	5	Actualización de toda la política con base en la estructura y los criterios de la norma NTC ISO 27001:2022.
20/05/2026	6	Se actualiza política para su alineación a la resolución 02277 de 2025 del MinTIC, a nivel de Nombre de la política, Objetivo, Compromiso, Alcance, inclusión y formalización de la gestión de excepciones y exenciones, fortalecimiento de los roles y responsabilidades y Sanciones.

Elaboró: Profesionales de Seguridad de la Información
Revisó: Angela Adriana Pulido Rivera. Profesional de Ciberseguridad
Erika Viviana Chacón Gamba, Profesional de Continuidad y Datos Personales
Yaneth Jimena Pimiento Cortés, Profesional Aseguramiento de la Calidad
Validó: Comité Institucional de Gestión y Desempeño.
Aprobó: Consejo Directivo