MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ETITC

Contenido

1. OBJETIVO DEL MANUAL

Establecer los lineamientos operativos, técnicos y de gestión que permitan implementar y mantener el Sistema de Gestión de Seguridad de la Información de la ETITC, definiendo responsabilidades, controles y medidas de protección para garantizar la confidencialidad, integridad, disponibilidad y uso adecuado de los activos de información, promoviendo la gestión del riesgo, el cumplimiento normativo y la cultura de seguridad institucional.

2. ALCANCE DEL MANUAL

El presente Manual de lineamientos de Seguridad de la Información aplica a todos los funcionarios, docentes, contratistas, aprendices, proveedores, consultores, terceros y visitantes que, por cualquier motivo, tengan acceso, interacción, manipulación, administración, procesamiento, almacenamiento, transmisión o uso de los activos de información de la Escuela Tecnológica Instituto Técnico Central (ETITC). Este alcance cubre tanto a las personas como a los procesos, tecnologías, entornos físicos, ambientes digitales y servicios externos que intervienen en el ciclo de vida de la información institucional.

El manual es de carácter obligatorio y comprende todas las dependencias, áreas y procesos misionales, estratégicos, tácticos y de apoyo de la ETITC, independientemente del tipo de vínculo laboral o contractual. Así mismo, aplica a los recursos tecnológicos, plataformas, sistemas de información, redes, dispositivos, infraestructura física y lógica, así como a cualquier medio mediante el cual se gestione información institucional, sin importar su formato (digital, físico, audiovisual, verbal o cualquier otra forma registrada o no registrada). Este alcance asegura que todas las personas bajo la responsabilidad de la ETITC cumplan los lineamientos establecidos y adopten las medidas necesarias para proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad en coherencia con la Política General de Seguridad de la Información y el SGSI institucional.

3. DEFINICIONES

- **Acceso lógico**: restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como identificación, autenticación y autorización
- **Activo de información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la Entidad.

- **Acuerdo de confidencialidad:** Es un documento, en los que los servidores públicos de la ETITC manifiestan su voluntad de mantener la confidencialidad de la información comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan.
- **Alerta de seguridad**: aviso que informa sobre un problema o riesgo que podría afectar un sistema, como fallas, errores o situaciones que alguien podría aprovechar. Puede presentarse como un boletín o comunicado para alertar y orientar sobre las acciones necesarias.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- **Análisis de riesgos de seguridad de la información:** Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad 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**: Permitir que algo o alguien acceda solamente a lo que le es permitido.
- **Ataque:** Cualquier tipo de actividad maliciosa que intente obtener acceso no autorizado a los servicios, recursos o información del sistema; comprometer la seguridad de la información o interrumpir, denegar o degradar los recursos del sistema de información.
- **Base De Datos:** es un conjunto de datos almacenados sistemáticamente y que son consultados mediante un sistema de información
- **Campus Virtual:** es una plataforma digital en línea que permite desarrollar actividades de enseñanza y aprendizaje a través de Internet. En ella, estudiantes y docentes pueden acceder a materiales educativos, realizar tareas, presentar evaluaciones, participar en foros y comunicarse de manera virtual.
- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- **Cibercrimen (Delito Cibernético):** conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).
- **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.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Criptografía:** Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
- **Custodio de la información:** es la persona o rol responsable de administrar, proteger y garantizar el uso adecuado de la información bajo las directrices definidas por el Dueño del Activo.
- **Derechos de autor:** Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Directriz:** Es una norma o una instrucción que se tiene en cuenta para realizar una tarea. También se trata de aquello que fija cómo se producirá algo. Las directrices, por lo tanto, sientan las bases para el desarrollo de una actividad o de un proyecto.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Dueño del activo:** es la persona, rol o área que tiene la autoridad y responsabilidad final sobre un activo de información. Es quien determina su valor, su criticidad, los niveles de protección requeridos, y cómo debe usarse, almacenarse y compartirse**.**
- **Entorno digital:** ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).
- **Entorno digital abierto:** entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

- **Equipo de cómputo:** Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Evento de seguridad:** Ocurrencia de una situación que tiene posibles implicaciones de seguridad potenciales para el sistema, la información o su entorno y que puede requerir una acción adicional (monitorear, investigar o reaccionar).
- **Incidente de seguridad:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Licencia de software:** Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **MFA(Autenticación multifactor):** Método de autenticación que requiere la validación de dos o más factores independientes para verificar la identidad de un usuario antes de conceder acceso a un sistema o recurso.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Perfiles de usuario:** Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información, a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Propiedad intelectual:** Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
- **Propietario de la información:** es la persona, rol o área responsable de establecer el valor, la clasificación, las reglas de uso y los requisitos de protección de la información bajo su control. Es quien toma decisiones sobre la información: cómo debe ser tratada, quién puede acceder, cómo se protege y qué controles aplican.

- **Recursos tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la entidad**.**
- **RPO (Recovery Point Objective):** Objetivo de Punto de Recuperación es la cantidad máxima de datos que una organización está dispuesta a perder después de una interrupción, falla o desastre. Se mide en tiempo.
- **RTO (Recovery Time Objective):** Tiempo máximo aceptable para restablecer un sistema, servicio o proceso después de una interrupción.
- **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.
- **Sistema de información**: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la ETITC o de origen externo, ya sea adquirido por el Instituto como un producto estándar de mercado o desarrollado para las necesidades de éste.
- **Software malicioso**: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Playbook:** Complementan a la Gestión de Incidentes, ya que definen las líneas de acción específicas para cada tipología de incidente.
- **Resiliencia:** es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).
- **Riesgo:** probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactando los objetivos de la Entidad.
- **Riesgo de seguridad digital:** es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que pueden afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

- **Terceros:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a La ETITC.
- **Vulnerabilidad:** es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. Punto en el cual un recurso es susceptible de ataque. (CONPES 3854, pág. 87).
- **VPN: (Virtual Private Network):** Red Privada Virtual es una tecnología que crea una conexión segura y cifrada entre un dispositivo y una red a través de Internet.

4. LINEAMIENTOS

La Escuela Tecnológica Instituto Técnico Central (ETITC) establece los presentes lineamientos de Seguridad de la Información como disposiciones obligatorias para todos los funcionarios, docentes, contratistas, proveedores, terceros, usuarios y visitantes que, en el ejercicio de sus funciones o actividades, accedan, utilicen, procesen o interactúen de cualquier forma con los activos de información institucionales. Estos lineamientos complementan la Política General de Seguridad de la Información y constituyen un marco normativo fundamental para garantizar la protección integral de la información bajo la responsabilidad de la entidad.

El incumplimiento, desconocimiento o vulneración de las Políticas y Lineamientos de Seguridad de la Información será objeto de análisis, investigación y aplicación de medidas correctivas y sancionatorias, conforme al marco normativo institucional y legal vigente.

Así mismo, las faltas que puedan comprometer la integridad de los sistemas de información, ocasionar daños, exponer datos personales o vulnerar la infraestructura tecnológica podrán ser elevadas a instancias administrativas, contractuales, fiscales, civiles o penales, según la naturaleza del incidente y la normativa aplicable.

Los lineamientos que se exponen a continuación se encuentran organizados por temáticas estratégicas y operativas, definidas a partir del análisis del contexto interno y externo de la entidad, la estructura organizacional, los riesgos identificados, las funciones institucionales y los requerimientos del Sistema de Gestión de Seguridad de la Información (SGSI). Cada temática establece las directrices necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información institucional, garantizando el cumplimiento normativo y la adecuada gestión de los riesgos de seguridad:

4.1 LINEAMIENTO DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La ETITC establecerá, mantendrá y fortalecerá una estructura organizacional de Seguridad de la Información que garantice el liderazgo, la coordinación, la toma de decisiones, la asignación de responsabilidades y la supervisión efectiva del Sistema de Gestión de Seguridad de la Información (SGSI). La entidad asegurará que la Alta Dirección ejerza el direccionamiento estratégico, proporcionando los recursos humanos, técnicos, financieros y administrativos necesarios para la gestión de los riesgos de seguridad y la protección de los activos de información institucionales.

La Entidad deberá definir roles, responsabilidades y autoridades específicas en materia de seguridad de la información, e incluirlos en la Política de Seguridad y Privacidad de la Información, de la Escuela Tecnológica Instituto Técnico Central, cada uno deberá cumplir funciones claras orientadas a la preservación de la confidencialidad, integridad y disponibilidad.

El lineamiento establece que la Seguridad de la Información debe integrarse de manera transversal en todos los procesos de la Escuela, garantizando que las decisiones institucionales incluyan la evaluación de riesgos, el cumplimiento normativo y la implementación de controles adecuados. La Escuela adoptará mecanismos formales de comunicación, escalamiento, monitoreo y reporte, asegurando la coordinación permanente entre Talento Humano, Jurídica, Control Interno, Gestión de TI, Gestión de Adquisiciones, Gestión documental, Gestión de Comunicaciones y demás áreas relevantes.

La ETITC gestionará y realizará seguimiento al Sistema de Gestión de Seguridad de la Información (SGSI) a través del Comité Institucional de Gestión y Desempeño. En este comité se revisarán periódicamente aspectos relacionados con el desempeño del SGSI, el estado de los riesgos de seguridad de la información, los incidentes de seguridad, los resultados de auditorías, el cumplimiento de controles y las oportunidades de mejora.

La Alta Dirección garantizará que los temas de seguridad de la información y privacidad de los datos sean tratados en el Comité Institucional de Gestión y Desempeño, promoviendo la toma de decisiones, la asignación de recursos y la priorización de iniciativas alineadas con la misión, los objetivos estratégicos y las actividades institucionales.

Este lineamiento exige que la institución promueva una cultura organizacional orientada a la protección de la información, establezca principios de responsabilidad y rendición de cuentas y asegure que su estructura organizacional soporte la operación efectiva del SGSI,

el cumplimiento normativo y la protección integral de los activos de información bajo su administración.

4.2 LINEAMIENTO DE SEGURIDAD DE LOS RECURSOS HUMANOS

La ETITC garantizará que la seguridad de la información sea incorporada en todas las etapas del ciclo de vida del talento humano —desde la selección, vinculación, permanencia y terminación de la relación laboral o contractual— con el fin de asegurar que todo el personal conozca y cumpla las responsabilidades derivadas del uso, acceso y protección de los activos de información institucionales.

a) Controles previos a la vinculación

- Durante los procesos de selección de personal de planta, contratistas, docentes, aprendices en práctica y cualquier tercero con acceso potencial a los activos de información, se realizarán verificaciones de antecedentes disciplinarios, fiscales, contractuales y, cuando corresponda, antecedentes judiciales, independientemente del cargo, nivel o naturaleza del rol.
- Estas verificaciones se efectuarán siguiendo los principios de legalidad, proporcionalidad y protección de datos personales, con el fin de asegurar que el personal seleccionado cumpla los requisitos definidos por la organización para el desempeño de funciones, de acuerdo con su nivel de criticidad.

b) Compromisos formales de seguridad

- Todo el personal que labore o preste servicios a la ETITC deberá firmar de manera obligatoria el GSI-SI-FO-01 Compromiso de Confidencialidad en cuanto al uso y divulgación de información de la ETITC.
- Estos documentos tendrán vigencia durante toda la relación laboral o contractual, y sus obligaciones de confidencialidad continuarán incluso después de la terminación del vínculo.

c) Responsabilidad y comportamiento esperado

- Todo personal de planta, contratistas, docentes, aprendices en práctica y cualquier tercero con acceso potencial a los activos de información deberá comprometerse a realizar un uso adecuado, responsable y seguro de los sistemas, recursos tecnológicos y activos de información de la ETITC, acatando los controles, procedimientos y restricciones definidos por la institución.

- Se exigirá el cumplimiento de conductas éticas, profesionales y de protección activa de la información, incluyendo la notificación inmediata de incidentes, fallas, accesos indebidos o comportamientos sospechosos.

d) Articulación con Talento Humano

- El Proceso de Talento Humano y Gestión de Adquisiciones deberá:
  - Incorporar estos compromisos en los procesos de inducción y reinducción.
  - Garantizar que todo el personal reciba capacitación inicial sobre seguridad de la información antes de adquirir acceso a los activos institucionales.
  - Mantener los registros de todos los acuerdos firmados y asegurar su disponibilidad como parte del SGSI.

Estos lineamientos buscan asegurar que únicamente personal confiable, informado y responsable tenga acceso a los activos de información institucionales, mitigando riesgos asociados a errores humanos, negligencia, fraude interno o divulgación no autorizada.

4.2.1 ANTES DE ASUMIR EL EMPLEO

La ETITC garantizará antes de iniciar cualquier tipo de vinculación laboral, contractual o de prestación de servicios, que todo servidor público, contratista, proveedor o tercero deberá cumplir los requisitos previos establecidos por la entidad en materia de seguridad de la información, incluyendo la firma de acuerdos de confidencialidad y aceptación de políticas, la validación de requisitos de acceso a los sistemas y activos de información, y el cumplimiento de los procesos institucionales de verificación y habilitación. Ninguna persona podrá acceder a información, recursos tecnológicos o instalaciones de la ETITC hasta haber completado estos requisitos y haber sido formalmente autorizada conforme a los lineamientos del SGSI.

4.2.2 DURANTE LA EJECUCION DEL EMPLEO

La ETITC garantizará durante la ejecución del empleo, que todas las personas vinculadas a la entidad incluyendo servidores públicos, personal administrativo, docentes, contratistas, proveedores y terceros, deberán cumplir de manera estricta las políticas, procedimientos, lineamientos y controles establecidos en materia de seguridad de la información.
Los funcionarios, docentes, contratistas, proveedores, terceros y usuarios debe proteger los activos de información bajo su responsabilidad, utilizar los sistemas y recursos institucionales exclusivamente para los fines autorizados, conservar la confidencialidad de la información a la que tengan acceso, mantener la integridad y disponibilidad de los recursos tecnológicos, participar en los programas de capacitación y sensibilización que la

institución disponga, reportar de manera inmediata cualquier incidente, anomalía o sospecha de vulneración, y aplicar las buenas prácticas de manejo seguro de la información. El incumplimiento de estas disposiciones podrá dar lugar a acciones disciplinarias, administrativas, contractuales o legales conforme a la normativa vigente y al SGSI de la ETITC.

4.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO

Los funcionarios, docentes, contratistas, proveedores y terceros al finalizar la relación laboral, contractual o en situaciones de cambio de rol dentro de la Escuela, deberá cumplir con los lineamientos establecidos (GIT-PC-15 Vinculación y/o desvinculación de Acceso a los Sistemas de Información) para la devolución, revocación y actualización de accesos, activos y permisos asociados a su posición, garantizando la protección de la información institucional.

El colaborador debe devolver equipos, dispositivos, credenciales, documentación o cualquier recurso asignado, así como firmar los documentos de terminación correspondientes; los accesos lógicos y físicos deberán ser deshabilitados de manera inmediata por las áreas responsables; cualquier información, copia, archivo o recurso digital deberá ser eliminado o entregado según las directrices del SGSI; y se prohíbe retener, divulgar o utilizar información institucional con posterioridad al retiro.

En los casos de cambio de empleo o reasignación de funciones, los accesos y privilegios deberán ser ajustados conforme al nuevo rol, aplicando el principio de mínimo privilegio y la autorización del Dueño del Activo o Propietario de la Información. El incumplimiento de estas disposiciones podrá acarrear sanciones disciplinarias, contractuales o legales según la normatividad vigente y los lineamientos de la ETITC. Ante cualquier novedad en la vinculación de un funcionario, incluyendo la terminación contractual, cambios de rol o cualquier otra modificación de su relación laboral, el área de Talento Humano, el supervisor, el líder del proceso o quien haga sus veces deberá informar oportunamente al área de TI para gestionar la desactivación de los accesos a los sistemas de información.

