ACUERDO NÚMERO **012** **DE**

(**26 de julio de 2024**)

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

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

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

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

Que, la Resolución 00500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

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

Que, el Decreto 0529 de 2024 modifica parcialmente el Capítulo 2 del Título 3 de la Parte 5 del Libro 2 del Decreto1075 de 2015 - Único Reglamentario del Sector Educación.

Que, en la sesión del 13 de junio de 2024 el Comité de Gestión y Desempeño Institucional validó propuesta presentada por la Rectoría para actualizar la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad de la Escuela Tecnológica Instituto Técnico Central. En tal sentido, la Secretaría Técnica emitió Certificación.

Que, en sesión ordinaria del 17 de julio de 2024 el Consejo Directivo discutió y aprobó la propuesta presentada por la Rectoría para actualizar la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad de la Escuela Tecnológica Instituto Técnico Central.

En mérito de lo anteriormente expuesto,

ACUERDA:

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

Artículo 2°-. Alcance. La política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad da comienzo desde la aplicación de los lineamientos institucionales en materia de Seguridad Digital, estos son aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ETITC, por tal motivo, deben ser conocidas y cumplidas por todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

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

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

Artículo 5°-. Vigencia. El presente Acuerdo rige a partir de la fecha de su publicación.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los 26 días del mes de julio de 2024.

La Presidente del Consejo Directivo,

ADRIANA MARÍA LÓPEZ JAMBOOS

El Secretario del Consejo Directivo

EDGAR MAURICIO LÓPEZ LIZARAZO

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

ANEXO ÚNICO

POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCION DE LA PRIVACIDAD.

1. Objetivo

Establecer lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad para la ETITC, con el fin de cumplir con los requisitos de seguridad digital alineados al modelo de seguridad y privacidad de la información de Gobierno Digital, que mediante su implementación permita contar con ambientes seguros que protejan los activos de información y aseguren el uso adecuado de los recursos, preservando la confidencialidad, integridad, disponibilidad y autenticación segura como principios esenciales para garantizar la continuidad del servicio.

2. Alcance

Desde la aplicación de los lineamientos institucionales en materia de Seguridad Digital, estos son aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ETITC, por tal motivo, deben ser conocidas y cumplidas por todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

3. Compromiso

La Alta Dirección de la ETITC aprueba los lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad, como muestra de su compromiso mediante el SGSI y el MSPI de Gobierno Digital.

La Alta Dirección demuestra su compromiso de apoyo a través de:

- La revisión y aprobación de lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad.
- La promoción activa de una cultura de seguridad de la información en los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas.
- Facilitar la divulgación de estos lineamientos a todos los Servidores Públicos, Proveedores, contratistas y demás partes interesadas.
- El aseguramiento de los recursos adecuados para implementar y mantener los lineamientos de seguridad de la información, contenidas en esta política.
- La verificación del cumplimiento de los lineamientos aquí mencionadas.

4. Glosario

- **Activo de información:** Todo lo importante para las actividades, declarado un "bien", por lo que tiene un valor significativo para el desempeño de las actividades de la institución.
- **Acuerdo de Confidencialidad:** Manifiesta querer mantener la confidencialidad de la información comprometiéndose a no divulgar, usar o explotar la información confidencial a la que acceden por la labor que desarrollan dentro de la misma.
- **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:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Ciberamenaza:** Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- **Ciberataque:** Intento deliberado de acceder, manipular, dañar o destruir sistemas informáticos, redes o dispositivos conectados a internet. Estos ataques pueden tener diversos objetivos, como robar información confidencial, interrumpir el funcionamiento normal de un sistema, extorsionar a individuos o empresas, o incluso causar daños físicos en infraestructuras críticas.

- **Ciberseguridad:** Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes, dispositivos y datos contra ataques cibernéticos, accesos no autorizados, daños y pérdidas. Su objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de la información y los recursos digitales.

- **Cifrado:** Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **Clave criptográfica:** es un parámetro que se utiliza junto con un algoritmo criptográfico para transformar, validar, autenticar, cifrar o descifrar datos.

- **Confidencialidad:** es la garantía de que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella.

- **Control:** Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

- **Continuidad del servicio:** Capacidad de la organización para prevenir, atender, recuperar y restaurar las funciones críticas del negocio ante un evento, de tal forma que continúen, sin importar las circunstancias.

- **Criptografía:** es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

- **Custodio de la información:** Son los líderes de las áreas.

- **Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

- **Hacking ético:** Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **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:** es la salvaguarda de la exactitud y totalidad de la información y los métodos de procesamiento de esta.

