PLAN 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), como institución de educación superior de carácter público, está obligada a adoptar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano, en cumplimiento de la Política de Gobierno Digital y en articulación con el Modelo Integrado de Planeación y Gestión (MIPG). Este Plan de Seguridad y Privacidad de la Información – vigencia 2026 se formula en armonía con la actualización del MSPI expedida por el Ministerio TIC mediante la Resolución 02277 de 2025, que fortalece la seguridad digital en las entidades públicas y la alinea con la norma técnica colombiana NTC ISO/IEC 27001:2022 y sus controles del Anexo A.

El Plan se integra con el Plan de Desarrollo Institucional (PDI) 2025–2032 y con la misión, visión y apuestas estratégicas de la ETITC, asegurando que las acciones de seguridad y privacidad habiliten y protejan los procesos misionales y de apoyo en todas las sedes. Asimismo, se articula con la Política de Seguridad y privacidad de la Información institucional (acuerdo 012 de julio del 2024), que será objeto de revisión durante la vigencia del presente plan.

Este documento adopta el enfoque de ciclo de vida del MSPI (diagnóstico, planificación, operación y evaluación), integrando la gestión de riesgos conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP), complementada la última con el detalle y profundidad que aporta y exige los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, integrados con los 93 controles del Anexo A de la norma NTC ISO/IEC 27001:2022, incluyendo los 11 controles nuevos sobre nube, inteligencia de amenazas, continuidad TIC, DLP, monitoreo, gestión de configuración y desarrollo seguro.

En coherencia con los 6 ejes estratégicos institucionales —(1) Formación y pedagogía de calidad; (2) Investigación y producción técnico-científica; (3) Extensión y proyección institucional; (4) Transformación institucional; (5) Ampliación y modernización de la infraestructura; (6) Cuidado por el bienestar y la vida— el Plan prioriza acciones que reduzcan la exposición a amenazas, fortalezcan la continuidad de los servicios académicos y administrativos, eleven la cultura de seguridad digital y aseguren el cumplimiento normativo.

2. OBJETIVO

Establecer y ejecutar el Plan de Seguridad y Privacidad de la Información de la ETITC para la vigencia 2026, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) actualizado, la NTC ISO/IEC 27001:2022, la Política de Seguridad de la Información institucional y articulado con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el propósito de proteger los activos de información institucionales, garantizar una adecuada gestión de la confidencialidad, integridad, disponibilidad y privacidad de la información, mitigar los riesgos asociados, y servir como habilitador para la continuidad de los servicios académicos, investigativos y administrativos, en coherencia con el Plan de Desarrollo Institucional 2025–2032 y los seis ejes estratégicos de la institución.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información – vigencia 2026 de la ETITC tiene un alcance institucional integral, que comprende:

Cobertura organizacional: Aplica a todas las dependencias, procesos misionales, estratégicos y de apoyo, así como a las sedes físicas y entornos virtuales de la institución.

Activos de información: Incluye datos, archivos físicos, información, sistemas, aplicaciones, infraestructura tecnológica, redes, servicios digitales y

cualquier recurso que soporte la operación académica, investigativa, administrativa y de extensión.
Sujetos obligados: Todo los funcionarios directivos, docentes, administrativos, contratistas y terceros que accedan, procesen o gestionen información institucional.

Ámbito normativo y técnico: Se fundamenta en el Modelo de Seguridad y Privacidad de la Información (MSPI), la NTC ISO/IEC 27001:2022, la Política de Seguridad y Privacidad de la Información institucional, la Guía DAFP y los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, asegurando la integración con el Plan de Desarrollo Institucional 2025–2032 y los 6 ejes estratégicos.

Temporalidad: Vigencia de un año (2026), con actividades planificadas para diagnóstico, implementación, seguimiento y mejora continua, enmarcadas en el ciclo de vida del MSPI.

4. MARCO NORMATIVO Y REFERENCIAL

El Plan se sustenta en el siguiente marco normativo, regulatorio y técnico:

Normativa nacional y sectorial:

- Ley 1581 de 2012 y normas complementarias sobre protección de datos personales.
- Ley 1712 de 2014 sobre transparencia y acceso a la información pública.
- Decreto 620 de 2020 y lineamientos de la Política de Gobierno Digital.
- Resolución 500 de 2021 del 2021, que establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad (MSPI) como habilitador de la política de Gobierno Digital.
- Resolución 02277 de 2025 del MinTIC, que actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP).

- Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MinTIC).