4.2.4 LINEAMIENTO DE SEGURIDAD DE LA COMUNIDAD ESTUDIANTIL

Para otorgar acceso a los recursos tecnológicos y de información de la ETITC, se deberán implementar los siguientes controles:

a) Controles previos al ingreso

La ETITC implementará controles con el fin de que los estudiantes conozcan y cumplan los lineamientos de seguridad de la información antes de acceder a los recursos institucionales. Para ello:

- Se asignarán cuentas y accesos institucionales de acuerdo con la condición académica del estudiante.
- Se divulgarán las políticas de seguridad de la información y uso aceptable de los recursos tecnológicos.
- Se informará sobre los canales de reporte de incidentes de seguridad y protección de datos personales.

b) Compromisos formales de seguridad

- Todo estudiante que acceda a sistemas, plataformas o información institucional deberá:
- Utilizar los recursos tecnológicos únicamente para fines académicos e institucionales.
- Proteger sus credenciales de acceso y no compartirlas con terceros.
- Respetar la confidencialidad de la información a la que tenga acceso.
- Cumplir con los lineamientos institucionales de seguridad de la información y protección de datos personales.

c) Responsabilidad y comportamiento esperado

- Los estudiantes son responsables del uso adecuado y seguro de los recursos tecnológicos de la ETITC. En consecuencia, deberán:
- Proteger la información institucional y sus datos personales.
- Reportar incidentes, vulnerabilidades o actividades sospechosas que puedan afectar la seguridad de la información.
- Hacer uso responsable de los equipos, laboratorios, redes y plataformas institucionales.

- Abstenerse de realizar actividades no autorizadas que comprometan la confidencialidad, integridad o disponibilidad de la información.

d) Articulación con bienestar universitario, registro y control académico y seguridad de la información

Las dependencias responsables coordinarán con Gestión de Informática y Telecomunicaciones la gestión de accesos, el tratamiento de incidentes de seguridad y la actualización o revocación de permisos cuando se presenten cambios en la condición académica del estudiante o finalice su vínculo con la Institución.

4.3 LINEAMIENTO DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

La ETITC establecerá y mantendrá un marco integral para la identificación, clasificación, uso, protección y administración de los activos de información, garantizando que dichos activos sean gestionados durante todo su ciclo de vida conforme a los principios de confidencialidad, integridad, disponibilidad.

a) Propiedad institucional de los activos

Toda información en formato físico, digital, audiovisual, verbal, impreso, electrónico o cualquier otro medio que sea generada, procesada, almacenada, transmitida o transformada por funcionarios, contratistas, docentes, proveedores o terceros utilizando recursos institucionales o en desarrollo de sus funciones, constituye un activo de información propiedad exclusiva de la ETITC.

Esto incluye información creada fuera de la infraestructura institucional cuando esté asociada a funciones o actividades oficiales.

b) Uso autorizado y propósito legítimo

Los activos provistos por la ETITC equipos, software, sistemas de información, cuentas, accesos, infraestructura, redes, dispositivos y medios de almacenamiento) deberán utilizarse exclusivamente para fines institucionales, en el marco de las responsabilidades laborales, contractuales o académicas.

Queda prohibido su uso para actividades personales, no autorizadas, fraudulentas o ajenas a los objetivos de la entidad.

El acceso o manipulación de activos deberá estar basado en:

- Necesidad de conocer (“need to know”).
- Función del cargo u actividades
- Principio de privilegios mínimos.
- Autorización formal y controlada.

c) Inventario, identificación y responsabilidad

El responsable de Seguridad de la Información debe establecer, mantener y actualizar una matriz formal de activos, gestionado de acuerdo con los manuales, procedimientos y registros establecidos, asumiendo el rol orientador metodológico, consolidador.

Es necesario resaltar que la responsabilidad del reporte y/o actualización del inventario de activos debe estar a cargo del propietario de los activos o responsable del proceso, este deberá realizarse como mínimo una vez al año o cada vez que se presente un cambio significativo relacionado con la creación, adquisición, modificación, traslado, reasignación, baja o retiro de un activo de información.

Para cada activo se deberá definir:

- Propietario del activo (responsable funcional/administrativo).
- Custodio del activo (responsable técnico/operativo).
- Tipo de activo, ubicación, criticidad y sensibilidad.
- Controles aplicables según la clasificación y el nivel de riesgo.

El propietario del activo será responsable de:

- Validar su clasificación.
- Autorizar accesos.
- Definir requisitos de protección.
- Reportar cambios, incidentes o riesgos asociados.

- **Caracterización de sistemas de información:**

Con base en el inventario de activos de información clasificado, la ETITC deberá mantener una caracterización formal de cada sistema de información, la cual incluirá, como mínimo: objetivo y alcance del sistema, propietario y custodio, clasificación y sensibilidad de los datos tratados, criticidad para los procesos institucionales, dependencias e interfaces, requisitos normativos aplicables, controles mínimos de seguridad, necesidades de continuidad, y repositorios autorizados para la gestión documental. Esta caracterización deberá actualizarse cuando se presenten cambios en los procesos, datos tratados, arquitectura, proveedores o resultados derivados de auditorías y gestión de riesgos.

d) Clasificación y tratamiento según sensibilidad

La información institucional deberá clasificarse de acuerdo con su naturaleza, sensibilidad, impacto y requisitos legales/contractuales, conforme a los lineamientos del SGSI y a la metodología GSI-SI-ME-01 Identificar, Clasificar y Valorar los Activos de Información de la ETITC.

La clasificación deberá permitir la implementación de controles según:

- Nivel de confidencialidad.
- Impacto en caso de alteración o pérdida.
- Obligaciones legales (datos personales, información pública, datos sensibles, etc.).

e) Protección durante todo el ciclo de vida

La ETITC aplicará controles para garantizar la seguridad de los activos desde su creación hasta su disposición final, incluyendo:

- Almacenamiento seguro.
- Accesos controlados.
- Seguridad física y lógica.
- Protección criptográfica cuando corresponda.
- Eliminación o destrucción segura en su disposición.

f) Seguimiento

La ETITC deberá asegurar la revisión periódica del inventario de activos de información, su adecuada clasificación y el cumplimiento de acuerdo con los lineamientos establecidos en el GSI-SI-ME-01 Metodología para identificar, clasificar y valorar los activos de información.

4.4 LINEAMIENTO DE CUMPLIMIENTO

La ETITC deberá asegurar el cumplimiento integral permanente de todos los requisitos legales, regulatorios, contractuales y normativos relacionados con la seguridad de la información, garantizando que el tratamiento de los datos, la gestión tecnológica, los servicios prestados, las relaciones con terceros, el uso de los activos institucionales y las actividades institucionales se realicen conforme a las disposiciones vigentes y a las políticas internas del SGSI; las áreas, funcionarios, contratistas y proveedores deberán acatar estrictamente estas obligaciones, someterse a procesos de auditoría, verificación y revisión de cumplimiento, así como implementar acciones correctivas o preventivas ante cualquier desviación identificada; queda prohibido cualquier uso, acceso, divulgación o tratamiento de la información que contravenga la normativa aplicable, los compromisos contractuales o los lineamientos institucionales, debiendo reportarse de inmediato cualquier incumplimiento para gestionar las medidas disciplinarias, administrativas o legales correspondientes.

Obligación de cumplimiento normativo específico:

La ETITC garantizará de manera permanente el cumplimiento del marco legal, regulatorio y normativo aplicable en materia de seguridad de la información, seguridad digital y privacidad, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Sistema de Gestión de Seguridad de la Información (SGSI) y los lineamientos de Gobierno Digital, incluyendo, entre otros:

- Seguridad y privacidad de la información.
- Protección de datos personales (Ley 1581 de 2012 y normas concordantes).
- Derechos de autor y propiedad intelectual.
- Delitos informáticos y uso indebido de medios tecnológicos (Ley 1273 de 2009).
- Transparencia, acceso a la información pública y datos abiertos (Ley 1712 de 2014 y normas complementarias).

- Normativa de seguridad digital, ciberseguridad y lineamientos del MinTIC (Resolución 500 de 2021, Resolución 02277 de 2025 y demás disposiciones aplicables).
- Requisitos contractuales y regulatorios que regulen la custodia, tratamiento, intercambio o transferencia de información.

El cumplimiento de estos requisitos será gestionado de manera articulada entre las diferentes instancias institucionales, de acuerdo con sus roles y responsabilidades definidos en la Política de Seguridad y Privacidad de la Información, en especial la Alta Dirección, el Comité Institucional de Gestión y Desempeño, la Oficina Jurídica, Control Interno, Talento Humano, Gestión de Adquisiciones, Gestión Documental y el Proceso de Gestión de Informática y Telecomunicaciones, bajo el liderazgo del SGSI.

Esta articulación garantizará que la seguridad de la información se administre con criterios de legalidad, gestión del riesgo, trazabilidad, responsabilidad, mejora continua e integración con el Modelo Integrado de Planeación y Gestión (MIPG).

a) Escritorio limpio:

La ETITC garantizará que los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas, que tengan acceso a las instalaciones físicas, sistemas de información y equipos de cómputo, mantengan sus escritorios libres de documentos o dispositivos de almacenamiento, guardándolos en sitios seguros, durante la jornada laboral y después de la misma, a su vez, mantengan el escritorio de los equipos de cómputo libres de documentación sensible y accesos directos.

- No deberán dejarse documentos con información clasificada o sensible en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo, es importante que bloqueen los equipos de cómputo para garantizar la seguridad de la información. Una forma común de hacerlo es utilizando la combinación de teclas Win + L. Esta acción activa la función de bloqueo de pantalla y requiere una contraseña para desbloquear el equipo, evitando el acceso no autorizado.
- Es recomendable utilizar cajoneras o archivadores con llave para almacenar de forma segura la información sensible o crítica
- No deben ingerir alimentos o bebidas cerca de equipos de cómputo, documentación física y medios magnéticos, así como, evitar manipular líquidos en su cercanía.

- Retirar de las impresoras, escáner y fax, toda documentación física, evitando de esta manera la exposición de la información a personal no autorizado.

b) Uso adecuado de internet:

El internet es un recurso valioso para el desempeño de las labores de todos los los funcionarios, docentes, contratistas, proveedores, terceros, usuarios y visitantes, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales como Facebook, WhatsApp, Instagram, Twitter, plataformas o servicios que expongan datos institucionales.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional Office 365).
- La utilización de modos de navegación privada, incógnita o cualquier funcionalidad similar disponible en los navegadores web institucionales deberá estar restringida o deshabilitada.
- Mantener buenas prácticas de navegación segura, y reportar inmediatamente cualquier sitio sospechoso comportamiento anómalo o posible incidente.
- Todo uso de Internet estará sujeto a monitoreo y controles técnicos establecidos por el SGSI, y el incumplimiento de estas directrices podrá derivar en medidas disciplinarias, contractuales o legales según corresponda.
- El Proceso de Gestión de Información y Telecomunicaciones (TI) podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

c) Uso adecuado de correo electrónico:

- Los buzones de correo asignados a los funcionarios, contratistas o partes interesadas pertenecen a La ETITC, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- Las cuentas de correo electrónico institucional asignadas a estudiantes son de uso exclusivo para fines académicos y estarán vigentes únicamente mientras el

usuario mantenga la condición de activo en la ETITC. Al adquirir la condición de egresado, retirarse, cancelar matrícula o perder la calidad de estudiante, el acceso al correo institucional y a los servicios asociados a la cuenta serán deshabilitado conforme a los procedimientos establecidos por la Entidad.

- Todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas deben utilizar el control MFA para todos los accesos, utilizando (token, SMS, app de autenticación) para su correo institucional.
- El Proceso de Gestión de Información y Telecomunicaciones (TI) podrá verificar el contenido de los buzones de los correos electrónico en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.
- El área de TI podrá bloquear, aislar o eliminar correos, adjuntos o archivos que sean identificados como maliciosos, sospechosos o potencialmente peligrosos, sin requerir autorización previa del dueño de la información, con el fin de proteger la infraestructura tecnológica y los activos institucionales.
- Todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas deberán abstenerse de abrir enlaces o adjuntos de origen desconocido, reportar de inmediato cualquier actividad sospechosa y cumplir con las medidas técnicas y procedimientos establecidos por el SGSI.

d) Uso de contraseñas y usuarios:

- Cada funcionario, contratista o terceros cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña siguiendo los lineamientos institucionales establecidos para ello.
- Las credenciales son personales e intransferibles.
- Queda estrictamente prohibido compartir, divulgar, enviar o almacenar contraseñas o credenciales de acceso por cualquier medio, incluyendo, pero no limitado a correo electrónico, herramientas de mensajería (como Teams, WhatsApp u otras), documentos digitales o físicos. En caso de requerirse restablecimiento o asignación de credenciales, este deberá realizarse únicamente a través de los mecanismos formales y seguros definidos por la ETITC.
- Asimismo, está prohibido mantener contraseñas expuestas, visibles o almacenadas en lugares de fácil acceso o consulta por terceros, tales como escritorios, pantallas, agendas, notas adhesivas, archivos físicos o cualquier otro medio que comprometa su confidencialidad.

- Todos los usuarios como Servidores Públicos, Proveedores, Contratistas y demás partes interesadas y dispositivos que accedan a la red de la ETITC, deberán utilizar contraseñas seguras y complejas conformadas por un mínimo de doce (12) caracteres que incluyan letras mayúsculas, minúsculas, números, símbolos y, de ser necesario, espacios.
- Implementar políticas de cambio de contraseñas periódicas (cada 90 días) para el dominio de la red administrativa y respectivamente cambio de contraseña (cada seis meses) para los sistemas de información.
- Todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas deben utilizar el control MFA para todos los accesos, utilizando (token, SMS, app de autenticación) para su correo institucional y demás sistemas de información.

4.5 LINEAMIENTO DE CONTROL DE ACCESO LÓGICO

La ETITC garantizará que el acceso a los sistemas de información, aplicaciones, redes, infraestructura tecnológica y demás recursos institucionales sea otorgado únicamente a personas autorizadas, aplicando los principios de:

- Mínimo privilegio, necesidad de saber (need-to-know) y segregación de funciones. Todo acceso deberá ser aprobado, asignado, gestionado, monitoreado y revocado conforme a los procedimientos definidos en el Sistema de Gestión de Seguridad de la Información (SGSI) y bajo la supervisión de la instancia responsable del SGSI adscrita a Planeación.
- Se implementarán controles formales para asegurar la autenticación robusta de los usuarios, incluyendo credenciales únicas, contraseñas seguras, autenticación multifactor (MFA) para el acceso al correo institucional y a los sistemas de información críticos, mecanismos de bloqueo por múltiples intentos fallidos y revisiones periódicas de cuentas, privilegios y roles. Queda estrictamente prohibido el uso compartido de credenciales, el acceso no autorizado, la suplantación de identidad o cualquier práctica que comprometa la trazabilidad del usuario.
- La ETITC establecerá procedimientos documentados para la gestión del ciclo de vida de accesos, incluyendo creación, modificación, revisión, suspensión y revocación inmediata de permisos cuando ocurra un retiro, terminación contractual, cambio de rol, reasignación de funciones o pérdida de la necesidad de acceso. Los accesos deberán ser monitoreados continuamente a través de registros, auditorías

y controles automáticos que permitan detectar actividades anómalas, accesos indebidos o comportamientos sospechosos.

- Para proteger los activos de información institucionales, se deberán implementar controles de acceso tanto a la infraestructura lógica (redes, sistemas, aplicaciones, bases de datos, plataformas en la nube) como a la infraestructura física (instalaciones, cuartos de comunicaciones, centros de datos, estaciones de trabajo), con el fin de mitigar los riesgos de acceso no autorizado, manipulación indebida, robo, fuga de información o alteración de activos críticos.
- Todos los servidores públicos, docentes, contratistas, proveedores y demás partes interesadas deberán utilizar MFA obligatorio para todos los accesos institucionales que lo soporten, empleando mecanismos como tokens, aplicaciones de autenticación, códigos SMS o equivalentes aprobados por la entidad. Ningún usuario podrá deshabilitar, evadir o manipular los mecanismos de autenticación establecidos.
- Cada usuario será responsable por la información física o digital a la que acceda, consulte, genere, procese o transmita, debiendo garantizar en todo momento la confidencialidad, integridad, disponibilidad de los activos institucionales. El uso de los accesos y credenciales deberá orientarse exclusivamente al cumplimiento de funciones laborales o contractuales, quedando prohibidas actividades no autorizadas, personales o ajenas a los fines institucionales.