- **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes a la Escuela.

- **Logs de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información y redes de datos de la universidad. Dichos

eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **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.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Teletrabajo suplementario:** Trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la institución y un lugar fijo fuera de ella. Se entiende que teletrabajan al menos dos días a la semana.
- **Vulnerabilidades:** Son las debilidades, hoyos de seguridad o falencias inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo.
- **Partes interesadas o grupos de interés:** Son personas naturales (estudiantes, profesores, administrativos, egresados, ciudadanos en general) o jurídicas (organizaciones públicas o privadas) que tienen un interés especial en la gestión, los resultados o son potenciales usuarios de los servicios y tramites ofertados.

5. Principios

El cumplimiento de los lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación; buscando sentar las bases para continuar protegiendo sus activos de información de todas las amenazas internas, externas bien sean deliberadas, accidentales o naturales y se regirá conforme a los siguientes principios:

- Confidencialidad de la información, de manera que únicamente usuarios autorizados tengan acceso.
- Integridad de la información, la cual será mantenida, evitando su alteración no autorizada.
- Disponibilidad de la información que es asegurada de acuerdo con los requerimientos de los procesos estratégicos, misionales, de apoyo y de evaluación.
- Autenticación segura para verificar la identidad de los usuarios de manera confiable y proteger el acceso a sistemas, aplicaciones y datos sensibles.

6. Monitoreo y revisión continua del SGSI

La ETITC, adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), bajo lineamientos en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (planeación, ejecución, evaluación y mejora continua), implementando la Política de Gobierno Digital al incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos; también se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas. El monitoreo y revisión se realiza mediante las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, el líder del Sistema de Gestión de Seguridad de la Información debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual. En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la Escuela Tecnológica Instituto Técnico Central. Así mismo, deberán tenerse en cuenta los incidentes de seguridad digital que hayan afectado a la institución y las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Gestión y Desempeño) y las partes interesadas.

7. Considerandos

7.1 Externos

- *Guía del DAFP – Resolución 1519 de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 20147 y se definen los requisitos materia de acceso de la información pública, accesibilidad web, seguridad digital y datos abiertos"*

- *Resolución 00500 de 2021"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*

- *Norma NTC ISO 27001:2022. Sistema de Seguridad de la Información. Esta Norma Internacional proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Seguridad de la Información.*

- *Directiva Presidencial No. 2 de 2022 "Reiteración de la Política Pública en Materia de Seguridad Digital".*

- *Decreto 767de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo del Título 9 de la parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*

- *Resolución 1951 de 2022: "Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital"*

- *Ley 2294 de 2023 "Por el cual se expide el plan nacional de desarrollo 2022- 2026 Colombia potencia mundial de la vida".*

- *Decreto 0529 de 2024: "Por el cual se modifica parcialmente el Capítulo 2 del Título 3 de la Parte 5 del Libro 2 del Decreto1075 de 2015 - Único Reglamentario del Sector Educación"*

7.2 Internos

- *Resolución 449 del 24 de octubre de 2017 "Por la cual se adopta Manual de Políticas de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central".*

- *Resolución 175 de 2018 "Por la cual se derogan las Resoluciones No. 581 del 28 de junio de 2011 y la 081 del 29 de febrero de 2017 y se crea el Comité Institucional de Gestión y Desempeño, en la Escuela Tecnológica Instituto Técnico Central".*

- *Resolución 169 del 29 de marzo de 2019 "Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión - MIPG en la Escuela Tecnológica Instituto Técnico Central y se definen otras políticas institucionales".*

- *Resolución 331 del 14 de octubre de 2020 "Por la cual se adoptan de los instrumentos de la gestión de la información pública de la Escuela Tecnológica Instituto Técnico Central".*

- *Acuerdo 014 del 20 de diciembre de 2020 del Consejo Directivo de la ETITC "Por el cual se aprueba y adopta el Plan de Desarrollo Institucional 2021-2024 Un nuevo acuerdo Institucional, Social y Ambiental por la consolidación de la Escuela".*

- *Acuerdo 018 del 17 de noviembre de 2021 del Consejo Directivo de la ETITC "Por el cual se actualiza la Política de Administración del Riesgo de la Escuela Tecnológica Instituto Técnico Central".*

8. Sanciones

Los lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad contenidas en esta política pretenden generar un compromiso, en todo el recurso humano de la Institución, que permita garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, logrando altos estándares de cultura, en temas de ciberseguridad.

