PLAN OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CLASIF. DE CONFIDENCIALIDAD	IPB	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1

Plan aprobado en Comité Institucional de Gestión y Desempeño bajo acta No. 001 del día 31 de enero del 2024.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Escuela Tecnológica Instituto Técnico Central (ETITC) considera la información que gestiona, recolecta y custodia, como un elemento indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Institución, razón por la cual es necesario que la misma, establezca un marco, en el cual, se asegure que la información es protegida de manera adecuada, independientemente, de la forma en la que ésta sea manipulada, procesada, transportada o almacenada.

Por lo anterior, el presente plan describe las actividades a desarrollar durante la vigencia 2024 definidas por la ETITC. Para la elaboración de este, se toma como referencia la norma ISO/IEC 27001:2013 y transición hacia la ISO/IEC 27001:2022 y los lineamientos de la estrategia Gobierno Digital, en especial las guías suministradas para el Modelo de Seguridad y Privacidad de la Información que tienen como objetivo: gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos. Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ETITC.

2. OBJETIVO DEL PLAN OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecer los lineamientos del SGSI con la NTC/IEC ISO 27001:2013 y transición a la nueva versión NTC/IEC ISO 27001:2022 con énfasis al Modelo de Seguridad y Privacidad de la Información y con las Políticas de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central.

3. ALCANCE

El plan operativo del Sistema de Gestión de Seguridad de la Información, aplica a los procesos de la Escuela Tecnológica Instituto Técnico Central,

donde se da cumplimiento de los requisitos y lineamientos, que tienen el alcance gestionar adecuadamente la seguridad de la información, gestión de activos, gestión de riesgos y la continuidad de los servicios ofrecidos y que respaldan el GSI-MA-03 Manual Operativo del SGSI (documento interno privado).

4. TERMINOS Y DEFINICIONES

DELITO INFORMÁTICO: Se conoce como delito informático cualquier acción ilícita o criminal que atente a aun sistema informática con el fin de causar un daño que atente a aun programa, sistema de procesamiento de información etc.

CIBERSEGURIDAD: La ciberseguridad se refiere a un conjunto de técnicas utilizadas para proteger la integridad de la arquitectura de seguridad de una organización y proteger sus datos contra ataques, daños o acceso no autorizado

INTEGRIDAD: La integridad se refiere a la cualidad de la información en la cual se debe ser legitima, sin modificación y correcta, esto quiere decir que debe encontrarse en un estado original manteniendo su estructura tal cual como fue generada sin ningún tipo de alteración por parte de terceros.

DISPONIBILIDAD: La disponibilidad se refiere a aquella información que se encuentra disponible y que se puede acceder a través de los medios y los canales adecuados en cualquier momento.

CONFIDENCIALIDAD: La confidencialidad se refiere a la propiedad de la información para ser suministrada únicamente usuarios autorizados a dicha información, por consiguiente, solo resultada accesible con una debida comprobación de los usuarios para ser accedida.

AUTENTICIDAD: La autenticidad se refiere a dicha situación en la cual se hace la verificación de que un documento pertenece o ha sido elaborado por quien dice ser el autor o dueño de un documento. En dicha situación se

hace la verificación de la identidad del usuario en la cual se confirma que dicha persona es quien dice ser, por consiguiente, si su identidad es auténtica será esta persona será autorizada.

NO REPUDIO: Es el servicio en el cual se relaciona con la autenticación y la aprobación de la participación de dos o más partes (emisor y receptor) en la comunicación y transmisión de la información. De la anterior, el no repudio puede ser tanto "No Repudio en Origen" y "No repudio en Destino". Por consiguiente, el no repudio se refiere a que si en un caso el emisor y el recetor niegan haber recibido y enviado información cualesquiera de los dos pueden probar que si se ha efectuado.