4.5.1 LINEAMIENTO DE CONTROL DE ACCESO LÓGICO

La ETITC gestionará de manera centralizada las identidades digitales, asegurando la creación, administración, revisión periódica y eliminación de cuentas de usuario, incluyendo cuentas privilegiadas.

Se deberán identificar y controlar las cuentas privilegiadas, administrativas y de servicio, aplicando monitoreo reforzado y controles adicionales de seguridad.

4.6 CRIPTOGRAFÍA

La ETITC deberá aplicar controles criptográficos aprobados por el SGSI para proteger la confidencialidad e integridad de la información, utilizando únicamente algoritmos, claves y mecanismos autorizados. El cifrado será obligatorio para la información sensible o confidencial tanto en tránsito como en reposo, y las claves criptográficas deberán

gestionarse de manera segura durante todo su ciclo de vida. Se prohíbe el uso de herramientas, métodos o soluciones criptográficas no aprobadas por la institución.

4.7 LINEAMIENTO DE SEGURIDAD FÍSICA Y DEL ENTORNO

La ETITC deberá implementar, mantener y supervisar un conjunto integral de controles de seguridad física y del entorno destinados a proteger las instalaciones institucionales, la infraestructura tecnológica, los activos de información, todo documentación que contenga información sensible y las áreas críticas frente a accesos no autorizados, daños accidentales, interferencias, amenazas ambientales y cualquier condición que pueda comprometer la continuidad operativa y la protección de la información. Estos controles deberán garantizar la confidencialidad, integridad, disponibilidad y resguardo físico de los activos bajo la responsabilidad de la institución.

La entidad establecerá medidas rigurosas para el control de acceso físico a todas las instalaciones, definiendo mecanismos diferenciados para áreas de acceso general y áreas seguras o de alta sensibilidad. Dichas áreas seguras deberán contar con controles de acceso físico reforzados, tales como sistemas de identificación y/o cerraduras electrónicas y/o tarjetas de proximidad, registro de ingresos, supervisión continua y restricciones basadas en roles y funciones. El acceso será permitido únicamente a personal autorizado y bajo los principios de necesidad operacional y privilegios mínimos.

La ETITC deberá asegurar que las áreas críticas como cuartos de comunicaciones, salas de servidores, centros de datos, nodos de red, espacios de energía y almacenamiento de activos sensibles cuenten con mecanismos de monitoreo ambiental y de seguridad, incluyendo control de temperatura y humedad, sistemas de detección y supresión de incendios, alarmas, sensores, cámaras de vigilancia, detección de intrusos y resguardo físico de equipos. Estos sistemas deberán permitir identificar oportunamente riesgos ambientales, fallas operativas o intentos de acceso no autorizado.

La gestión de visitantes, proveedores, contratistas y personal externo estará sujeta a controles formales de registro, acompañamiento y supervisión, asegurando que ninguna persona externa acceda a áreas sensibles sin autorización expresa. Todos los ingresos deberán documentarse y seguir el procedimiento institucional de acceso físico seguro.
Las áreas, funcionarios, docentes, contratistas, proveedores y terceros deberán cumplir estrictamente todos los lineamientos de acceso físico, uso adecuado de instalaciones, protección de equipos, reporte inmediato de anomalías o incidentes, y preservación de la infraestructura. Queda prohibido cualquier comportamiento que ponga en riesgo la seguridad física, la integridad del entorno o la protección de los activos institucionales.

La ETITC será responsable de definir, documentar y mantener las áreas seguras, así como los controles asociados a cada una de ellas, conforme al Manual de lineamientos de Seguridad y Privacidad de la Información. La entidad garantizará que dichas áreas cuenten con mecanismos de supervisión continua para proteger la información que en ellas se procese o almacene.

Todas las personas que ingresen a las instalaciones de la ETITC, sin excepción, deberán cumplir los lineamientos y procedimientos de acceso físico establecidos, aceptando las verificaciones, restricciones y controles requeridos para preservar la seguridad institucional.

4.7.1 USO DE EQUIPOS DE CÓMPUTO EXTERNOS (CONTROL DE ACCESO, AUTORIZACIÓN Y REGISTRO DE DISPOSITIVOS)

La ETITC establece los lineamientos para el uso seguro de equipos de cómputo externos (no institucionales), con el propósito de proteger los activos de información, la infraestructura tecnológica y los servicios institucionales frente a riesgos derivados del uso de dispositivos no controlados directamente por la entidad.
Se entiende por equipos de cómputo externos aquellos dispositivos de propiedad personal o de terceros, tales como computadores portátiles, tablets u otros dispositivos electrónicos, que requieran acceso a las instalaciones físicas, redes institucionales, sistemas de información o recursos tecnológicos de la ETITC.

a) Control de acceso y registro de dispositivos

Todo equipo de cómputo externo que pretenda ingresar o conectarse a la infraestructura institucional deberá ser previamente autorizado y registrado conforme a los procedimientos establecidos por la entidad. Este registro deberá permitir la identificación del dispositivo, su propietario y sus características técnicas, garantizando la trazabilidad y control sobre su uso dentro del entorno institucional.
La ETITC podrá restringir, suspender o bloquear el acceso de cualquier dispositivo que represente un riesgo para la seguridad de la información.

b) Requisitos mínimos de seguridad

Los equipos de cómputo externos deberán cumplir con las condiciones mínimas de seguridad definidas por la ETITC, incluyendo como mínimo:

- Uso de software antivirus o antimalware actualizado
- Sistema operativo actualizado con parches de seguridad vigentes
- Activación de mecanismos de protección como firewall y bloqueo automático de sesión

- Ausencia de software no autorizado, ilegal o potencialmente malicioso
- Cifrado de la información almacenada en el dispositivo, cuando se trate de información sensible o clasificada.

Adicionalmente:

- La ETITC podrá requerir la instalación de herramientas de gestión, monitoreo o control de seguridad sobre los dispositivos
- No se permite desactivar o alterar las configuraciones de seguridad establecidas por la institución

El incumplimiento de estos requisitos podrá dar lugar a la restricción o bloqueo del dispositivo.

c) Condiciones de acceso a la red institucional

El acceso de equipos externos a la red de la ETITC estará sujeto a controles de autenticación, autorización y segmentación, de acuerdo con el nivel de acceso requerido y el perfil del usuario. La institución podrá restringir el acceso a determinados recursos o asignar redes diferenciadas, con el fin de proteger los sistemas críticos y la información sensible.
La institución podrá:

- Exigir el uso de mecanismos de autenticación multifactor (MFA)
- Restringir el acceso a determinados recursos
- Asignar redes diferenciadas para dispositivos externos
- Requerir el uso de conexiones seguras o cifradas para el acceso remoto

Todo acceso deberá regirse por el principio de mínimo privilegio y necesidad de acceso.

d) Uso y tratamiento de la información institucional

El uso de información institucional desde equipos externos deberá regirse por los principios de confidencialidad, integridad y disponibilidad, así como por el principio de mínimo privilegio y necesidad de acceso.
Se prohíbe:

- El almacenamiento, procesamiento o transferencia de información sensible en dispositivos externos sin la debida autorización
- Compartir credenciales de acceso o permitir el uso del dispositivo por terceros para acceder a recursos institucionales

Los usuarios deberán evitar el almacenamiento local de información institucional; en este sentido deben acoger las recomendaciones entregas desde el área de tecnología proporcionadas para este fin.

e) Uso de dispositivos de almacenamiento externo

El uso de dispositivos de almacenamiento externo asociados a equipos de cómputo externos (como memorias USB o discos portátiles) estará sujeto a restricciones, controles de seguridad y monitoreo, de acuerdo con los lineamientos definidos por la ETITC, con el fin de prevenir la fuga de información o la introducción de código malicioso.

f) Gestión de la información institucional en dispositivos externos

La ETITC se reserva el derecho de eliminar información institucional almacenada en dispositivos externos en los siguientes casos:

- Terminación de la relación laboral o contractual
- Pérdida o robo del dispositivo
- Incidentes de seguridad de la información

La institución podrá aplicar mecanismos de borrado remoto o eliminación de datos cuando sea necesario para proteger los activos institucionales.
La ETITC no asumirá responsabilidad por la pérdida de información personal derivada de la aplicación de estos controles de seguridad.

g) Responsabilidades del usuario

Los usuarios que utilicen equipos de cómputo externos serán responsables de:

- Garantizar el cumplimiento de los lineamientos de seguridad establecidos
- Proteger la información institucional a la que tengan acceso
- Utilizar redes confiables y mecanismos de conexión segura
- Reportar de manera inmediata cualquier incidente, anomalía o sospecha de vulneración
- Abstenerse de realizar acciones que comprometan la seguridad de los sistemas y servicios institucionales
- Utilizar el OneDrive como único medio de almacenamiento autorizado.

h) Monitoreo y control

La ETITC se reserva el derecho de implementar mecanismos de monitoreo, control y restricción sobre el uso de dispositivos externos, incluyendo la validación de cumplimiento de requisitos de seguridad, el control de acceso a sistemas y la desconexión de dispositivos que representen un riesgo para la institución.

i) Prohibiciones

Queda estrictamente prohibido:

- Conectar dispositivos externos no autorizados a la infraestructura tecnológica institucional
- Acceder a los sistemas de información desde equipos que no cumplan los requisitos de seguridad
- Instalar software no autorizado o manipular configuraciones de seguridad
- Utilizar equipos externos para almacenar o transferir información institucional sin control o autorización
-

j) Gestión de incumplimientos

El incumplimiento de los presentes lineamientos será tratado como un incidente de seguridad de la información y podrá dar lugar a la aplicación de medidas disciplinarias, administrativas, contractuales o legales, de acuerdo con la normativa vigente y las disposiciones del Sistema de Gestión de Seguridad de la Información (SGSI).

4.7.2 SEGURIDAD EN TELETRABAJO

La ETITC permitirá el desarrollo de actividades bajo la modalidad de teletrabajo, siempre que se implementen y mantengan las medidas de seguridad necesarias para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Todo funcionario autorizado para desempeñar sus funciones fuera de las instalaciones de la entidad deberá cumplir los lineamientos y controles de seguridad definidos por la ETITC, utilizando únicamente los mecanismos, herramientas, servicios y accesos remotos previamente autorizados para el tratamiento de la información y el acceso a los activos institucionales.

Los equipos de cómputo externos que se utilicen para el desarrollo de actividades bajo la modalidad de teletrabajo deberán ser previamente revisados, validados y autorizados por el Grupo de Gestión de Información y Telecomunicaciones (TI). Solo después de la aprobación correspondiente, el funcionario podrá utilizar dichos dispositivos para el cumplimiento de sus funciones.

El funcionario autorizado será responsable de la custodia y uso seguro del equipo de cómputo utilizado durante el teletrabajo, así como del cumplimiento de las disposiciones establecidas en el numeral 4.7.1 Uso de Equipos de Cómputo Externos, del presente Manual.

Responsabilidades del usuario en teletrabajo

El personal autorizado para teletrabajo deberá:

- Utilizar únicamente los dispositivos, aplicaciones y medios de acceso aprobados por la ETITC.
- Mantener actualizados los mecanismos de protección del equipo autorizado (Antivirus, Office y sistema operativo).
- Proteger sus credenciales de acceso y no compartirlas con terceros.
- Asegurar que la información institucional no sea visualizada, copiada o utilizada por personas no autorizadas.
- Bloquear el equipo cuando no se encuentre en uso.
- Reportar inmediatamente cualquier incidente o situación que pueda afectar la seguridad de la información institucional.
- El almacenamiento y manejo de la información se debe realizar únicamente por medio del correo y OneDrive institucional, no se debe almacenar información institucional en los equipos de cómputo.
- Realizar conexión a internet únicamente por la red verificada y autorizada, no realizar conexiones en redes públicas.
- Reportar cualquier falla o requerimiento de tecnología por medio de mesadeayuda@itc.edu.co

4.7.3 LINEAMIENTO DE SEGURIDAD DE DISPOSITIVOS MÓVILES (MDM)

La ETITC deberá implementar controles de seguridad para dispositivos móviles (teléfonos inteligentes, tablets y otros dispositivos portátiles) que accedan, procesen o almacenen información institucional, con el fin de prevenir el acceso no autorizado, la fuga de información y la exposición a amenazas.

Se deberán aplicar como mínimo las siguientes medidas:

- Uso de mecanismos de autenticación segura (PIN, patrón, biometría o MFA).
- Cifrado de la información almacenada en el dispositivo.
- Habilitación de bloqueo automático tras periodos de inactividad.
- Implementación de capacidades de borrado remoto (wipe) en caso de pérdida o robo.

- Control de instalación y uso de aplicaciones mediante herramientas de gestión de dispositivos móviles (MDM), cuando aplique.
- Prohibición de uso de aplicaciones no autorizadas para el tratamiento de información institucional.
- Actualización periódica del sistema operativo y aplicaciones.
- Restricción del acceso a información institucional en dispositivos no autorizados o comprometidos.
- Monitoreo y control de cumplimiento de políticas de seguridad sobre dispositivos móviles.

La ETITC podrá restringir o bloquear el acceso a los recursos institucionales desde dispositivos móviles que no cumplan con los requisitos de seguridad definidos.
Los usuarios serán responsables de proteger los dispositivos móviles bajo su custodia y reportar de manera inmediata cualquier incidente de seguridad, pérdida o robo.

4.8 LINEAMIENTO DE SEGURIDAD EN LAS OPERACIONES

La ETITC deberá establecer, implementar y mantener un marco integral de seguridad en las operaciones que garantice la administración segura, confiable y continua de los sistemas de información, infraestructura tecnológica y servicios institucionales. Todas las actividades operativas deberán ejecutarse conforme a procedimientos formales, documentados y autorizados dentro del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la protección permanente de la información y la adecuada gestión de los recursos tecnológicos.

La entidad deberá aplicar controles de seguridad operativa que cubran, como mínimo:

- **Gestión de cambios controlados**, asegurando que toda modificación a infraestructura, software, configuraciones o servicios sea aprobada, probada, documentada y registrada.
- **Gestión de vulnerabilidades**, incluyendo escaneo periódico, evaluación de riesgos, priorización y aplicación oportuna de parches y actualizaciones.
- **Monitoreo continuo de eventos y registros**, con mecanismos de trazabilidad, alertas, correlación, registro seguro y análisis de actividades anómalas.
- **Administración de configuraciones** basadas en estándares, plantillas endurecidas, revisiones periódicas y prohibición expresa de configuraciones no autorizadas.

- **Respaldo, recuperación y pruebas de restauración**, garantizando copias de seguridad seguras, cifradas cuando corresponda, verificadas regularmente y con procedimientos de recuperación documentados.
- **Control de capacidades y desempeño**, asegurando la disponibilidad adecuada de recursos técnicos y evitando saturaciones que afecten los servicios.
- **Segregación de entornos** (producción, pruebas, desarrollo), evitando cruces no permitidos que pongan en riesgo la integridad o disponibilidad de los servicios.
- **Operación segura diaria de servicios**, manteniendo estabilidad, disponibilidad, control, revisiones rutinarias y mantenimiento preventivo.

La ETITC deberá planear, administrar, proteger y monitorear la infraestructura tecnológica que soporta las funciones institucionales, aplicando los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información. Todo lo anterior deberá alinearse con los procedimientos, protocolos y manuales definidos para el SGSI.

Todas las áreas y el personal responsable de operaciones deberán cumplir estrictamente estos lineamientos, reportar de forma inmediata cualquier anomalía, incidente, falla operativa, actividad sospechosa o riesgo materializado; así mismo deberán garantizar la integridad de los entornos productivos, evitar cambios no autorizados, asegurar la trazabilidad de las acciones realizadas y operar los servicios conforme a los principios de control, monitoreo permanente, registro detallado y cumplimiento normativo.