Por tal motivo, las violaciones de las políticas de seguridad digital serán objeto de análisis y sanción, aplicando de esta manera, medidas correctivas, mediante la Secretaría General, la cual implementará el GCD-PC-01 Procedimiento Responsabilidad Disciplinaria, tomando como base el Código General Disciplinario (Ley 1952 de 2019, Artículo 55, Numeral 1), para de esta manera, impartir las respectivas correcciones, ante la violación presentada.

9. Objetivos del SGSI

Objetivo General
Mantener un ambiente razonablemente seguro, alineado a la misión, permitiendo proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la confidencialidad, integridad, disponibilidad y la autenticación segura como principios esenciales para garantizar la continuidad del servicio.

Objetivos Específicos
- Asegurar una transición exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con los requisitos establecidos en la norma NTC ISO/IEC 27001:2022, garantizando un ambiente seguro dentro de la institución.

- Implementar medidas específicas para fortalecer la protección de los activos de información de acuerdo con los nuevos requisitos y controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2022.

- Sensibilizar y capacitar a la comunidad educativa sobre los cambios y actualizaciones en el SGSI, con un enfoque en la prevención y la promoción de una cibercultura, alineada con mecanismos específicos de verificación de identidad.

- Dar continuidad con el proceso estructurado de inteligencia de amenazas para identificar, analizar y responder a potenciales ciberataques en toda la institución.

- Ejecutar acciones en base a los resultados de inspecciones técnicas y auditorías al SGSI, asegurando así la adaptación continua, requisitos cambiantes y la mejora continua de su desempeño.

10. POLITICAS DE CONTROLES ORGANIZACIONALES

9.1 Política organizacional de seguridad de la información

Planificar estrategias para dar cumplimiento a los requerimientos de grupos de valor Servidores Públicos, Proveedores, Contratistas y demás partes interesadas para trazar políticas y objetivos de seguridad de la información, ciberseguridad y protección de la privacidad con el fin de lograr un óptimo funcionamiento de la institución.

9.2 Política de roles y responsabilidades en la seguridad de la información

Generar lineamientos para los roles y responsabilidades con el fin evitar fallos en el sistema de gestión, riesgos y/o incidentes que pongan bajo amenaza la confidencialidad, integridad, disponibilidad y la autenticación de la información.

9.3 Política para segregación de deberes

Generar lineamientos para la segregación de deberes basada en dividir responsabilidades para evitar que una sola persona tenga control total sobre uno o varios procesos, previniendo así fraudes, errores y conflictos de interés.

9.4 Política de responsabilidad de la Dirección

La Alta Dirección fomentará de forma activa una cultura de seguridad de la información, ciberseguridad y protección de la privacidad en los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas.

9.5 Política de contacto con las autoridades y grupos de interés especial

Garantizar y brindar los lineamientos a las partes internas encargadas en la seguridad de la información en la interacción y comunicación con las autoridades y grupos de interés especial, estableciendo una guía en caso de presentarse algún incidente de seguridad que pueda poner en riesgo la seguridad de la información esto con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

9.6 Política para inteligencia de amenazas

Proporciona un marco para la identificación, evaluación y respuesta a las amenazas a la seguridad de la información de la organización. La inteligencia de amenazas permitirá a la organización tomar decisiones informadas sobre la gestión de riesgos y la implementación de medidas de seguridad.

9.7 Política de seguridad de la información en la gestión de proyectos

Se crea un modelo para la gestión y operación basado en Ciberseguridad para trazar los eventos relacionados con inteligencia de amenazas, respaldado por un SOC (Centro de Operaciones de Seguridad) el que tendrá los recursos de infraestructura y redes, físicos y responderá a los incidentes relacionados con Ciberseguridad asignando las tareas y responsabilidades pertinentes que deberán reportarse al Líder de Ciberseguridad.

9.8 Política de inventario de información, otros activos asociados y devolución de activos

Se cuenta con procedimientos para la identificación y registro actualizado de todos los activos de información y asociados con el fin de garantizar la seguridad y el uso adecuado de los activos. A su vez mantiene la recuperación completa para devolución de todos los activos al finalizar la relación con la institución como parte del proceso de salida de los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas

9.9 Política de clasificación y etiquetado de la información

Contar con procedimientos para asegurar que la información de la institución sea adecuadamente protegida según su nivel de sensibilidad, minimizando riesgos y cumpliendo con las normativas vigentes de acuerdo con los criterios de clasificación de la información como confidencialidad, integridad y disponibilidad, así como de etiquetado donde todos los propietarios de los documentos tienen el deber de controlar la distribución de dichos documentos.