5. NORMATIVIDAD

NORMA	DESCRIPCIÓN
Constitución Política de Colombia	Artículo 15.
Ley 527 de 1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000	Por medio de la cual se expide la Ley General de Archivos.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1221 del 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Resolución 2999 del 2008	Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TICS se crea la agencia Nacional de espectro y se dictan otras disposiciones.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
Ley 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Ley 1978 de 2019	Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
Resolución 2034 de 2016	Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Resolución 1151 de 2019	Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018.
Decreto 620 de 2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 2306 de 2020	Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018
Resolución 924 de 2020	Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
Resolución 2256 de 2020	Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 331 de 2020	Por la cual se adoptan de los instrumentos de la gestión de la información pública de la ETITC.
Resolución 2256 de 2020	Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Directiva presidencial 03 de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Directiva presidencial 02 de 2022	Reiteración de la Política Pública en materia de Seguridad Digital
Decreto 338 de 2022	Por la cual se adiciona el título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
Resolución 448 de 2022	Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución 2256 de 2020
Decreto 1263 de 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
NTC-ISO/IEC 27001:2022	Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información.

6. PLAN OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se determinan las actividades del plan operativo del Sistema de Gestión de Seguridad de la Información para el periodo comprendido entre el 13 de enero hasta el 31 de diciembre de 2025.

Estrategia	Actividades	Evidencia	Fecha de Programación de Tareas		SEGUIMIENTO
			Fecha Inicial	Fecha Final	
Planificación de Seguridad y Privacidad de la Información	Plan Operativo de Seguridad y Privacidad de la Información	Programación operativa	13-Ene-2025	31-Ene-2025	Se realizo y se publicó en la web 1 trimestre
	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Matriz GDC-FO-09 Mapa y Plan de Tratamiento de Riesgos publicada en el sitio web	13-Ene-2025	31-Ene-2025	Esta en articulación de todos los sistemas 1 trimestre
Actualización de Activos de la Información	Levantamiento de Activos de Información	Identificar y/o actualizar activos de información en cada dependencia y establecer su criticidad	03-Feb-2025	31-Mar-2025	1 trimestre 0% 2 trimestre 40%
	Socialización nuevo formato de	Identificar activos de información en cada dependencia en	03-Feb-2025		Actividad planeada Tercer trimestre

	Activos de Información	especial con el tipo Recurso Humano y establecer prioridad del servicio		31-Mar-2025	
	Publicación de Activos de Información	Actualizar el Inventario de Activos de registro de activos de información, índice de información clasificada y reservada	01-Sep-2025	30-Sep-2025	1 trimestre 0% 2 trimestre 0% Tercer trimestre planeado
		Publicar los activos de información	01-Oct-2025	04- Oct -2025	Planeado 4 trimestre
Gestión de Riesgos	Identificación de Riesgos de Seguridad de la Información	Identificar, analizar y evaluar los riesgos relacionados con la Seguridad de la Información, Seguridad Digital, Ciberseguridad alineado con la Continuidad del Servicio	03-Feb-2025	31-May-2025	1 Primer 2 trimestre Actualización matriz de riesgos Eliminación riesgo transición
	Administrar los Riesgos de Seguridad de la Información	Verificar y administrar el cumplimiento de los riesgos de seguridad de la información y mantenerlos en niveles aceptables de acuerdo con la guía para la administración del riesgo y el diseño de controles en entidades públicas en su versión No. 5	03-Feb-2025	16-Dic-2025	Identificaron riesgos Pendiente publicación
	Implementar riesgos de acuerdo con la transición e implementación de nuevos controles de la norma NTC ISO/IEC 27001:2022	Revisión de cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y de auditorías internas planificadas a intervalos regulares	03-Feb-2025	16-Dic-2025	100 se realiza la implementación de la norma Documento revisión por la dirección
	Monitoreo de Riesgos de	Generación, presentación y reporte de monitoreo			Presentación al directorio activo