Cualquier desviación operativa, incumplimiento de procedimientos, alteración no autorizada de configuraciones o acción que comprometa la continuidad o seguridad de los servicios tecnológicos será gestionada como incidente de seguridad y podrá derivar en acciones correctivas, preventivas, administrativas o disciplinarias conforme a los lineamientos institucionales.

4.8.1 PLANIFICACION Y CONTROL OPERACIONAL DE SEGURIDAD

Las actividades operativas de TI y seguridad deberán planificarse en ventanas autorizadas, con evaluación de riesgos previa, comunicación a partes interesadas, verificación posterior y evidencias en los sistemas institucionales.

4.8.2 DETECCION DE ACTIVIDADES ANOMALAS

La ETITC mantendrá capacidades de detección mediante registros centralizados, correlación (SIEM), umbrales y alertas, baselines de comportamiento y análisis de eventos para identificar accesos indebidos o patrones anómalos.

4.9 LINEAMIENTO DE PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

La ETITC establecerá, documentará y mantendrá procedimientos operacionales que aseguren la ejecución segura, consistente y controlada de las actividades relacionadas con el uso, gestión y protección de los sistemas de información. Todas las responsabilidades asociadas a estos procedimientos deberán estar claramente definidas, asignadas y comunicadas a los propietarios, custodios y usuarios de la información.

Los procedimientos deberán incluir controles para la operación diaria, gestión de cambios, manejo de incidentes, respaldo de información, monitoreo de sistemas y cualquier otra actividad necesaria para garantizar la continuidad, integridad, disponibilidad y confidencialidad de los servicios tecnológicos. Todo miembro de la institución que participe en procesos operativos estará obligado a cumplir estos lineamientos y a reportar cualquier desviación o actividad no autorizada.

4.9.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS

La ETITC deberá establecer, documentar, implementar y mantener procedimientos de operación que aseguren la ejecución segura, estandarizada y controlada de todas las actividades relacionadas con los sistemas de información. Estos procedimientos deberán estar formalmente aprobados, actualizados y disponibles para los responsables operativos, garantizando que las tareas críticas se realicen de manera consistente y conforme a los lineamientos del SGSI.

Asimismo, todos los procesos operativos —incluyendo operación diaria, gestión de cambios, respaldo de información, monitoreo, mantenimiento y manejo de incidentes— deberán contar con responsables claramente definidos, así como reglas precisas para su ejecución. Cualquier desviación, cambio o actualización en los procedimientos deberá ser gestionada siguiendo los controles establecidos por la institución.

4.9.2 GESTIÓN DE CAMBIOS

La ETITC deberá asegurar que todo cambio relacionado con infraestructura tecnológica, sistemas de información, aplicaciones, configuraciones, servicios, componentes de seguridad o procesos operativos sea gestionado de manera controlada, documentada y autorizada, de acuerdo con lo establecido en los lineamientos de la entidad.

Todos los cambios deberán ser evaluados en términos de su impacto en la confidencialidad, integridad, disponibilidad y continuidad de los servicios, así como en el cumplimiento de requisitos legales y contractuales. Ningún cambio podrá implementarse sin la debida aprobación por los responsables designados y sin haber sido registrado en el procedimiento correspondiente.

La ejecución de los cambios deberá realizarse siguiendo un plan definido, que incluya validaciones previas, pruebas, comunicación a las partes interesadas y mecanismos de reversión. Todo cambio implementado deberá ser revisado posteriormente para garantizar que no generó afectaciones operativas, de seguridad o de cumplimiento.

4.9.3 GESTIÓN DE CAPACIDAD

La ETITC deberá planificar, monitorear y gestionar la capacidad y el desempeño de la infraestructura tecnológica, plataformas, servicios y sistemas de información para asegurar que puedan soportar de manera eficiente las cargas actuales y futuras de trabajo. Los recursos deberán dimensionarse y ajustarse oportunamente para prevenir degradaciones, indisponibilidades o afectaciones a la continuidad operativa.

Todo incremento, modificación o ajuste de capacidad deberá basarse en análisis de tendencias, métricas de desempeño, indicadores de uso y proyecciones de demanda. Asimismo, cualquier acción relacionada con ampliación, optimización o redistribución de recursos tecnológicos deberá ser documentada y aprobada conforme a los procedimientos institucionales.

El proceso de TI será responsable de implementar mecanismos de monitoreo continuo que permitan anticipar riesgos de saturación, establecer planes de mejora y garantizar que los servicios tecnológicos mantengan niveles de desempeño adecuados y alineados con los requisitos del SGSI.

4.9.4 SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN

La ETITC deberá mantener ambientes segregados de desarrollo, pruebas y operación para minimizar riesgos de cambios no autorizados, fugas de datos y afectaciones a la disponibilidad de los servicios. Queda prohibida la utilización de datos productivos en ambientes no operativos, salvo cuando se realiza un proceso de anonimización y autorización formal.

El acceso a cada ambiente deberá estar controlado por roles y privilegios mínimos, diferenciando responsables de desarrollo, pruebas, despliegue y operación. Todo flujo de promoción entre ambientes (Dev → QA → Prod) deberá seguir el procedimiento de gestión de cambios, incluyendo control de versiones, evidencias de pruebas, validaciones de seguridad y mecanismos de reversión.

Las configuraciones de cada ambiente deberán estar aisladas (redes, credenciales, claves, secretos, endpoints, colas, buckets, bases de datos) y administradas mediante gestión

segura de configuraciones y código como infraestructura cuando aplique. Cualquier excepción a esta política deberá ser justificada, aprobada y documentada conforme a los lineamientos del SGSI.

4.10 LINEAMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

La ETITC deberá establecer, implementar y mantener controles preventivos, detectivos y correctivos que garanticen la protección integral de todos los sistemas de información frente a códigos maliciosos, tales como malware, ransomware, spyware, adware, troyanos, rootkits, botnets, así como cualquier software o componente que pueda comprometer la confidencialidad, integridad, disponibilidad o trazabilidad de la información institucional.

Los equipos de cómputo, servidores, dispositivos móviles institucionales, infraestructura tecnológica, servicios en la nube y cualquier activo digital deberán contar con soluciones de seguridad actualizadas y configuradas siguiendo buenas prácticas, tales como antivirus, antimalware, EDR/XDR, filtros de contenido, análisis heurístico, sandboxing y protección de correo electrónico. El proceso de TI será responsable de asegurar la actualización oportuna de firmas, parches, motores de detección y políticas de seguridad.

Se prohíbe estrictamente la instalación, ejecución o descarga de software no autorizado, así como la manipulación de archivos provenientes de fuentes desconocidas o no confiables. Toda actividad anómala, comportamiento sospechoso, alerta de seguridad o indicio de posible código malicioso deberá ser reportado de inmediato al proceso de TI para su verificación, contención, erradicación y recuperación, siguiendo el procedimiento de Gestión de Incidentes de Seguridad de la Información.

El proceso de TI deberá realizar monitoreo continuo del entorno tecnológico, análisis de tendencias, revisión de indicadores y pruebas periódicas para validar la eficacia de los controles implementados. Adicionalmente, el líder de gestión de seguridad de la información apoyara con campañas de sensibilización orientadas a fortalecer la cultura de seguridad entre los usuarios, incluyendo prácticas seguras de navegación, manipulación de archivos, uso del correo electrónico y prevención del fraude digital.
En caso de detección de código malicioso, software no autorizado o archivos potencialmente peligrosos, el proceso de Gestión de Informática y Telecomunicaciones (TI) estará facultado para ejecutar de manera inmediata acciones de contención, aislamiento, bloqueo, eliminación o remediación sobre los activos, sistemas o repositorios institucionales involucrados, sin requerir autorización previa del usuario, cuando exista riesgo para la seguridad de la información.

Estas acciones deberán estar debidamente soportadas en evidencias técnicas (herramientas de monitoreo, alerta o correlación de eventos tales como SIEM, EDR/XDR u

otras soluciones de seguridad), y deberán ser registradas, documentadas y trazables conforme al procedimiento de Gestión de Incidentes de Seguridad de la Información.
El proceso de TI deberá notificar posteriormente al usuario o área afectada, cuando aplique, garantizando el debido registro, análisis y cierre del incidente.

Cualquier excepción a las medidas de protección contra código malicioso deberá ser debidamente justificada, autorizada y documentada conforme a los lineamientos del SGSI.

4.11 LINEAMIENTO DE COPIAS DE RESPALDO

El Proceso gestión de TI deberá ejecutar copias de respaldo para sistemas de información y bases de datos, almacenándolas en al menos dos ubicaciones seguras (incluyendo repositorios fuera del sitio), en formato cifrado y con acceso restringido; adicionalmente, se realizarán pruebas de restauración para validar su integridad y disponibilidad, dejando registro de cada actividad en la bitácora institucional, y en caso de incidentes como corrupción de datos, se seleccionará la versión más reciente intacta y se documentará la restauración conforme al procedimiento de gestión de incidentes, revisándose este procedimiento anualmente como parte de la mejora continua del SGSI

4.12 LINEAMIENTO DE REGISTRO Y SEGUIMIENTO

La Escuela Tecnológica Instituto Técnico Central ETITC establece que todos los procesos, actividades, eventos, incidentes y actuaciones relacionadas con la Seguridad de la Información deberán contar con registros oficiales, íntegros y actualizados, que permitan garantizar la trazabilidad, transparencia y control sobre la operación institucional. Cada proceso será responsable de generar, custodiar y actualizar los registros asociados a sus activos, servicios, actividades y procedimientos, asegurando que estos se encuentren debidamente documentados, sean accesibles para auditorías internas o externas, y estén protegidos frente a modificaciones no autorizadas. Todos los registros deberán mantenerse conforme a su tiempo de retención definido, alineados al ciclo PHVA del SGSI, y sujetos a seguimiento periódico por parte del Proceso de Gestión de Seguridad de la Información, quien verificará la existencia, completitud, vigencia y exactitud de la información registrada.

El seguimiento incluirá la revisión de bitácoras, evidencias de ejecución, reportes de incidentes, controles implementados, cumplimiento normativo, y la evaluación de actividades de mejora continua, garantizando que cualquier desviación, no conformidad o brecha detectada sea registrada, tratada y cerrada en los tiempos establecidos. Este lineamiento aplica a funcionarios, contratistas y terceros que generen o administren registros institucionales y constituye un componente fundamental para la gestión efectiva de riesgos, la toma de decisiones informada y la sostenibilidad del SGSI en la ETITC.

4.12.1 REGISTRO DE EVENTOS

La Escuela Tecnológica Instituto Técnico Central – ETITC establece que todos los sistemas, plataformas, aplicaciones, infraestructuras tecnológicas y servicios institucionales deberán generar, conservar y proteger registros de eventos que permitan garantizar la trazabilidad, integridad y disponibilidad de la información relacionada con su operación.

Los eventos registrados deberán incluir, como mínimo, accesos exitosos y fallidos, actividades administrativas, cambios de configuración, uso de privilegios, fallos del sistema, alertas de seguridad, actividad anómala y cualquier operación relevante para identificar incidentes o comportamientos no autorizados. El Proceso Gestión de TI será responsable de asegurar que los registros se generen de forma continua, se almacenen en repositorios seguros, estén protegidos contra alteraciones o eliminación indebida y se conserven por el tiempo establecido en las políticas institucionales.

El Proceso de Gestión de Seguridad de la Información, adscrito a Planeación, realizará revisiones periódicas de dichos registros como parte del monitoreo y del ciclo de mejora continua del SGSI, verificando su integridad, completitud y utilidad para la detección temprana de incidentes, el análisis forense y el cumplimiento normativo. Toda desviación, ausencia de registro o falla en los mecanismos de auditoría deberá ser reportada, analizada y gestionada según el procedimiento de incidentes de seguridad.

Este lineamiento aplica a todos los funcionarios, contratistas y proveedores que administren, operen o soporten sistemas institucionales y constituye un componente esencial para fortalecer la seguridad, la gobernanza y la confiabilidad operativa de la ETITC.

4.12.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO

La Escuela Tecnológica Instituto Técnico Central – ETITC establece que toda la información contenida en los registros generados por los sistemas, aplicaciones, plataformas tecnológicas, servicios institucionales y equipos de infraestructura deberá ser protegida con el fin de garantizar su confidencialidad, integridad, disponibilidad y trazabilidad, constituyéndose en un recurso crítico para la detección de incidentes de seguridad, el análisis forense y el cumplimiento normativo.

Los registros deberán mantenerse íntegros y libres de alteraciones no autorizadas mediante la aplicación de controles técnicos como cifrado, protección contra escritura, firmas digitales, controles de acceso basados en privilegios mínimos y segregación entre ambientes operativos y de auditoría.

El acceso a los registros se limitará exclusivamente al personal autorizado del Proceso Gestión de TI y del Proceso de Gestión de Seguridad de la Información, adscrito a Planeación, garantizando que su consulta, extracción o uso esté debidamente justificado, documentado y sujeto a supervisión. Los repositorios de almacenamiento deberán ubicarse en entornos seguros, protegidos contra eliminación accidental, corrupción de datos o manipulación maliciosa, y deberán contar con mecanismos de respaldo y retención según lo definido en las políticas institucionales.

Cualquier intento de alteración, eliminación o acceso no autorizado a la información de registro deberá ser tratado como un incidente de seguridad e informado inmediatamente para su análisis y escalamiento. Este lineamiento es de obligatorio cumplimiento para funcionarios, contratistas y proveedores que administren o soporten sistemas institucionales, y constituye un pilar fundamental para la gobernanza, transparencia y robustez del SGSI de la ETITC.

4.12.3 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR

La Escuela Tecnológica Instituto Técnico Central – ETITC establece que todo administrador y operador de sistemas, plataformas tecnológicas, servicios informáticos o infraestructuras institucionales deberá generar y mantener registros completos, trazables y verificables de las actividades realizadas en el ejercicio de sus funciones. Estos registros constituyen un mecanismo esencial de control, auditoría y rendición de cuentas, y permiten garantizar la transparencia, la integridad operativa y la detección oportuna de eventos o incidentes de seguridad.

Los administradores y operadores deberán documentar, como mínimo, las acciones relacionadas con cambios de configuración, creación o modificación de cuentas de usuario, gestión de privilegios, instalación o eliminación de software, intervenciones en bases de datos, parches aplicados, reinicios de servicios, actividades de mantenimiento, ejecución de scripts o automatizaciones, y cualquier operación administrativa o técnica que pueda impactar la seguridad, disponibilidad o estabilidad de los sistemas. Dichos registros deberán consignarse en los mecanismos oficiales definidos por el Proceso Gestión de TI (bitácoras, sistemas de gestión de cambios, plataformas de ticketing o repositorios de auditoría), y deberán ser precisos, fechados, íntegros y protegidos contra alteración o eliminación indebida.
El acceso a estos registros estará limitado al personal autorizado y al Proceso de Gestión de Seguridad de la Información, adscrito a Planeación, para efectos de verificación, monitoreo continuo, análisis forense y cumplimiento normativo. Cualquier omisión en el registro, inconsistencia, manipulación no autorizada o ausencia de evidencia documental será considerada incumplimiento a las políticas de la ETITC y deberá ser reportada según el procedimiento de incidentes de seguridad.

Este lineamiento es de obligatorio cumplimiento para todo administrador y operador que tenga injerencia técnica en activos o sistemas institucionales y constituye un componente clave para la gobernanza, control y robustez del SGSI de la ETITC.

4.12.4 SINCRONIZACIÓN DE RELOJES

La ETITC establece que todos los sistemas, servidores, equipos de red, aplicaciones institucionales y servicios críticos de la entidad deben operar con una hora exacta, uniforme y centralizada, sincronizada mediante protocolos seguros (como NTP/NTP seguro) con fuentes confiables internas o externas. Esta sincronización es obligatoria para garantizar la correlación precisa de eventos, la confiabilidad de los registros de auditoría, la trazabilidad durante la gestión de incidentes, la validez de la evidencia digital y el adecuado funcionamiento de los controles de seguridad y continuidad. La administración de esta sincronización deberá ser gestionada por TI/Infraestructura, quien asegurará que todos los sistemas apunten a servidores de tiempo autorizados, mantengan sincronización automática, registren fallas o desviaciones y ejecuten acciones correctivas. Los sistemas que estén sin sincronización activa o con ajustes manuales deberán ser reportada al SGSI para evitar impactos en la investigación de incidentes, validación de transacciones, integridad de los logs y cumplimiento normativo.