9.10 Política de transferencia de la información

Asegurar el uso adecuado de los diferentes canales para realizar la transferencia de información entre la institución y Servidores Públicos, Proveedores, Contratistas y demás partes interesadas, antes de efectuarse la transferencia de dicha información se deberá firmar acuerdos de confidencialidad de las partes interesadas en los cuales se registren las

responsabilidades que garantice la reserva de la información y el alcance frente a su tratamiento y su uso.

9.11 Política de control de acceso

La institución se encarga de facilitar las condiciones y recursos para la implementación de controles de acceso lógico y físico de los activos de información con un enfoque de prevención buscando mitigar el impacto y la probabilidad de la materialización de un riesgo de la información.

9.12 Política de gestión de identidad y autenticación

Garantiza que se implementen medidas adecuadas para verificar la identidad de los usuarios y proteger los sistemas de accesos no autorizados, a través de los controles de autenticación técnica, como el uso de contraseñas fuertes, autenticación multifactorial, biometría, el cifrado de contraseñas se realizan con las técnicas cifradas aprobadas para contraseñas evitando que los usuarios reutilicen sus contraseñas entre otros. Todos los Servidores Públicos, Proveedores, Contratistas y demás partes interesadas deben seguir las reglas establecidas para el uso seguro de sus credenciales de acceso y colaborar con el equipo de seguridad en la detección y reporte de posibles vulnerabilidades o intentos de acceso no autorizados.

9.13 Política para abordar la seguridad de la información y acuerdos con los proveedores

Contar con procedimientos para identificar proveedores críticos como aquellos de servicios TIC, logística, servicios públicos, componentes de infraestructura TIC, seguridad física, etc. Evaluando cada uno de ellos con análisis de mercado, referencias de clientes, evaluaciones in situ, certificaciones y a su vez asignando supervisores que validen el cumplimiento de los requisitos a través de acuerdos de confidencialidad y no divulgación.

9.14 Política de gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)

Exigir a sus proveedores de servicios TIC, propagar las políticas de seguridad digital de la Escuela a lo largo de la cadena de suministro cada vez que los productos y servicios que incluyan componentes comprados o adquiridos como software o hardware se detallen las especificaciones técnicas para un funcionamiento seguro. Adicionalmente para el caso de análisis de vulnerabilidades la Escuela, prepara ambientes de pruebas, aislados, segmentados y seguros donde se apliquen pruebas o testing o ethical hacking que no comprometan los activos de la información, de esta manera aplica controles preventivos en la confidencialidad, integridad y disponibilidad de la información.

9.15 Política para la planificación y preparación de la gestión de incidentes de seguridad de la información

Establecer un marco para la planificación, preparación y respuesta efectiva a los incidentes de seguridad de la información dentro de la Escuela, con el fin de minimizar el impacto y restaurar las operaciones normales lo más rápido posible. Basado en los objetivos de detección y respuesta rápida: identificando y brindando respuesta inmediata a los incidentes de seguridad de manera oportuna, con la finalidad de minimizar el impacto y restaurando los servicios afectados lo más rápido posible. A su vez aprendiendo de los incidentes para mejorar las defensas y procedimientos.

9.16 Política de seguridad de la información durante una interrupción y preparación de las TIC para continuidad del servicio

Garantizar que la Escuela identifique los eventos, que constituyan una emergencia o desastre, elaborando con esto, planes de contingencia que permitirán mitigar los efectos adversos de la situación y le darán una continuidad al negocio exitosa, disminuyendo así, los riesgos de afectación de las operaciones institucionales, que afectan considerablemente el cumplimiento de la misión.

9.17 Política de cumplimiento de requisitos legales y contractuales

Garantizar que los requisitos legales, reglamentarios o contractuales, aplicables, se revisen periódicamente y se actualicen, respetándose con esto, el derecho de autor del software licenciados y en uso por parte de la Institucional, para el desarrollo de las funciones del colectivo laboral y el cumplimiento de la misión y objetivos institucionales realizando evaluaciones de riesgos de seguridad digital y se determinan las actividades de tratamiento a riesgos de acuerdo con la legislación y normativas gubernamentales.

9.18 Política de derechos de propiedad intelectual

Identificar y establecer las obras creadas por el personal administrativo, estudiantes, docentes, u otro tipo de personal vinculado a la misma, en desarrollo de sus actividades (Software, bases de datos, obras literarias y artísticas), definiendo de manera clara la titularidad de los derechos morales y patrimoniales que se generen de las mismas a través del manual de procedimientos y protocolos de propiedad intelectual.