	Seguridad de la Información con herramientas especializadas del SGSI	al directorio activo y servidor de archivos para evidenciar los riesgos de Seguridad y que brindan cumplimiento a la NTC ISO/IEC 27001, a través de la herramienta SEM	03-Feb-2025	16-Dic-2025	Y al servidor de archivos Planear auditoria tercer trimestre Informe final
Gestión de Incidentes de Seguridad de la Información	Eventos e Incidentes	Tratamiento y seguimiento a eventos e incidentes asociados al Sistema de Gestión de Seguridad de la Información	03-Feb-2025	16-Dic-2025	Materialización de riesgo 100% 1 y segundo trimestre
	Realizar actividades de Seguridad Técnica en: Análisis de Vulnerabilidades, Hacking Ético y Pentesting	Realizar escaneo para encontrar vulnerabilidades, fallos de seguridad con la finalidad de retener, mitigar y evitar fugas de información hacia la posibilidad de un ataque informático	03-Feb-2025	16-Dic-2025	1 trimestre 0% 2 trimestre EP 40% 3 trimestre 30% 4 trimestre 30%
	Participar en los grupos de respuesta a incidentes (CSIRT)	Socializar boletines informativos de Ciberseguridad a través de correo institucional o medios de comunicación	03-Feb-2025	16-Dic-2025	1 trimestre 100% 2 trimestre 100% comunicados 3 trimestre 50%
	Reportes periódicos del uso de software especializado en Ciberseguridad	Monitoreo constante de logs de eventos de seguridad a nuestra infraestructura tecnológica clasificando su severidad y reportar a Gestión de Informática y Telecomunicaciones sus acciones preventivas	03-Feb-2025	16-Dic-2025	1 trimestre informe trimestral de revisión de logs 2 trimestre monitoreo de logs durante proceso electoral 3 trimestre programar informe para presentar en el comité
	Gestionar los incidentes de Seguridad de la Información identificados	Mantener en condiciones estables los incidentes y riesgos de seguridad de la información de acuerdo con	03-Feb-2025	16-Dic-2025	Gestion de incidentes 100% 2 trimestre no se han presentado incidentes

		procedimiento definido			
Gestión de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.	Toma de conciencia y comunicación a los servidores públicos, proveedores y partes interesadas en temas relacionados al SGSI	Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad	03-Feb-2025	16-Dic-2025	3 trimestre se realiza la socialización
		Activos de información			3 trimestre se realiza la socialización
		Inducción IBTI, PES, Docentes, Servidores Públicos y partes interesadas			2 trimestre se realiza socialización
		Inducción y Reinducción a Servidores Públicos			2 trimestre
		Phishing e Ingeniería Social			2 trimestre capacitación
		Protección de Datos durante el Trabajo en Casa			3 trimestre se realiza la socialización
		El Bullying y Ciberacoso			3 trimestre se realiza la socialización
		Cibercultura para padres de familia			3 trimestre se realiza la socialización
		Gestión de contraseñas			2 trimestre
		Desintoxicación digital			3 trimestre se realiza la socialización
		Ciberhigiene y Tips de Seguridad Digital			3 trimestre
	Participar en entrenamiento especializado en Ciberseguridad que invite Gobierno	Recibir capacitaciones en temas identificados como: Hardening y Ethical Hacking Mitigación de Riesgo IOT e Inteligencia de Artificial Simulaciones y Ejercicios Técnicos de Ciberseguridad	01-Mar-2025	16-Dic-2025	2 trimestre actualización nuevos lineamientos del MSPI 2 trimestre horizonte digital seguro