4.13 LINEAMIENTO DE CONTROL DE SOFTWARE OPERACIONAL

La ETITC deberá asegurar que todo software, componente, actualización o configuración que se implemente en ambientes operacionales sea gestionado mediante un proceso formal de control de cambios, garantizando que únicamente versiones autorizadas, probadas y trazables sean instaladas en producción. Todo cambio debe contar con aprobación del Dueño del Servicio, TI/Infraestructura, y Seguridad de la Información, manteniendo separación de ambientes (Desarrollo, Pruebas y Producción), control de versiones y evidencia de validación técnica. El despliegue de software solo podrá realizarse en ventanas autorizadas, con mecanismos de reversa, controles de integridad y registros completos de lo ejecutado.

Se prohíben cambios directos, no documentados o sin pruebas previas, y cualquier excepción deberá ser justificada, aprobada y registrada. Este lineamiento busca asegurar la integridad, disponibilidad y confiabilidad del software institucional y reducir riesgos derivados de modificaciones no controladas en producción.

4.13.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

La instalación de software en los sistemas operativos institucionales deberá realizarse únicamente por personal autorizado del Proceso TI/Infraestructura, siguiendo un proceso formal que garantice la seguridad, integridad y confiabilidad de los equipos y servicios de la ETITC. Todo software por instalar debe ser licenciado, legítimo, validado y aprobado.

Se prohíbe la instalación de aplicaciones no autorizadas, freeware no validado, ejecutables externos o herramientas que no cuenten con requerimiento formal y justificación operativa. La instalación deberá registrarse en los sistemas correspondientes, mantener evidencias y aplicarse bajo cuentas administrativas controladas. Cualquier excepción deberá ser aprobada por Seguridad de la Información y documentada, garantizando que las configuraciones del sistema operativo permanezcan estables, seguras y alineadas con los estándares institucionales.

4.14 LINEAMIENTO DE GESTIÓN DE CONFIGURACIÓN SEGURA (HARDENING)

La ETITC deberá garantizar que todos los sistemas de información, servidores, estaciones de trabajo, dispositivos de red, plataformas en la nube y aplicaciones institucionales sean configurados de acuerdo con estándares de seguridad definidos, eliminando configuraciones por defecto y reduciendo la superficie de ataque.

Se deberán implementar como mínimo las siguientes directrices:

- Aplicar configuraciones seguras (Hardening) basadas en estándares y buenas prácticas reconocidas.
- Deshabilitar servicios, puertos, protocolos y cuentas innecesarias o no autorizadas.
- Eliminar o modificar configuraciones predeterminadas que representen riesgos de seguridad.
- Aplicar controles de seguridad en sistemas operativos, bases de datos, aplicaciones y dispositivos de red.
- Garantizar la gestión segura de configuraciones mediante líneas base (baselines) aprobadas.
- Implementar revisiones periódicas de configuraciones para detectar desviaciones (config drift).
- Controlar y documentar los cambios de configuración mediante el proceso formal de gestión de cambios.

La configuración segura deberá ser gestionada por el Proceso de Gestión de Información y Telecomunicaciones (TI), en coordinación con el Líder del SGSI, garantizando su actualización conforme a nuevas amenazas, vulnerabilidades y cambios tecnológicos.

4.15 LINEAMIENTO DE GESTIÓN DE LA VULNERABILIDAD TÉCNICA

La ETITC deberá identificar, analizar y mitigar de manera sistemática las vulnerabilidades técnicas presentes en sistemas operativos, aplicaciones, infraestructura tecnológica, dispositivos de red, servicios en la nube y cualquier activo tecnológico institucional.
Para ello, se deberán ejecutar escaneos periódicos, evaluaciones de seguridad, revisiones de configuración y monitoreo continuo, garantizando que toda vulnerabilidad detectada sea clasificada según su criticidad y gestionada dentro de los tiempos definidos por el SGSI. Todo hallazgo deberá contar con un responsable, fecha compromiso y evidencia de cierre, priorizando aquellas vulnerabilidades que representen riesgo alto o crítico para la confidencialidad, integridad o disponibilidad de la información. Se prohíbe la operación de sistemas con vulnerabilidades críticas sin mitigación o controles compensatorios aprobados.

La Gestión de la Vulnerabilidad Técnica será coordinada por Seguridad de la Información en conjunto con TI/Infraestructura, manteniendo trazabilidad, reportes y acciones de mejora continua alineadas con las buenas prácticas de ciberseguridad institucional.

4.15.1 RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE

La instalación de software en los equipos, servidores y sistemas operativos institucionales estará estrictamente restringida y solo podrá ser realizada por el personal autorizado del Proceso TI/Infraestructura, garantizando la protección de los activos tecnológicos y la integridad del entorno operativo de la ETITC.
Se prohíbe la instalación de aplicaciones no autorizadas, software no licenciado, herramientas descargadas desde sitios no oficiales, aplicaciones que no cuenten con validación de Seguridad de la Información o que representen riesgo para la estabilidad y seguridad de los sistemas.
Cualquier solicitud de instalación deberá estar justificada, documentada y aprobada mediante los canales oficiales, y deberá verificarse su legitimidad, licenciamiento y compatibilidad antes de realizarse.

No se permitirá que usuarios, contratistas o terceros instalen software por cuenta propia, y toda excepción deberá ser autorizada por TI y Seguridad de la Información, dejando evidencia formal del análisis y la aprobación correspondiente. Este lineamiento busca evitar el ingreso de malware, vulnerabilidades, configuraciones inseguras o software no conforme que comprometa la operación institucional.

4.16 LINEAMIENTO DE CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

La ETITC deberá garantizar que todas las auditorías realizadas a los sistemas de información se ejecuten de manera controlada, planificada y segura, asegurando que las actividades de verificación no afecten la disponibilidad, integridad o confidencialidad de los servicios tecnológicos institucionales. Toda auditoría técnica, interna o externa, deberá contar con la autorización previa del Proceso TI y Seguridad de la Información, definiendo claramente su alcance, métodos de prueba, herramientas permitidas y ventanas de ejecución.

El personal auditor solo podrá acceder a los sistemas bajo el principio de mínimo privilegio y mediante cuentas controladas, manteniendo trazabilidad completa de las actividades realizadas.

Está prohibido ejecutar pruebas intrusivas, escaneos de alta carga o cambios en la configuración sin aprobación previa. Los hallazgos deberán ser documentados y tratados conforme al SGSI, y cualquier evidencia obtenida será manejada con estricta reserva y cumpliendo las políticas de confidencialidad institucional.

4.16.1 CONTROLES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

La ETITC deberá asegurar que todas las auditorías a los sistemas de información, internas o externas se realicen bajo controles estrictos que garanticen la seguridad, estabilidad y continuidad de los servicios tecnológicos institucionales.
Toda auditoría deberá ser autorizada previamente por el Proceso TI y Seguridad de la Información, definiendo su alcance, cronograma, herramientas permitidas y nivel de acceso requerido. Durante la auditoría, el personal auditor solo podrá operar bajo el principio de mínimo privilegio, con cuentas controladas, supervisadas y con registro detallado de cada actividad realizada.

Se prohíbe la ejecución de pruebas intrusivas, cambios de configuración, escaneos agresivos o actividades no incluidas en el alcance aprobado. Finalizada la auditoría, los hallazgos deberán ser documentados, analizados y gestionados conforme al procedimiento institucional de tratamiento de vulnerabilidades y acciones de mejora, garantizando la trazabilidad y la confidencialidad de la información evaluada.

4.17 LINEAMIENTO DE SEGURIDAD DE LAS COMUNICACIONES

La ETITC deberá implementar, mantener y supervisar un conjunto integral de controles de seguridad en las comunicaciones orientados a proteger la información durante su transmisión interna y externa, garantizando su confidencialidad, integridad y disponibilidad, mediante el uso exclusivo de canales, protocolos y mecanismos aprobados por la institución.

La entidad adoptará medidas técnicas y administrativas para proteger las comunicaciones electrónicas, enlaces, redes, dispositivos de interconexión, plataformas de mensajería, servicios de correo institucional, comunicaciones IP, servicios en la nube y cualquier medio por el cual circule información institucional. Estas medidas incluirán, como mínimo:

a) Protección de las comunicaciones y las redes

- Uso de canales seguros (TLS, VPN corporativa, HTTPS, SSH y protocolos cifrados).
- Implementación de cifrado en tránsito para toda información sensible o crítica.
- Segmentación de redes internas, VLAN seguras y controles de acceso basados en roles.
- Monitoreo continuo del tráfico de red, detección de anomalías, IDS/IPS y filtrado avanzado.
- Controles contra accesos no autorizados, ataques de red, sniffing, spoofing y manipulación de paquetes.
- Prohibición del uso de redes públicas, no autorizadas o inseguras para actividades institucionales.

b) Control de acceso y operación de redes

El Grupo de Tecnologías de la Información y las Comunicaciones administrará y protegerá la infraestructura de red aplicando controles de acceso lógico, configuraciones endurecidas, autenticación robusta, monitoreo centralizado y políticas que garanticen el cumplimiento de los acuerdos de niveles de servicio (SLA) definidos y aprobados por la Alta Dirección.
Toda configuración, modificación o activación de servicios de red deberá estar autorizada, documentada y alineada con los procedimientos operativos del SGSI.

c) Transferencia y comunicación segura de información

La ETITC definirá y aplicará procedimientos formales para la transferencia segura de información, tanto interna como externa, incluyendo:

- Validación de autorizaciones antes de transferir información.
- Uso de herramientas institucionales certificadas.
- Cifrado en tránsito para información clasificada, crítica o personal.
- Prohibición del uso de medios no autorizados (correo personal, servicios no institucionales, aplicaciones no aprobadas, mensajería informal).
- Registro y trazabilidad de transferencias que involucren información sensible.

d) Uso responsable de medios y canales de comunicación

Todo el personal, servidores públicos, docentes, contratistas, proveedores, visitantes y terceros deberá:

- Utilizar únicamente los canales institucionales autorizados.
- Reportar de inmediato anomalías, accesos indebidos o fallas de comunicación.
- Proteger la información que transmiten y reciben.
- Evitar divulgaciones no autorizadas o transferencias por medios inseguros.
- Cumplir estrictamente con los lineamientos del SGSI y con las directrices de Planeación como órgano rector.

Queda estrictamente prohibido el uso de herramientas, protocolos, redes o canales externos no certificados o no autorizados para transmitir, almacenar o intercambiar información institucional.

e) Aseguramiento de la disponibilidad

La ETITC implementará controles de redundancia, monitoreo, continuidad de comunicaciones, administración de enlaces y pruebas periódicas para garantizar que la infraestructura de red y las comunicaciones institucionales operen de forma estable, segura y confiable.

4.17.1 GESTION DE SEGURIDAD DE LAS REDES

La ETITC implementará controles técnicos y administrativos para proteger la infraestructura de red, garantizando su disponibilidad, integridad y confidencialidad, mediante la aplicación de mecanismos de segmentación, control y monitoreo.

Se deberán aplicar las siguientes directrices:

- Implementar segmentación de red lógica y/o física (por ejemplo, VLAN), separando usuarios, servidores, sistemas críticos y ambientes de desarrollo, pruebas y producción, de acuerdo con su nivel de criticidad.
- Controlar y restringir el tráfico entre segmentos de red mediante listas de control de acceso (ACL), firewalls u otros mecanismos de filtrado, aplicando el principio de mínimo privilegio.
- Implementar autenticación robusta para el acceso a dispositivos y servicios de red.
- Aplicar configuraciones seguras (Hardening) en todos los dispositivos de red.
- Gestionar los cambios en la infraestructura de red mediante procedimientos formales, asegurando su evaluación, aprobación, documentación, pruebas y reversibilidad.
- Implementar monitoreo continuo de la red mediante herramientas como IDS/IPS, SIEM u otras, que permitan detectar eventos anómalos o incidentes de seguridad.
- Garantizar el registro, trazabilidad y auditoría de las actividades realizadas sobre la infraestructura de red.

4.17.2 TRANSFERENCIA SEGURA DE INFORMACION

Toda transferencia interna o externa que involucre información institucional deberá realizarse por canales autorizados como correo institucional, OneDrive o intranet, con validación previa de autorizaciones, registro y trazabilidad. Se prohíben medios no aprobados (correos personales, apps no institucionales).

4.18 LINEAMIENTO DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La ETITC deberá asegurar que todos los procesos de adquisición, desarrollo, implementación, mantenimiento, actualización y retiro de sistemas de información, infraestructura tecnológica, software y aplicaciones se realicen bajo criterios de seguridad desde el diseño (Security by Design), incorporando controles que garanticen la confidencialidad, integridad y disponibilidad de la información; todo producto o servicio tecnológico adquirido o desarrollado deberá cumplir los requisitos de seguridad definidos por el SGSI, incluir evaluaciones de riesgos, validación de proveedores, revisión de código o pruebas de seguridad cuando aplique, y utilizar entornos controlados para desarrollo, pruebas y producción con adecuada segregación; cualquier modificación, mejora o actualización deberá gestionarse mediante procedimientos formales de gestión de cambios,

asegurando que no se introduzcan vulnerabilidades y que los controles de seguridad permanezcan vigentes; asimismo, queda prohibido el uso, instalación o desarrollo de sistemas, software o componentes tecnológicos no autorizados, y todo personal interno o externo involucrado deberá cumplir estrictamente con los lineamientos institucionales para garantizar la operación segura y confiable de los sistemas de información de la ETITC.

Lineamientos obligatorios:

a) Requisitos y evaluación previa

- Todo proyecto debe documentar requisitos de seguridad y privacidad (clasificación de la información, controles mínimos, cumplimiento legal), análisis de riesgos, y criterios de aceptación con condiciones de seguridad verificables.
- Cualquier adquisición debe pasar por revisión técnica de TI y validación de Planeación (SGSI) antes de la orden de compra/contrato.

b) Desarrollo e integración seguros

- Aplicar ciclo de vida de desarrollo seguro (SDLC): arquitectura segura, principios de ingeniería, segregación de entornos (dev/test/producción), gestión de dependencias y SBOM (inventario de componentes), gestión de secretos y claves, control de versiones y CI/CD con controles de seguridad.
- Exigir revisión de código (peer review) y pruebas de seguridad proporcionales al riesgo: SAST/DAST/IAST, pruebas de dependencia (SCA), hardening de contenedores e infraestructura como código (IaC).
- Para desarrollos tercerizados, exigir metodología segura, evidencias de pruebas, remediación de vulnerabilidades y transferencia de propiedad intelectual según contrato.

c) Gestión de cambios y configuración

- Todo cambio (software, infraestructura, parámetros, middleware, bases de datos, integraciones) se gestiona de acuerdo con los lineamientos establecidos por la entidad, teniendo en cuenta: solicitud, evaluación de riesgo/impacto, aprobación, pruebas, ventana de ejecución, plan de rollback, verificación post-implementación y registro.
- Mantener configuraciones endurecidas (baselines), registro de configuraciones (CMDB), y revisiones periódicas de desvíos (drift).

d) Mantenimiento, parches y vulnerabilidades

- Inventario de versiones/paquetes; parcheo oportuno de seguridad según criticidad (SLA de remediación); gestión de vulnerabilidades con escaneos periódicos y pruebas específicas antes de mover a producción.
- Prohibición expresa de operar en producción con vulnerabilidades críticas sin decisión formal de asunción de riesgo por Planeación y plan de mitigación aprobado.

e) Transferencia, datos y privacidad

- Para intercambios de datos: autorización previa, canales cifrados, controles de acceso, registro y trazabilidad; prohibido usar medios no autorizados (correos personales, apps no aprobadas).
- Cumplimiento de protección de datos personales; minimización de datos, retención y eliminación segura según clasificación y normativa.

f) Aceptación, puesta en producción y operación

- Ningún sistema o versión pasa a producción sin cumplir criterios de aceptación (funcionales, seguridad, desempeño, respaldo, monitoreo, logging, continuidad).
- Habilitar monitoreo, registro de eventos y alertas; documentar procedimientos operativos y de soporte; definir propietario y custodio.

g) Retiro y disposición final

- En el retiro: plan de descomisionamiento con borrado/anonimización de datos, revocación de accesos, retiro de claves/certificados, actualización de inventarios/CMDB, archivo de evidencias y contratos.

h) Prohibiciones

- **Prohibidos**: software/sistemas no autorizados (shadow IT), licenciamiento irregular, uso de servicios en la nube no aprobados, ambientes sin segregación, saltarse gestión de cambios, manipulación de controles de seguridad o deshabilitar MFA/registro.