9.19 Política de privacidad y protección de la información de identificación personal.

Garantizar que los datos personales almacenados, en los sistemas de información, repositorios y recursos informáticos reciban una protección óptima, para preservar la confidencialidad, integridad y disponibilidad de estos. Para el cumplimiento se identifica los sistemas de información, repositorios y recursos informáticos que almacenan, recolectan y procesan datos personales, para fines institucionales. Adicional se revisa la Ley 1581 de 2012 o Ley de Protección de Datos Personales.

10. POLÍTICAS DE CONTROLES DE PERSONAS

10.1 Política de selección, términos y condiciones de empleo, conciencia de seguridad de la información, educación y formación y responsabilidades después de la terminación o cambio de empleo

Garantizar que los Acuerdos y/o Cláusulas de Confidencialidad y Aceptación de Políticas de Seguridad de la Información, sean incluidos en los contratos o cualquier otra forma de vinculación laboral, de Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de información.

Durante el empleo los servidores públicos deberán asistir a charlas o capacitaciones en temas de seguridad digital. Si el servidor público, proveedor y demás partes interesadas generan incumplimiento, así como cualquier otro tipo de violación, que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información se verán inmersos en un proceso disciplinario.

Finalmente, todos los servidores públicos que se desvinculen tomen licencia o vacaciones, sea inhabilitado su acceso en el sistema de control de acceso, además, todo servidor público que cambie de posición laboral obtenga los privilegios adecuados de acceso a los sistemas de información.

10.2 Política de proceso disciplinario

Contar con procedimientos del proceso disciplinario, para el tratamiento de las violaciones a las políticas de seguridad digital, acuerdos o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información, o cualquier otro tipo de incidente de seguridad que ponga en riesgo la preservación de la confidencialidad, integridad, disponibilidad y autenticación segura de la información. Este proceso disciplinario quedará registrado en los expedientes académicos de los estudiantes, historial laboral del servidor público, así como expedición de certificado a proveedores.

10.3 Política de Teletrabajo

La ETITC, a través de la resolución 224 del 12 de mayo de 2023 “Por medio del cual se confiere la modalidad de teletrabajo suplementario a algunos servidores públicos de la ETITC”. Los servidores públicos se comprometen a respetar la legislación en materia de protección de datos y de la Política de Seguridad y Privacidad de la información, que la entidad ha implementado, como también a:

- Utilizar los datos de carácter personal a los que tenga acceso única y exclusivamente para cumplir con sus obligaciones para con la entidad.
- Cumplir con las medidas de seguridad que la entidad haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso.
- No ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.

10.4 Política de Consentimiento Informado

Antes de iniciar a grabar la sesión virtual en el aplicativo Teams, enuncia a sus asistentes bajo la ley 1581 de 2012 y al decreto 1377 de 2013 de políticas de privacidad, protección de datos y habeas data la autorización de grabación, solicitando la apertura de cámara web y encendido de audio así mismo a que cada asistente se presente y mencione su nombre, apellido, cargo y aceptando la grabación o no de esta sesión.

11. POLITICAS DE CONTROLES FISICOS

11.1 Política de perímetros de seguridad física

La ETITC, como responsable del tratamiento de datos, informa a sus Servidores Públicos, Proveedores, Contratistas y demás partes interesadas que contamos con cámaras de videovigilancia y que, al ingresar a nuestras instalaciones físicas, usted autoriza a ser grabado y monitoreado por nuestro Sistema de Circuito Cerrado de Televisión. Su información será conservada en nuestras bases de datos por un término máximo de noventa (90) días y será destinada para fines de control y seguridad, así como para realizar investigaciones administrativas, disciplinarias y penales, solo será compartida con las autoridades competentes que la soliciten en ejercicio de sus funciones.

11.2 Política de entrada física

Contar con procedimientos para garantizar el control de ingreso de servidores públicos, proveedores, visitantes y demás partes interesadas: en la recepción se cuenta con controles de ingreso con registro de ingreso y salida. El personal de seguridad física entrega un stiker al personal que nos visita y este debe regresarlo a la salida. En el ingreso vehicular también se tiene incorporado sistema llamado TOIOTEM para el registro del personal haciendo uso del escaneo de código de barras de la cédula de ciudadanía.

Adicionalmente se ha adaptado para el ingreso de Equipos Externos, es necesario registrar una única vez el activo tipo hardware (Laptop, Tablets) a través del siguiente link: https://forms.office.com/r/Birqgy3jfZ luego dirigirse al Salón E102 (Laboratorio Festo), para la adición del stiker QR único para (Laptop, Tablets). Adicional, debe figurar el propietario de cada activo con sus datos de identificación en este caso cédula de ciudadanía, serial del equipo, color y marca. En caso contrario se debe diligenciar bitácora de seguridad física.