		Aseguramiento de evidencias digitales, Análisis Forense Digital e Inteligencia de Amenazas			
	Realizar actividades para mantener la certificación del Sistema de Gestión de Seguridad de la Información NTC ISO/IEC 27001	Mantenimiento del Sistema de Gestión de Seguridad de la Información NTC ISO 27001	13-Ene-2025	16-Dic-2025	Tercer trimestre auditoría externa de seguimiento
	Modelo de Seguridad y Privacidad de la Información	Realizar actualización a la herramienta de autodiagnóstico anual, con el fin de identificar brechas y las acciones para su mitigación.	03-Feb-2025	16-Dic-2025	3 trimestre Agosto
	Actualización de SOA con la aplicabilidad de nuevos controles y reglas generadas en el manejo de puertos USB.	Aplicar estrategias para validar el cumplimiento de las políticas de Seguridad y Privacidad de la información	03-Feb-2025	16-Dic-2025	3 trimestre Agosto
	Verificar módulo de contraseñas de los aplicativos del Sistema de Información Académica Gnosoft	Realizar informe de cumplimiento, incluyendo sensibilización a los estudiantes del Instituto de Bachillerato Técnico Industrial	13-Ene-2025	31-Mar-2025	Auditoria 29 de julio
Acciones correctivas y de mejora al Sistema de Gestión de Seguridad de la Información	Acompañamiento a Entidades del sector Educación y de Gobierno en materia de Seguridad Digital	Participar en los talleres de acompañamiento a las entidades adscritas y vinculadas al sector educación en la implementación de políticas de Gobierno y Seguridad Digital	03-Feb-2025	16-Dic-2025	quitarlo
Planeación anual SGSI.	Revisión Manual Políticas de Seguridad de la Información.	Actualizar el Manual Políticas de Seguridad de la Información.	13-Ene-2025	16-Dic-2025	Averiguar con anay cada cuanto se deben actualizar la politica

Gobierno Digital	Modelo de Seguridad y Privacidad de la Información y Seguridad Digital.	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	03-Feb-2025	16-Dic-2025	3 trimestre
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la normatividad vigente.			2 trimestre documentos electrónicos Matriz de riesgo,
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2022	Participar en las auditorías internas programadas en el Plan Anual de Auditorías	03-Feb-2025	16-Dic-2025	3 trimestre Ajustar cronograma para auditoria interna 2 trimestre auditoria aires acondicionados UPS 100%
		Realizar seguimiento al plan de mejoramiento	Trimestralmente	16-Dic-2025	Después de la auditoria
		Participar en auditorías externas de la norma ISO 27001:2022	03-Feb-2025	16-Dic-2025	4 trimestre
		Realizar inspecciones a diferentes procesos (Auditorías Internas)	Trimestralmente	16-Dic-2025	Establecer plan de auditorías 1 inspección segundo semestre
		Recopilar y Analizar amenazas de Seguridad de la Información acerca de Inteligencia de Amenazas	03-Feb-2025	16-Dic-2025	Establecer cual es el top 10 de la escuela hablar con Angelica para generar el informe
Protección de datos personales	Revisión de bases de datos	Socializar y revisar la información recolectada por las diferentes áreas de la ETITC mediante el manual de anonimización.	01-May-2025	16-Dic-2025	2 Trimestre recolección de datos personales,

		Reportar de manera adecuada las Bases de Datos ante la Superintendencia de Industria y Comercio			
Gestión de Continuidad del Servicio	Diseño del Plan de Continuidad del Servicio para el SGSI	Documentar Análisis de Impacto del Negocio – BIA	01-May-2025	16-Dic-2025	
		Actualizar documentación y política Continuidad del Servicio	01-May-2025	16-Dic-2025	
		Implementar el plan de continuidad de acuerdo con los resultados de la evaluación de riesgos y eventos identificados	01-May-2025	16-Dic-2025	
		Realizar simulacros, pruebas, mantenimiento y reevaluación al plan de Continuidad del Servicio			

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
26/01/2024	1	Adopción del Documento
27/01/2025	2	Actualización del Plan Operativo Anual de acuerdo con los nuevos lineamientos del Plan de Desarrollo Institucional 2025-2032 en su Meta Estratégica "Alcanzar el 92% en el Índice de Desempeño Institucional del FURAG." – Inclusión de actividades de Recopilación y análisis de Seguridad de la Información acerca de Inteligencia de Amenazas.
14/08/2025	3	Actualización de codificación del Documento

ELABORÓ	REVISÓ	APROBÓ
Ing. SANDRA J. GUERRERO G. Líder de Gestión de Seguridad de la Información	**ANAY PINTO** Administrador de la Documentación	**COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**

CLASIF. DE CONFIDENCIALIDAD	IPB	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1