4.18.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La ETITC deberá asegurar que todos los sistemas de información —adquiridos, desarrollados internamente o provistos por terceros— cumplan con los requisitos de seguridad necesarios para proteger la información institucional durante todo su ciclo de vida, incluyendo diseño, implementación, operación, mantenimiento y retiro.
Estos requisitos deberán definirse desde las etapas iniciales, bajo un enfoque basado en riesgos, incorporando criterios de confidencialidad, integridad, disponibilidad y cumplimiento normativo.

Para cada sistema de información, deberán establecerse de manera formal los requisitos mínimos de seguridad, incluyendo como mínimo:

- Controles de acceso lógico Aplicando el principio de mínimo privilegio y acorde a los roles y necesidades de uso.
- Requisitos de protección de datos personales y sensibles, conforme a la Ley 1581 de 2012 y normas complementarias.
- Uso de mecanismos criptográficos para la protección de la información en tránsito y en reposo, cuando aplique.
- Registro, monitoreo y trazabilidad de las acciones de usuarios y administradores.
- Validación de proveedores y cumplimiento de requisitos de seguridad en acuerdos contractuales, cuando el servicio sea provisto por terceros.
- Requisitos de disponibilidad, continuidad y resiliencia, de acuerdo con la criticidad del proceso.
- Gestión segura de vulnerabilidades, parches y actualizaciones.
- Ejecución de pruebas de seguridad antes de la puesta en operación o ante cambios significativos.

Los propietarios de los sistemas de información, en coordinación con el Proceso de Gestión de Información y Telecomunicaciones (TI) y el Líder del Sistema de Gestión de Seguridad de la Información, serán responsables de definir, documentar, revisar y aprobar los requisitos de seguridad correspondientes. Ningún sistema podrá entrar en producción, ni recibir cambios relevantes, sin verificar previamente el cumplimiento de los requisitos establecidos.

La ETITC deberá asegurar la actualización periódica de estos requisitos ante cambios tecnológicos, ajustes funcionales, resultados de auditorías, evolución de amenazas, cambios normativos o modificaciones en los procesos institucionales.

Estos requisitos servirán como base para el diseño seguro, desarrollo, pruebas, aceptación, operación y mantenimiento de los sistemas de información.

4.18.2 LINEAMIENTO DE DATOS DE PRUEBA

La ETITC deberá garantizar que los **datos utilizados en actividades de pruebas, validación, desarrollo y aseguramiento de calidad (QA)** sean gestionados de manera segura, evitando la exposición, tratamiento inadecuado o uso indebido de información institucional durante estos procesos. El uso de datos de prueba deberá asegurar la protección de la confidencialidad, integridad y disponibilidad de la información, incluso cuando esta no corresponda a ambientes productivos.

Los datos empleados en ambientes de prueba deberán ser, preferiblemente, **datos ficticios, anonimizados o generados artificialmente**, evitando el uso de información real o sensible. Únicamente en casos estrictamente necesarios y debidamente justificados

podrá utilizarse información productiva, lo cual requerirá autorización formal del Líder del Sistema de Gestión de Seguridad de la Información y del Proceso de Gestión de Información y Telecomunicaciones (TI), además de la aplicación de controles adicionales de seguridad y medidas de minimización de datos.

Cuando se utilicen datos anonimizados, estos deberán asegurar la imposibilidad de reconstruir o identificar a personas, procesos o activos institucionales. Las bases de prueba deberán mantenerse protegidas bajo los mismos principios de seguridad que rigen para los datos operativos, incluyendo controles de acceso lógico, gestión de privilegios, protección criptográfica cuando aplique, y almacenamiento seguro.

El acceso a datos de prueba será otorgado únicamente al personal autorizado para actividades de desarrollo, aseguramiento de calidad y soporte técnico, limitándose estrictamente al alcance requerido por sus funciones. Cualquier copia, derivado o base de prueba generada deberá contar con un responsable claramente definido y con un ciclo de vida controlado, que incluya creación, uso, modificación y eliminación segura.

Este lineamiento es obligatorio para todos los sistemas, proyectos y proveedores que intervengan en actividades de desarrollo o pruebas dentro de la ETITC, y deberá aplicarse de manera coherente con la segregación de ambientes definida en el numeral 4.9.4 del presente manual.

4.19 LINEAMIENTO DE RELACIONES CON LOS PROVEEDORES

La ETITC deberá establecer, implementar y mantener controles integrales para la gestión segura de las relaciones con proveedores, contratistas y terceros que tengan acceso, directo o indirecto, a información institucional, sistemas de información, infraestructura tecnológica, servicios digitales o activos críticos. Estos controles serán aplicados durante todo el ciclo de vida de la relación contractual, desde la selección del proveedor hasta la terminación del servicio, asegurando la protección de la información y la continuidad operativa.

La entidad garantizará que todos los acuerdos, contratos, órdenes de compra, convenios, servicios tercerizados y adquisiciones tecnológicas incluyan requisitos formales de seguridad de la información, confidencialidad, protección de datos personales, gestión de riesgos, cumplimiento normativo, niveles de servicio (SLA/OLA), deber de reporte de incidentes, cláusulas de auditoría y obligaciones postcontractuales. Ningún proveedor podrá iniciar actividades sin haber aceptado y firmado dichos compromisos.

Antes de iniciar la ejecución de cualquier contrato, se deberán suscribir acuerdos de confidencialidad (NDA) que incluyan cláusulas explícitas de seguridad de la información

aplicables durante y después de la terminación del contrato, garantizando la protección continua de los activos institucionales.

Como parte de la gobernanza del SGSI, la ETITC deberá realizar una evaluación previa del proveedor, que incluye:

- Análisis de riesgos asociado a la relación contractual.
- Revisión de la capacidad técnica y los controles de seguridad del proveedor.
- Verificación de cumplimiento normativo y contractual.
- Validación de certificaciones, políticas, infraestructura y prácticas de seguridad.
- Evaluación de la cadena de suministro del proveedor cuando aplique.

Durante la ejecución del contrato, se deberá asegurar:

- Supervisión continua del cumplimiento de requisitos de seguridad.
- Monitoreo del desempeño del proveedor y de los niveles de servicio (SLA).
- Gestión de cambios autorizada y documentada.
- Control y revocación oportuna de accesos otorgados a los proveedores.
- Reporte inmediato de incidentes, vulnerabilidades o fallas de seguridad.
- Gestión segura de la información compartida o procesada por terceros.

Queda estrictamente prohibido contratar, adquirir, habilitar, integrar o utilizar proveedores, servicios, plataformas, aplicaciones o componentes tecnológicos que no cumplan los requisitos de seguridad definidos por la ETITC o que vulneren las políticas del SGSI. Así mismo, se prohíbe otorgar accesos no autorizados o mantener accesos activos de proveedores después de la finalización del contrato.
Al finalizar la relación contractual, se deberá garantizar la correcta revocación de accesos, devolución y/o eliminación segura de la información, destrucción certificada cuando aplique, retiro de credenciales, desactivación de usuarios, actualización de inventarios y cierre formal del proveedor según los procedimientos del SGSI.

La ETITC establecerá lineamientos claros y requisitos específicos de seguridad para mitigar los riesgos asociados a cada proceso de contratación, asegurando que las relaciones con proveedores contribuyan a la protección de la información institucional y no generen vulnerabilidades en la operación, infraestructura o servicios.

4.20 SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

La ETITC deberá integrar de forma transversal la seguridad de la información dentro de su modelo de continuidad de negocio, garantizando que los procesos críticos, activos de

información, infraestructura tecnológica, servicios institucionales y dependencias externas cuenten con estrategias que aseguren la confidencialidad, integridad y disponibilidad ante interrupciones, fallas, incidentes mayores o desastres.

La entidad deberá realizar Análisis de Impacto al Negocio (BIA), evaluaciones de riesgos asociados a la continuidad y definir estrategias de recuperación que abarquen: respaldo y restauración de información, conmutación por falla, operación en modo degradado, recuperación de servicios críticos, redundancia tecnológica, continuidad de seguridad y retorno controlado a la normalidad. Dichas estrategias se documentarán en los Planes de Continuidad Tecnológica y Planes de Recuperación de Desastres (DRP), los cuales deberán ser actualizados, aprobados y supervisados por Planeación como órgano rector del SGSI.

El Proceso de Gestión de Información y Telecomunicaciones (GTI), en conjunto con el profesional responsable de continuidad, generará, mantendrá y ejecutará el Plan de Continuidad Tecnológica, asegurando que este incorpore los lineamientos del BIA, los requisitos de seguridad del SGSI, los controles de protección, la segregación de entornos y los mecanismos de restauración oportuna de servicios ante escenarios de contingencia.

Los planes deberán contener, como mínimo:

- Roles y responsabilidades claramente definidos.
- Procedimientos de activación, escalamiento, comunicación interna y externa.
- Estrategias de recuperación priorizadas según criticidad.
- Procedimientos de respaldo y restauración probados.
- Mecanismos para asegurar la protección de la información durante la contingencia.
- Criterios de retorno a la normalidad.
- Registro de lecciones aprendidas en cada activación o simulación.

La ETITC deberá diseñar y ejecutar un Plan de Pruebas de Continuidad que verifique la eficacia de las estrategias definidas y la capacidad real de recuperación. Estas pruebas deberán realizarse mínimo dos (2) veces al año e incluir, entre otros métodos:

- Prueba de lista de verificación (Checklist Test)
- Prueba de simulacro o ejercicio práctico (Simulation/Drill Test)

Los resultados deberán documentarse, analizarse y utilizarse para la mejora continua del plan, abordando brechas de desempeño, tiempos de respuesta y falencias en procesos o recursos.

Las áreas de la ETITC deberán actualizar los planes cada vez que se presenten cambios significativos en infraestructura, aplicaciones, procesos, información crítica, dependencias tecnológicas o proveedores. De igual forma, los proveedores y terceros identificados como críticos deberán cumplir los requisitos contractuales de continuidad y seguridad, demostrando capacidad de recuperación y disponibilidad conforme a las necesidades institucionales.

Todo funcionario, contratista o tercero deberá estar capacitado para ejecutar los planes que le correspondan, reportar incidentes de forma inmediata y cumplir con los procedimientos establecidos durante contingencias. Queda estrictamente prohibido realizar acciones o aplicar prácticas que comprometan la seguridad de la información, la integridad de los activos, el proceso de recuperación o la continuidad de los servicios institucionales, tanto durante la interrupción como en el restablecimiento de operaciones.

4.21 LINEAMIENTO DE GESTIÓN DE INCIDENTES

La ETITC deberá garantizar una gestión estructurada, oportuna y efectiva de los incidentes de seguridad de la información mediante la implementación de procesos formales para la identificación, reporte, registro, clasificación, análisis, contención, erradicación, recuperación, cierre y lecciones aprendidas. Todo incidente deberá gestionarse conforme a los lineamientos del SGSI, preservando la confidencialidad, integridad y disponibilidad de la información, así como la continuidad operativa de los servicios institucionales.

Gestión del reporte y notificación

Cualquier funcionario, docente, contratista, proveedor o tercero que detecte un evento, anomalía, vulnerabilidad, debilidad o posible incidente relacionado con la seguridad de la información deberá reportarlo de inmediato a través de la mesa de servicios institucional, utilizando los medios oficiales dispuestos para tal fin.
El no reporte oportuno será considerado una falta a las políticas de seguridad.

Coordinación y respuesta

El Grupo de Gestión de Información y Telecomunicaciones (TI) deberá seguir estrictamente los procedimientos establecidos para la gestión de incidentes y cumpliendo los tiempos de respuesta definidos. En la medida que se contrate la participación de un tercero para la gestión de incidentes, estas tareas pueden ser compartidas.

Documentación y trazabilidad

El Grupo Gestión de Informática Telecomunicaciones -GIT en coordinación con Gestión de Seguridad de la Información y/o el tercero encargado de gestionar los incidentes (Si existiere), deberá registrar y conservar toda la documentación asociada a los incidentes, incluyendo:

- Tipo y clasificación del incidente (p. ej., *phishing, malware, fuga de información, ransomware, defacement, intrusión, denegación de servicio*, entre otros).
- Cronología detallada del incidente.
- Evidencias recolectadas (logs, alertas, artefactos, capturas, reportes).
- Tiempos de detección, respuesta, contención, erradicación y recuperación.
- Responsables de atención según clasificación.
- Líneas de atención y procedimientos ejecutados.
- Indicadores de medición y reporte para auditoría y mejora continua.

La preservación de evidencias deberá cumplir los principios de cadena de custodia, evitando su alteración y garantizando su validez para auditorías o procesos disciplinarios/legales.

Acciones posteriores y mejora continua

Todo incidente deberá finalizar con:

- Cierre formal del caso.
- Documentación de lecciones aprendidas.
- Identificación de fallas de control, causas raíz y debilidades sistémicas.
- Ejecución de acciones correctivas y preventivas.
- Actualización de procedimientos, controles o configuraciones afectadas.

La gestión de incidentes será revisada periódicamente para mejorar la capacidad de respuesta institucional.

Responsabilidades institucionales

- Gestión de seguridad de la información: Análisis y gestión de controles (esta labor puede ser compartida con un tercero)
- Grupo de gestión de informática y telecomunicaciones (TI): Ejecución técnica de acciones de contención, erradicación y recuperación; registro de evidencias; actualización de controles (Esta labor puede ser compartida con un tercero).

- Planeación (SGSI): Supervisión del cumplimiento, evaluación de riesgos derivados, revisiones de desempeño y mejora del proceso.
- Áreas y funcionarios: Reporte inmediato, colaboración plena en la investigación y cumplimiento de procedimientos.
- Proveedores y terceros: Obligación de reportar incidentes, colaborar con la respuesta y cumplir las cláusulas contractuales de seguridad.

Prohibiciones

Queda estrictamente prohibido:

- Omitir el reporte de incidentes.
- Manipular, alterar o destruir evidencias.
- Realizar acciones no autorizadas durante la contención o investigación.
- Ocultar fallas de seguridad o vulnerabilidades.

Gestión de incidentes que afecten datos personales

La ETITC deberá gestionar los incidentes de seguridad de acuerdo con el GSI-SI-PC-05 Gestión de Incidentes de la Seguridad de la Información que involucren datos personales, garantizando la protección de los derechos de los titulares y el cumplimiento de las obligaciones legales y regulatorias aplicables.

Se considerarán incidentes de datos personales, entre otros:

- Acceso no autorizado a datos personales.
- Divulgación accidental o intencional de información personal.
- Pérdida, robo o extravío de información que contenga datos personales.
- Alteración no autorizada de datos personales.
- Destrucción accidental o indebida de información personal.
- Secuestro, cifrado malicioso o indisponibilidad de bases de datos que contengan datos personales.
- Transferencias o transmisiones no autorizadas de datos personales.

Gestión de incidentes por terceros

La ETITC podrá contratar o apoyarse en terceros especializados para la prestación de servicios relacionados con la detección, monitoreo, análisis, investigación, contención,

respuesta, recuperación y gestión de incidentes de seguridad de la información, incluyendo servicios de SOC, CSIRT, MSSP, análisis forense digital, monitoreo de seguridad, inteligencia de amenazas u otros servicios especializados de ciberseguridad.