11.3 Política de escritorio y pantalla limpia

Garantizar 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 deben ingerir alimentos o bebidas cerca de equipos de cómputo, documentación física y medios magnéticos, así como, evitar manipular líquidos en su cercanía.
- Guardar toda la documentación física y/o medio magnético en cajones, archivadores o sitios seguros, durante su ausencia del puesto de trabajo, manteniendo el mismo, libre de documentación física y medios magnéticos.

- Evitar colocar documentos sensibles o accesos directos a los mismos, en el escritorio del equipo de cómputo, manteniendo el mismo, limpio y seguro.
- Retirar de las impresoras, escáner y fax, toda documentación física, evitando de esta manera la exposición de la información a personal no autorizado.

12. POLITICAS DE CONTROLES TECNOLOGICOS

12.1 Política de dispositivos de punto final de usuario.

Garantizar que los servidores públicos, proveedores y partes interesadas, que tengan acceso a los sistemas de información y equipos de cómputo permanezcan bloqueadas la sesión de usuario, cuando se ausente del puesto de trabajo y/o deje los equipos desatendidos, para proteger el acceso a la documentación digital, aplicaciones y servicios, haciendo uso de las teclas Windows + L o Ctrl+Alt+Supr.

- Cerrar correctamente la sesión de usuario y apagar el equipo de cómputo y periféricos, cuando finalice la jornada laboral, garantizando con esto, una desconexión satisfactoria de la red institucional.
- No se deben alojar o almacenar contraseñas en los navegadores de búsqueda del equipo de cómputo y mantener la papelera de reciclaje vacía.
- Hacer uso de Gestor de Contraseñas para recordación de usuario y contraseñas diferentes a los servicios de Google.
- Debe validar que la sincronización de One Drive esté funcionando correctamente.

12.2 Política de derechos de acceso privilegiado y de restricción de acceso a la información

Todos los equipos de usuario final, que se conecten o deseen conectarse, a las redes de datos, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados limitando su acceso según el perfil y los permisos asignados.

A su vez se garantiza la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información, contemplando la creación, modificación, bloqueo o eliminación de las cuentas de usuarios en general y de las de acceso privilegiado.

12.3 Política de restricción de acceso a la información

Todos los equipos de usuario final, que se conecten o deseen conectarse, a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados limitando su acceso según el perfil y los permisos asignados.

A su vez se garantiza la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información, contemplando la creación, modificación, bloqueo o eliminación de las cuentas de usuarios.

12.4 Política de autenticación segura

Contar con una política de autenticación segura donde se establece una serie de pasos y controles que aseguran que solo usuarios y dispositivos autorizados puedan acceder a la red y recursos.

Aplicable a todos los usuarios como Servidores Públicos, Proveedores, Contratistas y demás partes interesadas y dispositivos que accedan a la red de la ETITC. A través de contraseñas seguras y complejas como (mínimo de 12 caracteres, que incluyan letras mayúsculas, minúsculas, números, símbolos y barra espaciadora).

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 habilitar el control MFA para todos los accesos, utilizando (token, SMS, app de autenticación) para su correo institucional y demás sistemas de información.

12.5 Política para la Gestión de Capacidad

Monitorear constantemente de conformidad con las necesidades actuales y previstas en los servicios de procesamiento de información, recursos humanos, oficinas, para mejorar la disponibilidad y eficiencia de los sistemas realizando pruebas para satisfacer los requisitos de rendimiento máximo y realizando proyecciones de los futuros requisitos de capacidad que se debe tener en cuenta con base las tendencias actuales y proyectadas de las capacidades de procesamiento de la información de la Escuela.

12.6 Política de protección contra malware

Implementar reglas y controles que impiden y detectan el uso de software no autorizado y se tiene lista de aplicaciones permitidas, se realiza creación de lista negra de sitios web sospechosos, de igual manera se configura de manera correcta las herramientas de detección contra malware constantemente de acuerdo con los procedimientos establecidos por la Escuela.

12.7 Política de gestión de vulnerabilidades técnicas.

Establecer funciones y responsabilidades asociadas a la gestión técnica de vulnerabilidad, donde incluye la supervisión de la vulnerabilidad, la evaluación de riesgo de la vulnerabilidad, la actualización, seguimiento de los activos con el fin de mantener la conciencia sobre ellas. Adicionalmente se realiza análisis de vulnerabilidades con el fin de comprobar si la aplicación de parches de vulnerabilidades se ha realizado correctamente; en caso de contar con soporte técnico con proveedores se recomiendan las acciones que ellos deben aplicar al interior de sus aplicativos para que cumpla con los requisitos de codificación segura.