La participación de terceros no exime a la ETITC de su responsabilidad sobre la gestión de los incidentes de seguridad de la información ni del cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

Todo tercero que participe en actividades de gestión de incidentes deberá:

- Cumplir los lineamientos, políticas, procedimientos y controles definidos por la ETITC.
- Suscribir acuerdos de confidencialidad y protección de la información.
- Cumplir las disposiciones sobre tratamiento y protección de datos personales cuando aplique.
- Garantizar la protección, integridad y confidencialidad de las evidencias recolectadas.
- Mantener la trazabilidad de las actividades ejecutadas.
- Reportar oportunamente los eventos e incidentes identificados.
- Cumplir los acuerdos de nivel de servicio (SLA) establecidos contractualmente.
- Permitir actividades de seguimiento, auditoría y verificación por parte de la ETITC.

La coordinación, supervisión y toma de decisiones frente a los incidentes continuará siendo responsabilidad de la ETITC a través del Grupo de Gestión de Información y Telecomunicaciones (TI), el Líder del Sistema de Gestión de Seguridad de la Información y las instancias de gobierno definidas por la entidad, quienes validarán las acciones ejecutadas por el tercero y autorizarán, cuando corresponda, las actividades que puedan generar impacto sobre los activos de información institucionales.

4.21.1 RECUPERACION Y RESTAURACION POST-INCIDENTE

La recuperación y restauración de servicios tras un incidente se ejecutará de forma controlada, priorizando servicios críticos, coordinando con Continuidad Tecnológica (4.19), y dejando evidencia de validación funcional y de seguridad.

4.22 IDENTIFICACION Y COMUNICACIÓN DE INFRAESTRUCTURA CRITICA

La ETITC identificará su infraestructura crítica, la documentará y comunicará a las partes interesadas pertinentes, articulando responsabilidades y planes de protección y continuidad, según lineamientos nacionales aplicables.

4.23 LINEAMIENTO DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS

La ETITC deberá garantizar que todos los proyectos institucionales —académicos, administrativos, tecnológicos o de transformación digital— incorporen de manera explícita y obligatoria los requisitos de seguridad de la información desde su formulación hasta su cierre, con el fin de proteger los activos institucionales, prevenir riesgos y asegurar el cumplimiento normativo durante todo el ciclo de vida del proyecto.

Todo proyecto deberá considerar, desde su fase inicial, los requisitos de seguridad y privacidad, incluyendo la identificación de activos involucrados, la clasificación de la información tratada, los riesgos asociados, los controles mínimos requeridos, el cumplimiento de la normativa vigente (datos personales, derechos de autor, propiedad intelectual, transparencia), y los criterios de aceptación en materia de seguridad.

La gestión de cada proyecto deberá incluir actividades de análisis de riesgos, definición de controles, validación técnica de seguridad, y verificación de impacto sobre los sistemas de información, procesos institucionales e infraestructura tecnológica. Las fases de diseño, desarrollo, adquisición, integración, pruebas y despliegue deberán realizarse de manera segura, siguiendo los procedimientos de gestión de cambios, segregación de ambientes, pruebas de seguridad, documentación técnica y aseguramiento de calidad.

El Líder del Sistema de Gestión de Seguridad de la Información y el Proceso de Gestión de Información y Telecomunicaciones (TI) deberán participar como partes interesadas en la revisión y validación de los entregables del proyecto, asegurando que estos cumplan los requisitos de seguridad definidos y que no introduzcan vulnerabilidades en el entorno institucional. Los responsables del proyecto deberán garantizar la trazabilidad de las decisiones, actividades y controles aplicados, dejando evidencia en los repositorios institucionales autorizados.

Ningún proyecto podrá avanzar a etapas críticas ni ser puesto en operación sin la validación formal de seguridad, que certifique el cumplimiento de los requisitos definidos, la implementación de controles, la gestión adecuada de los riesgos y la inexistencia de impactos no tratados. Cualquier excepción deberá ser aprobada por la Alta Dirección, con justificación documentada y controles compensatorios definidos.

Este lineamiento es de obligatorio cumplimiento para todo proyecto ejecutado por personal interno, contratistas o proveedores, y constituye un componente fundamental para asegurar que el crecimiento y la modernización institucional se realicen bajo estándares de protección, confiabilidad, trazabilidad y continuidad operativa.

4.24 LINEAMIENTO DE SEGURIDAD EN SERVICIOS EN LA NUBE

La ETITC deberá garantizar que el uso de servicios en la nube institucionales o de terceros se realice de manera segura, controlada y conforme a los lineamientos del SGSI, asegurando la protección de la información durante todo su ciclo de vida.
Todo servicio en la nube deberá ser evaluado previamente en términos de seguridad, cumplimiento normativo, ubicación de datos, responsabilidad compartida y riesgos asociados.
Se deberán aplicar como mínimo las siguientes medidas:

- Uso exclusivo de servicios en la nube autorizados por la ETITC.
- Control de accesos con MFA obligatorio.
- Cifrado de la información en tránsito y en reposo.
- Monitoreo continuo de actividades y registros.
- Gestión de identidades y privilegios bajo principio de mínimo privilegio.
- Evaluación de proveedores cloud conforme al lineamiento de terceros.

Se prohíbe el uso de servicios en la nube no autorizados para el almacenamiento o procesamiento de información institucional.

4.25 LINEAMIENTO DE PROTECCIÓN DE DATOS PERSONALES Y ATENCIÓN DE DERECHOS DE LOS TITULARES

La ETITC protege los datos personales que recolecte, almacene, use, circule, transmita o suprima, asegurando que su tratamiento se realice conforme a la legislación legal vigente en protección de datos personales, los principios de privacidad de la información, la Política de Protección de Datos Personales, de la Escuela Tecnológica Instituto Técnico Central y los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI).

La ETITC realizará el tratamiento de los datos personales únicamente para finalidades legítimas, específicas, explícitas e informadas al titular, relacionadas con el desarrollo de su misión institucional, la prestación de servicios académicos, administrativos, contractuales, laborales, legales, disciplinarios, financieros y demás actividades necesarias para el cumplimiento de sus funciones.
Para tal fin, la Entidad implementará controles administrativos, físicos, técnicos y organizacionales que permitan proteger los datos personales contra pérdida, acceso no autorizado, alteración, divulgación, destrucción, uso indebido o cualquier tratamiento no autorizado o fraudulento.

Los titulares de los datos personales podrán ejercer sus derechos de:

- Conocer la información personal que repose en las bases de datos de la ETITC.
- Solicitar la actualización de sus datos personales.
- Solicitar la rectificación de información inexacta, incompleta o desactualizada.
- Solicitar la supresión de los datos personales cuando proceda legalmente.
- Solicitar la revocatoria de la autorización otorgada para el tratamiento de sus datos personales.
- Presentar consultas, quejas o reclamos relacionados con el tratamiento de sus datos personales.

Canales de atención

Las solicitudes relacionadas con el ejercicio de los derechos de los titulares deberán presentarse a través de los canales institucionales definidos por la ETITC, tales como:

- Sistema Institucional de PQRSD.
- Ventanilla Única de Correspondencia.
- Correo electrónico institucional atencionalciudadano@itc.edu.co relacionado con Protección de Datos Personales.
- Página web institucional

4.25.1 PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES Y TRATAMIENTO DE DATOS PERSONALES DE MENORES DE EDAD

El tratamiento de datos personales de niños, niñas y adolescentes deberá respetar su interés superior y asegurar el respeto de sus derechos fundamentales. Dicho tratamiento solo podrá realizarse en los casos permitidos por la normatividad vigente y observando los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Los sistemas de información, aplicaciones, portales web, aulas virtuales, servicios digitales y demás plataformas institucionales dirigidas o accesibles a menores de edad deberán incorporar medidas de privacidad por diseño y privacidad por defecto, garantizando que:

- Solo se recolecte la información estrictamente necesaria para el cumplimiento de finalidades legítimas y autorizadas.
- Los perfiles de usuario se configuren con el mayor nivel de privacidad posible.
- Se restrinja el acceso a información personal por parte de terceros no autorizados.
- Se impida el perfilamiento con fines comerciales, publicitario o de mercadeo dirigido menores de edad.
- Se prohíba la comercialización, cesión o explotación de datos personales para finalidades distintas de las autorizadas.
- Se evalúen los riesgos asociados al tratamiento de datos cuando este pueda afectar los derechos y libertades de los menores.

Accesibilidad e inclusión digital

La ETITC promoverá que los portales institucionales, plataformas educativas, aplicativos y servicios digitales dirigidos o utilizados por menores de edad sean diseñados y operados bajo criterios de accesibilidad, usabilidad e inclusión, atendiendo estándares internacionales vigentes de accesibilidad digital y las disposiciones nacionales aplicables, incorporando cuando corresponda enfoques diferenciales y ajustes razonables.

Gestión de incidentes relacionados con la protección de menores

Cuando se identifique material, contenido, información o evidencias relacionadas con explotación sexual infantil, abuso sexual de menores, pornografía infantil o cualquier otra

conducta que vulnere los derechos de niños, niñas o adolescentes a través de los recursos tecnológicos institucionales, la ETITC deberá:

- Preservar las evidencias siguiendo principios de integridad y cadena de custodia.
- Reportar inmediatamente la situación a las autoridades competentes.
- Escalar el caso a las entidades que correspondan según la normatividad vigente.
- Activar los mecanismos institucionales de atención y gestión de incidentes.
- Garantizar la confidencialidad y la protección de la información asociada al caso y de las personas involucradas.

5. ALCANCE MSPI (MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN)

El Modelo de Seguridad y Privacidad de la Información (MSPI) aplica de manera integral a todas las actividades, procesos, servicios, unidades académicas y administrativas de la ETITC, abarcando el ciclo completo de vida de la información institucional desde su creación, uso, almacenamiento, transmisión, procesamiento y eliminación, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de los datos. Su alcance comprende la totalidad de los activos de información, incluyendo infraestructura tecnológica, servicios en la nube, sistemas de información, aplicaciones internas y externas, dispositivos móviles, redes de comunicaciones, recursos de almacenamiento, plataformas académicas y administrativas, así como las operaciones que dependen de ellos.

El MSPI es obligatorio para todo el personal que interactúe con información institucional: funcionarios, contratistas, docentes, personal administrativo, estudiantes con acceso autorizado, proveedores y terceros que procesen, administren o soporten información o servicios de la ETITC. Asimismo, cubre la gestión de riesgos de seguridad y privacidad, la implementación y uso de controles técnicos y organizacionales, la administración de incidentes de seguridad, la continuidad de los servicios, la protección de datos personales, el cumplimiento normativo y el aseguramiento de las obligaciones legales vinculadas al tratamiento de la información.

El alcance también incluye los servicios tercerizados o administrados por proveedores, quienes deberán cumplir con los requisitos definidos por la institución en materia de seguridad, privacidad, disponibilidad y niveles de servicio. Esto implica que cualquier solución tecnológica o servicio contratado debe alinearse con los principios y controles del

MSPI, incluyendo la evaluación de riesgos, cláusulas de seguridad, acuerdos de confidencialidad y mecanismos de supervisión.

Finalmente, el MSPI abarca los mecanismos para la medición, auditoría, seguimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, garantizando que los controles se mantengan actualizados frente a nuevas amenazas, cambios tecnológicos, evolución normativa y necesidades institucionales, con el fin de preservar la resiliencia y confiabilidad de los servicios que soportan la misión educativa y administrativa de la ETITC.

IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La ETITC establecerá y mantendrá un proceso sistemático, continuo y documentado para la identificación, análisis, valoración y priorización de los riesgos de seguridad y privacidad de la información, conforme a los lineamientos del MSPI, la normativa aplicable y las buenas prácticas internacionales. Este proceso inicia con la identificación de los activos de información, sus propietarios y su clasificación, lo cual permite determinar el contexto de protección requerido. Para cada activo se identificarán amenazas, vulnerabilidades, escenarios de riesgo y posibles impactos sobre la confidencialidad, integridad y disponibilidad, considerando tanto riesgos tecnológicos como riesgos operacionales, humanos, legales y de terceros.

Una vez identificados los riesgos, se realizará su análisis y valoración empleando metodologías institucionales alineadas con ISO/IEC 27005, determinando la probabilidad de ocurrencia y el nivel de impacto para asignar un nivel de riesgo inherente y residual. Los riesgos serán categorizados y priorizados para orientar la toma de decisiones, la definición de controles, la asignación de recursos y la planificación de acciones de tratamiento. Los propietarios de proceso y propietarios de activos deberán participar activamente en la valoración, ya que son responsables de validar la criticidad operativa y los impactos al negocio.

Cada riesgo identificado deberá contar con un tratamiento documentado, el cual podrá incluir controles preventivos, correctivos o detectivos; controles compensatorios; aceptación formal del riesgo; transferencia; o mitigación mediante acciones técnicas y organizacionales. Todo tratamiento será monitoreado por el SGSI y revisado periódicamente en función de cambios en la infraestructura, evolución de las amenazas, resultados de auditorías, hallazgos de incidentes, requisitos legales y la evolución de la institución.

La identificación y valoración de riesgos deberá actualizarse de manera periódica y cada vez que se presenten cambios significativos en los sistemas, servicios, procesos, proveedores o en el entorno tecnológico. Los resultados serán insumo para la mejora continua del SGSI, la planificación de controles, la gestión de vulnerabilidades, la continuidad del negocio y la toma de decisiones estratégicas sobre la seguridad de la información en la ETITC.

NOTA: Esta actividad es responsabilidad del Dueño del Proceso y del Dueño del Activo, con el acompañamiento de Seguridad de la Información para orientar y validar la correcta valoración. Los riesgos deben actualizarse cuando haya cambios en los procesos, se presenten incidentes, surjan hallazgos de auditorías o aparezcan nuevas amenazas.

6. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La ETITC establecerá un proceso formal y sistemático para el tratamiento de los riesgos de seguridad y privacidad de la información, asegurando que los riesgos identificados y valorados sean gestionados de manera coherente con los objetivos institucionales, la normativa vigente y los lineamientos del MSPI. El tratamiento del riesgo deberá seleccionarse con base en el nivel de riesgo residual aceptable para la institución, priorizando aquellos riesgos que representen amenazas significativas a la confidencialidad, integridad y disponibilidad de los activos de información.

Para cada riesgo identificado, se deberá definir un plan de tratamiento que especifique la estrategia adoptada, pudiendo incluir:

1. **Mitigación:** Implementación o fortalecimiento de controles técnicos, administrativos u organizacionales (por ejemplo: endurecimiento de sistemas, control de accesos, cifrado, monitoreo, procedimientos, entrenamiento, segmentación de red o actualizaciones de seguridad).
2. **Transferencia:** Delegación parcial o total del riesgo mediante seguros, acuerdos contractuales, proveedores externos o servicios especializados.
3. **Evitar el riesgo:** Eliminación de la actividad, proceso o tecnología que origina el riesgo, cuando su permanencia represente un impacto inaceptable.
4. **Aceptar el riesgo:** Aprobación formal del riesgo residual cuando se encuentre dentro de los niveles tolerables definidos por la Alta Dirección y exista justificación documentada.

Todo tratamiento deberá estar documentado y contará con responsables, recursos, plazos, métricas y evidencias de ejecución, registradas en el sistema institucional de riesgos del

SGSI. La implementación del plan de tratamiento será monitoreada por el propietario del riesgo y validada por Seguridad de la Información, garantizando que las acciones adoptadas reduzcan efectivamente el riesgo residual a niveles aceptables.

La eficacia del tratamiento deberá revisarse periódicamente, así como en respuesta a cambios significativos en la infraestructura tecnológica, en los servicios institucionales, en los resultados de auditorías, en nuevos patrones de amenazas, en la materialización de incidentes o cuando existan actualizaciones normativas. El proceso de tratamiento forma parte del ciclo de mejora continua del SGSI y constituye un insumo fundamental para la toma de decisiones, priorización de inversiones y fortalecimiento de la seguridad institucional.

7. EXCEPCIONES A LOS LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CONTROLES

La ETITC podrá autorizar excepciones temporales o permanentes frente a los lineamientos establecidos en el presente Manual cuando existan razones técnicas, operativas, tecnológicas, presupuestales, regulatorias o relacionadas con la continuidad de la prestación de los servicios institucionales. Las excepciones permanentes solo podrán aprobarse cuando exista una justificación técnica o normativa debidamente documentada.