12.8 Política de gestión de configuración

Implementar procedimientos y herramientas de configuración para hardware, software y servicios a través de configuraciones de seguridad para sistemas recién instalados y para sistemas operativos a lo largo de su vida útil, asegurando el control de satisfactorio de todos los cambios de configuración, dentro de los cuales se cuenta con configuración segura de hardware, software, servicios y redes minimizando el número de identidades con derechos de acceso a nivel de administrador, deshabilitando identidades innecesarias, restringiendo el acceso a potentes programas de utilidad y de parámetros de host, etc.

12.9 Política de eliminación, enmascaramiento de datos y prevención de fuga de datos

La Escuela evita la exposición innecesaria de información confidencial cumpliendo con los requisitos legales, reglamentarios y contractuales para la eliminación de información. El enmascaramiento debe limitar la exposición de datos sensibles donde se incluyen cifrado, anulación y eliminación de caracteres, sustitución de datos confidenciales y anonimización de datos en control de acceso, acuerdos o restricciones sobre el uso de los datos procesados a la vez se mantienen medidas de prevención de fugas de datos a los sistemas de información, redes y cualquier dispositivo que procese, almacene o transmita información confidencial.

12.10 Política de copia de seguridad de la información

Para el cumplimiento de la Política de Copias de Respaldo de la Información es necesario la elaboración y aprobación del procedimiento de Copia de Respaldo a través de GIC-PC-05 Procedimiento de Copia de Respaldo de la Información, así mismo el procedimiento de Restauración GIC-PC-17 Restauración de la Información.

Adicional la escuela debe contar con suficiente tecnología de almacenamiento, para soportar por periodos prolongados, las copias de seguridad de la información generadas donde se define en el formato GSI-FO-03 Matriz de inventario general de activos de la ETITC los criterios de este:

Periocidad del backup: Mensual – Diario – Trimestral – Semestral y/o Anual
Tipo de backup: Completo y/o Incremental
Lugar de almacenamiento: Virtual – Físico o en los dos casos Virtual/Físico

12.11 Política de redundancia de las instalaciones de procesamiento de la información

Garantizar que todos los sistemas de información, servicios y recursos tecnológicos sean clasificados como críticos, cuenten con una solución redundante en su operación, para favorecer la preservación de la disponibilidad en su funcionamiento. Para el cumplimiento de la Política de Redundancias, la Escuela debe identificar los sistemas de información, servicios y recursos tecnológicos que contribuyen, en gran medida, al cumplimiento de los objetivos y misión institucional.

12.12 Política de registro

Proteger los registros contra cambios no autorizados de registro y problemas operativos con la instalación de registro, modificaciones de los tipos de mensajes que se graban, archivos de registro que se están editan o eliminan de acuerdo al seguimiento mediante la gestión de eventos, reglas de firewall y sistemas de detección de intrusiones o firmas de malware.

12.13 Política de seguridad de redes

Garantizar que los accesos a las redes de datos institucionales cuenten con lineamientos y controles de seguridad, que impidan que personal, no autorizado, conecten equipos en la LAN de la ETITC para fines no esclarecidos, manteniendo la documentación actualizada, incluidos diagramas de red, como router, switches, autenticación de sistemas de red, restringiendo y filtrando la conexión de los sistemas a la red mediante firewall.

12.14 Política de uso de la criptografía

Garantizar que todos los sistemas de información posean un certificado digital, permitiendo, de esta manera, que toda la información que viaja de origen a destino, lo haga de manera cifrada, preservando, a su vez, la confidencialidad e integridad de la información y se cuenta con métodos para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves cifrados y registro de auditorías con actividades relacionadas en el uso de la criptografía.

12.15 Política de requisitos de seguridad de las aplicaciones

Contar con la gestión de proyectos para fortalecer la seguridad de la información, ciberseguridad y protección de la privacidad para recomendar y adquisición de aplicaciones seguras que permitan el cumplimiento de requisitos de seguridad que no pongan en riesgo nuestra infraestructura tecnológica ante ataques malintencionados o interrupciones no intencionadas como desbordamiento de búfer o inyecciones de lenguaje de consulta estructurados (SQL), etc.