No podrán aprobarse excepciones que impliquen el incumplimiento de requisitos legales, regulatorios, contractuales, de protección de datos personales o de otras obligaciones de cumplimiento aplicables a la ETITC, salvo disposición expresa de la autoridad competente.

Toda excepción deberá:

- Solicitarse por el líder del proceso o la dependencia donde se presente la necesidad, a través de la mesa de servicios institucional.
- Estar debidamente justificada y documentada.
- Encontrarse soportada en un análisis de riesgos de seguridad de la información.
- Identificar los activos de información, procesos o servicios afectados.
- Establecer e implementar controles compensatorios que reduzcan el riesgo residual a niveles aceptables cuando la excepción afecte controles de seguridad definidos por el SGSI.

- Definir una vigencia y fecha de revisión.

El estudio de las solicitudes debe contar con la participación y análisis del área Gestión de Informática y Telecomunicaciones, de Gestión de Seguridad de la Información.

Una vez realizado el análisis técnico, operativo y de riesgos, la solicitud de excepción deberá consolidarse en un informe que incluya la justificación, los riesgos identificados, los controles compensatorios definidos y la recomendación correspondiente. Dicho informe será presentado al líder del proceso para su evaluación y aprobación formal, de acuerdo con el nivel de riesgo y el impacto institucional asociado.

Las excepciones otorgadas deberán registrarse y mantenerse como información documentada del Sistema de Gestión de Seguridad de la Información (SGSI), conservando la trazabilidad de su análisis, aprobación, seguimiento, revisión, renovación cuando aplique y cierre.

Las excepciones aprobadas deberán ser objeto de seguimiento y revisión periódica para verificar que las condiciones que justificaron su aprobación continúan vigentes, que los controles compensatorios mantienen su efectividad y que el riesgo residual permanece dentro de los niveles aceptables definidos por la ETITC.

8. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La Escuela Tecnológica Instituto Técnico Central (ETITC), a través del Sistema de Gestión de Seguridad de la Información (SGSI), articulará las actividades de sensibilización, concienciación y fortalecimiento de competencias en Seguridad y Privacidad de la Información con el Plan Institucional de Capacitación (PIC) y demás estrategias institucionales de formación.

Para tal fin, el proceso de Seguridad de la Información propondrá e incorporará periódicamente contenidos específicos relacionados con seguridad de la información, ciberseguridad, protección de datos personales, gestión de riesgos, uso seguro de los activos de información, prevención de incidentes, ingeniería social, phishing, manejo seguro de credenciales, protección de información institucional y demás temáticas que contribuyan al fortalecimiento de la cultura de seguridad en la entidad.

9. CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN

La ETITC promoverá una Cultura Institucional de Seguridad de la Información basada en la concientización permanente, el cumplimiento normativo y la adopción de comportamientos seguros por parte de todos los funcionarios, docentes, contratistas, proveedores y terceros con acceso a la información institucional. Para ello, el Proceso de Talento Humano y Contratación integrará de manera obligatoria las temáticas de seguridad de la información dentro de los programas de inducción, reinducción, capacitación continua, planes de formación y actividades de desarrollo del talento, asegurando que todo personal vinculado conozca, comprenda y aplique las políticas, lineamientos y responsabilidades asignadas dentro del SGSI.

El Líder del sistema de Gestión de Seguridad de la Información, El profesional de Ciberseguridad, Líder de gestión de El Proceso de Gestión de Información y Telecomunicaciones (TI) y/o terceros, brindarán acompañamiento técnico en estos espacios formativos, suministrando contenidos actualizados sobre amenazas, riesgos, incidentes comunes, buenas prácticas, uso seguro de los recursos tecnológicos, clasificación de la información y responsabilidades legales aplicables.

Para fortalecer la cultura organizacional, la entidad implementará estrategias sostenidas de sensibilización, comunicación efectiva y gestión del cambio, orientadas a fomentar hábitos seguros y una actitud proactiva de protección de la información. Estas estrategias incluirán campañas institucionales, simulaciones, material pedagógico, actividades de participación, mensajes orientadores y acciones de refuerzo que contribuyan a interiorizar el autocuidado digital como parte del comportamiento cotidiano de los funcionarios, docentes, contratistas, proveedores, terceros y usuarios.

La construcción de esta cultura deberá contemplar:

- **Identificación de perfiles de conocimiento:** segmentación del personal de acuerdo con su rol, nivel de acceso, tipo de información manipulada y competencias tecnológicas.

- **Definición del público objetivo por nivel de riesgo:** priorizando áreas críticas o con mayor exposición a amenazas.

- **Planeación anual de temáticas formativas:** basadas en incidentes reportados, tendencias de ciberataques, controles ISO 27001 aplicables y necesidades estratégicas del SGSI.

- **Estrategias de apropiación del cambio:** alineadas al modelo de gestión del cambio institucional, promoviendo la adopción gradual y sostenida de prácticas seguras.

- **Medición y seguimiento:** evaluación periódica mediante indicadores de impacto, participación, cumplimiento, resultados de simulaciones de phishing, encuestas de percepción y auditorías internas.

El fortalecimiento de la cultura de seguridad de la información es un componente fundamental del SGSI y constituye una responsabilidad compartida que busca garantizar que la protección de los activos de información sea un comportamiento natural, consistente y alineado con los objetivos estratégicos de la ETITC.

10. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de La ETITC.

Las políticas de Seguridad de la Información de la ETITC serán aprobadas formalmente por la Alta Dirección, en cumplimiento de sus responsabilidades de liderazgo y gobernanza del Sistema de Gestión de Seguridad de la Información (SGSI). A partir de su aprobación, las políticas entrarán en vigor y serán de obligatorio cumplimiento para todos los funcionarios, docentes, contratistas, proveedores y terceros con acceso a los activos de información de la entidad.

La Alta Dirección garantizará que las políticas se mantengan actualizadas, pertinentes y alineadas con los riesgos institucionales, los requisitos legales y contractuales aplicables, y los objetivos estratégicos de la ETITC. Para ello, las políticas deberán ser revisadas al menos una vez al año, como parte del ciclo de mejora continua del SGSI, e igualmente cuando se presenten cualquiera de las siguientes condiciones:

- **Incidentes de seguridad de la información** que evidencien brechas en los controles, cambios en las amenazas o fallas en el cumplimiento de lineamientos vigentes.

- **Modificaciones tecnológicas, organizacionales o normativas** que afecten el tratamiento, almacenamiento, acceso o intercambio de información.

- **Cambios significativos en los procesos, estructura o funciones institucionales**, que requieran actualización de roles, responsabilidades o controles.

- **Hallazgos derivados de auditorías internas, externas, revisiones por la dirección o evaluaciones de riesgos.**

Toda actualización deberá registrarse con control de versiones y conservar sus evidencias de aprobación, fecha de entrada en vigencia, alcance de los cambios y responsables involucrados. El Líder del sistema de Gestión de Seguridad de la Información y el Líder de gestión de El Proceso de Gestión de Información y Telecomunicaciones (TI) serán responsables de proponer ajustes, justificar las modificaciones requeridas y coordinar su revisión con los líderes de proceso pertinentes.

La revisión sistemática de las políticas garantiza su vigencia, aplicabilidad y eficacia, fortaleciendo la capacidad de la ETITC para proteger los activos de información y mantener la coherencia del SGSI con las mejores prácticas internacionales.

11. INCUMPLIMIENTOS Y SANCIONES

Todos los funcionarios, docentes, estudiantes, contratistas, proveedores y terceros que tengan acceso, uso, administración o interacción con los activos de información de la ETITC deberán cumplir las disposiciones, lineamientos y controles establecidos en la presente Política y en los documentos que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI).

El desconocimiento de la Política y de los Lineamientos de Seguridad y Privacidad de la Información no exime del cumplimiento de las obligaciones establecidas ni de las responsabilidades derivadas de su incumplimiento.

Cualquier incumplimiento, desconocimiento o vulneración de las disposiciones contenidas en esta política será considerado una infracción a las normas internas relacionadas con la protección de la información y el uso adecuado de los recursos tecnológicos institucionales, pudiendo dar lugar a medidas correctivas, preventivas, disciplinarias, administrativas, laborales, contractuales, civiles o penales, según la naturaleza, gravedad e impacto de los hechos, y de conformidad con la normatividad vigente aplicable.

Reporte de incumplimientos

Todo funcionario, docente, estudiante, contratista, proveedor, tercero o cualquier persona que identifique, detecte o tenga conocimiento de un posible incumplimiento de las Políticas y Lineamientos de Seguridad y Privacidad de la Información deberá reportarlo oportunamente a través de los canales institucionales definidos por la ETITC, tales como:

Mesa de Servicios Institucional.
Líder de Gestión de Seguridad de la Información.

Análisis y gestión de los incumplimientos

Los incumplimientos reportados serán gestionados inicialmente por Gestión de Seguridad de la Información, el cual actuará como instancia técnica responsable de realizar el análisis preliminar de los hechos, la valoración del impacto y la emisión del concepto técnico correspondiente, en coordinación con las áreas competentes cuando sea necesario.

La actuación de Gestión de Seguridad de la Información no sustituye ni limita las competencias disciplinarias, contractuales, administrativas o legales asignadas a otras dependencias de la entidad.

Cuando del análisis realizado se evidencie una posible falta disciplinaria, se elaborará por parte del Líder de Gestión de Seguridad de la Información un Informe Técnico y remitirá a la Líder de Control Disciplinario, de la Secretaría General, para que se efectúe la evaluación de su pertinencia y adelanten las actuaciones que resulten procedentes conforme a la normatividad vigente.

Cuando el incumplimiento involucre a estudiantes el caso será remitido a la Dirección del Instituto Bachillerato Técnico Industrial, IBTI, o la Decanatura de Facultad competente, según sea el caso, para su análisis y trámite conforme a lo establecido en la reglamentación vigente y aplicable.

Cuando el incumplimiento involucre a contratistas, proveedores o terceros, será remitido al supervisor correspondiente y al área de Gestión de Adquisiciones, de la Vicerrectoría Administrativa y Financiera; la entidad podrá aplicar las medidas contractuales establecidas, incluyendo requerimientos formales, planes de mejoramiento, sanciones contractuales, declaratorias de incumplimiento o cualquier otra actuación prevista en el contrato y en la normatividad vigente.

Cierre

Todos los incumplimientos deberán quedar debidamente documentados y registrados, garantizando su trazabilidad desde el reporte hasta el cierre. Asimismo, deberán gestionarse mediante acciones correctivas, preventivas o disciplinarias, según corresponda.

12. NORMATIVIDAD APLICABLE

Decretos

- Decreto 1078 de 2015 (Gobierno Digital y sector TIC), Título 9: Política de Gobierno Digital.
- Decreto 1074 de 2015, Capitulo 25, Reglamentación parcial de la Ley 1581 de 2012

Resoluciones y lineamientos

- Resolución MinTIC 500 de 2021 (adopta el MSPI). ARTÍCULO 4. Sistema de gestión de seguridad de la información y seguridad digital.
- Resolución MinTIC 2277 de 2025 (actualización del MSPI). ARTÍCULO 1. Actualización del anexo 1 de la resolución número 500 de 2021

Normas técnicas

- ISO/IEC 27001:2022. Cláusula 5. Liderazgo, numeral 5.2 Política.
- ISO/IEC 27005:2022. Identificación, Análisis, Evaluación, Tratamiento, Aceptación y Monitoreo del Riesgo.

13. REFERENCIAS

GIT-PC-15 Vinculación y/o desvinculación de Acceso a los Sistemas de Información
GSI-SI-ME-01 Identificar, Clasificar y Valorar los Activos de Información de la ETITC.
GSI-SI-PC-05 Gestión de Incidentes de la Seguridad de la Información

14. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
30/09/2016	1	Adopción del Documento.
19/04/2017	2	Inclusión del etiquetado del documento. Modificación de la Política General de Seguridad de la Información.
09/04/2018	3	Actualización del capítulo 7. Sanciones. Actualización de las políticas relacionadas con sistemas de información.

FECHA	VERSIÓN	CAMBIOS
		Actualización de la Política de Protección de los Datos de Prueba. Actualización de la Política de Controles Criptográficos.
30/04/2019	4	Eliminación del Comité de Seguridad de la Información e inclusión del Comité Institucional de Gestión y desempeño. Inclusión de la Política General de Seguridad de la Información dentro del marco de la Política del Sistema de Gestión Integrado. Cambios en la redacción del documento. Adopción de los lineamientos de la estrategia de Gobierno Digital en el Manual.
30/04/2020	5	Cambios en la redacción del documento. Actualización de la sección términos y definiciones. Actualización 9.1- Política de Estructura Organizacional de Seguridad de la Información Inclusión de la 20.3- Política de Uso de Herramientas Institucionales en Teletrabajo
26/02/2021	6	Cambios en la redacción del documento Adopción lineamientos protección de datos personales
19/10/2022	7	Cambios en la redacción del documento Cambio de frases “Servidores públicos, Proveedores, Estudiantes, Ciudadanos y/o Visitantes”; y “Servidores públicos, Estudiantes, Proveedores y Partes Interesadas” por Servidores Públicos, Proveedores y demás partes interesadas. Actualización sección 14. POLÍTICAS DE SEGURIDAD FISICA Y DEL ENTORNO. Adopción lineamientos de carné digital en la 14.1- Política de Áreas Seguras, Sección- Servidores Públicos, Proveedores y demás partes interesadas. Inclusión de nueva Política 14.3- Política de Seguridad para el Ingreso de Equipos Externos.

FECHA	VERSIÓN	CAMBIOS
		Asignación de numeral 14.3- al numeral 14.4- Política de Escritorio Limpio y Pantalla Limpia.
11/09/2023	8	Se realizan las siguientes mejoras al manual de políticas de seguridad de la información: Actualización sección 4. Términos y Definiciones el concepto de Teletrabajo suplementario. Actualización Sección 7. Sanciones: Tomando como base la derogatoria del Código Único Disciplinario (Ley 734 de 2022, Artículo 48 #43) por cambio al Código General Disciplinario (Ley 1952 de 2019. Artículo 55 #1). Inclusión de la periocidad y tipo de backup y lugar de almacenamiento en la sección 15.3- Política de Copias de Respaldo de la Información Inclusión del rol y la responsabilidad del líder del SGSI en la sección 15.4- Política de Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información. Inclusión del rol y la responsabilidad del Líder del SGSI, ante la política 13. POLÍTICAS DE CRIPTOGRAFÍA. Inclusión del rol y responsabilidad del área de Contratación donde incluya las Obligaciones del Contratista, definidas en el formato GAD-
10/08/2026	9	Se fortalece las responsabilidades relacionadas con la protección de la información, la gestión de riesgos, el cumplimiento normativo y el tratamiento adecuado de los datos institucionales. En este sentido los cambios más significados están relacionados con: • Alineación con ISO 27001:2022, ISO 27005:2022 y MSPI 2025. • Inclusión de gestión formal de riesgos. • Incorporación de gestión de excepciones.

FECHA	VERSIÓN	CAMBIOS
		• Formalización de responsabilidades de los líderes de proceso sobre activos. • Inclusión de estudiantes y terceros dentro del alcance. • Fortalecimiento de controles de ciberseguridad (MFA, SIEM, hardening, vulnerabilidades). • Fortalecimiento de privacidad y protección de datos personales. • Mayor control sobre proveedores.

ELABORÓ	REVISÓ	APROBÓ
LUIS JAVIER TOVAR TURCIO Líder del Sistema de Gestión de Seguridad de la Información **ÁNGELA ADRIANA PULIDO RIVERA** Profesional de Ciberseguridad **ERIKA VIVIANA CHACÓN GAMBA** Profesional de Continuidad	**YANETH JIMENA PIMIENTO CORTÉS** Líder de Gestión del Sistema Integrado de Aseguramiento **YAZMIN ANTON SANTIAGO CABRERA** Profesional Sistema Gestión de Calidad	**Comité Institucional de Gestión y Desempeño.**