12.16 Política de arquitectura de sistemas seguros y principios de ingeniería

Contar con procedimientos para el cumplimiento de principios de ingeniería donde incluyen controles de seguridad para prevenir, detectar o responder a eventos de seguridad, a su vez permite cifrar información sensible y tiene procedimiento para criterios de aceptación de software nuevo con requerimientos técnicos no funcionales para la operación del sistema, autenticación y creación de usuarios, Implementación de RBAC (Rol Based Access Control), es decir, que el desarrollo permita la creación de roles con permisos, para controlar los privilegios que cada usuario puede tener dentro del servicio de reporte, los roles se definirán durante el desarrollo del proyecto, teniendo en cuenta la arquitectura de seguridad AAA (Autorización, Autenticación & Accounting).

12.17 Política de desarrollo externalizado

Revisar las actividades relacionadas con el desarrollo de sistemas tercerizados y acuerdan si la entrega del trabajo subcontratado cumple con las expectativas de licencia, propiedad del código y derechos de propiedad intelectual, adicionalmente se aplica testing para evitar la presencia de contenido malicioso o código malintencionado antes de la entrega del desarrollo.

12.18 Política de gestión de cambio

Implementar procedimientos de control de cambios para asegurar el ciclo de vida del desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento para la infraestructura y software de TI. Planificando los cambios y evaluando el impacto potencial, pruebas de aceptación, planes de despliegue, consideraciones de emergencia y contingencia ambientales.

13. DISPOSICIONES FINALES

13.1 Comunidad educativa del Instituto de Bachillerato Técnico Industrial (IBTI), Programas de Educación Superior (PES), administrativos, servidores públicos, proveedores y demás partes interesadas

Todos los Servidores Públicos, Proveedores, Contratistas, Padres de Familia, Acudientes, Estudiantes, Docentes y demás partes interesadas, deberán cumplir los lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad, apoyarán reportando a la mesa de servicios (mesadeayuda@itc.edu.co), correos sospechosos y evitarán reenviar cadenas malintencionadas de spam, phishing, suplantación de identidad, fraudes, estafas y malware, etc. a través de los sistemas de información o correo institucional. Cabe resaltar que se encuentra prohibido aplicar técnicas de ingeniería social, pruebas de pentesting y simulaciones de ciberseguridad, el incumplimiento de la política acareará sanciones de acuerdo con la normatividad vigente colombiana.

13.2 Violaciones a las políticas de seguridad de la información, ciberseguridad y protección de la privacidad

Cualquier situación que evidencie la violación a las políticas de seguridad de la información por parte de los estudiantes, graduados, docentes, padres de familia, acudientes, servidores públicos, proveedores y demás partes interesadas que tengan relación directa e indirecta en el manejo de la infraestructura tecnológica y sistemas de información, podrá resultar en un proceso que deberá ser iniciado por parte del líder del proceso, jefe inmediato o responsable del tercero, con base a las evidencias recopiladas las cuales pueden incluir, más no estar limitadas a:

- Acción de tipo disciplinario por parte del Control Interno Disciplinario según los lineamentos establecidos por el código sustantivo del trabajo, reglamento estudiantil, reglamento docente o reglamento interno del trabajo según el rol del implicado, las cláusulas especiales que se establezcan con los colaboradores en sus contratos laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.
- Suspensión o acceso restringido a las áreas de procesamiento de la información.
- Terminación del contrato de trabajo o relación comercial basados en las disposiciones emitidas por las leyes colombianas en materia laboral y el reglamento interno de trabajo.
- Demanda de tipo civil o penal como resultado de las acciones de tipo disciplinario
- Asunción de consecuencias legales derivadas de la investigación que adelante la Autoridad.

13.3 Difusión y divulgación políticas de seguridad de la información, ciberseguridad y protección de la privacidad

La presente política y su anexo técnico estará disponible para su consulta en la página web y rige a partir de la fecha de expedición.

14. Control de cambios

Fecha	Versión	Cambios
8/07/2016	1	Adopción de la política.
14/09/2017	2	Se añade la fila Etiqueta en la página principal del documento
19/04/2017	3	La Política General de Seguridad de la Información se alinea con los requisitos contenidos en las cláusulas de la 4 a la 10, de la norma ISO 27001:2013
01/04/2019	4	Ingreso al Sistema de Gestión de Calidad Modificaciones en el contenido de la Política General de Seguridad de la Información, acorde al habilitador transversal de Seguridad de la Información de Gobierno Digita.
26/07/2024	5	Actualización de toda la política con base en la estructura y los criterios de la norma NTC ISO 27001:2022.

Elaboró: Sandra J. Guerrero G. -, Profesional de Seguridad de la Información
Revisó: Jorge Herrera Ortiz – Jefe Oficina Asesora de Planeación
Validó: Comité Institucional de Gestión y Desempeño.
Aprobó: Consejo Directivo.