Normas técnicas y estándares internacionales:

- NTC ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- GTC ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- NTC ISO/IEC 27701:2020 – Técnicas de seguridad. Ampliación de las NTC ISO/IEC 27001 y GTC ISO/IEC 27002 para la gestión de la privacidad de la información (referencial).

Referentes institucionales:

- Política de Seguridad de la Información institucional (Acuerdo 012 de julio del 2024).
- Plan de Desarrollo Institucional (PDI) 2025–2032.
- Política de Gobierno Digital y lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

5. PRINCIPIOS Y POLÍTICA INSTITUCIONAL

5.1 Principios Rectores del Modelo de Seguridad y Privacidad de la Información

El presente Plan adopta los principios establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano y los articula con los lineamientos institucionales definidos en el Plan de Desarrollo Institucional (PDI) 2025–2032. Estos principios orientan la gestión integral de la seguridad y la privacidad en la ETITC y constituyen la base conceptual sobre la cual se planifican y ejecutan las acciones del Sistema de Gestión de Seguridad de la Información (SGSI). Los principios rectores son los siguientes:

a. Confidencialidad: Asegurar que la información institucional, independientemente de su formato o medio, y en aquellos casos

exceptuados por la Ley 1712 de 2014 sobre transparencia y acceso a la información pública, sea accesible únicamente por personas, procesos o sistemas autorizados. Este principio se extiende tanto a datos administrativos como académicos, investigativos y de terceros.

b. Integridad: Asegurar que la información sea precisa, completa, consistente y esté protegida contra modificaciones no autorizadas, manteniendo la confiabilidad necesaria para la toma de decisiones institucionales.
c. Disponibilidad: Asegurar que la información, los sistemas y los servicios que la soportan estén accesibles y operativos cuando los usuarios autorizados los requieran para el cumplimiento de las funciones misionales, académicas, administrativas e investigativas.
d. Privacidad: Proteger los datos personales conforme a la normatividad vigente, asegurando su tratamiento adecuado, proporcional, informado y orientado a la protección de los derechos de los titulares.
e. Legalidad y Cumplimiento Normativo: Dar cumplimiento a las leyes, reglamentos, políticas y estándares técnicos aplicables a la seguridad y privacidad de la información, incorporando buenas prácticas nacionales e internacionales dictadas en el MSPI, la norma NTC ISO/IEC 27001:2022 y los lineamientos del MinTIC.
f. Gestión del Riesgo: Tomar decisiones con base en la identificación, análisis, evaluación y tratamiento de riesgos conforme a la Guía DAFP y los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información, asegurando la priorización de controles.
g. Responsabilidad y Rendición de Cuentas: Promover que cada servidor público, docente, administrativo, contratista y tercero entienda y asuma sus responsabilidades en materia de seguridad y privacidad de la información.
h. Mejora Continua: Consolidar un enfoque sistemático de revisión, evaluación y perfeccionamiento del SGSI, asegurando adaptabilidad ante riesgos emergentes, nuevas tecnologías y cambios normativos.
i. Cultura Institucional de Seguridad: Impulsar la sensibilización, formación y apropiación del comportamiento seguro por parte de toda la comunidad institucional, como elemento transversal al PDI y a los seis ejes estratégicos.

5.2 Política Institucional de Seguridad de la Información

La ETITC cuenta con una Política de Seguridad de la Información institucional (Acuerdo 012 de julio del 2024), que será revisada durante la vigencia del presente Plan con el propósito de verificar su alineación a:

- Resolución 02277 de junio del 2025.
- Versión actualizada 2025 del MSPI.
- El Sistema de Gestión de Seguridad de la Información basado en NTC ISO/IEC 27001:2022.
- Los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información.
- El PDI 2025–2032 y sus seis ejes estratégicos.

5.3 Relación entre los Principios, la Política y la Gestión Institucional

Los principios rectores y la Política de Seguridad de la Información constituyen los lineamientos base que permiten:

- Alinear la seguridad con los ejes estratégicos del PDI 2025–2032.
- Orientar la toma de decisiones basada en gestión del riesgo.
- Facilitar la planificación del año 2026 dentro del ciclo del MSPI.
- Permitir asegurar que los controles del Anexo A de la NTC ISO/IEC 27001:2022 respondan a necesidades reales, priorizadas y verificables.
- Guiar las acciones de sensibilización, formación y cultura de seguridad digital.

En consecuencia, este capítulo sienta las bases conceptuales que permitirán que el Plan de Seguridad y Privacidad de la Información se ejecute con coherencia, solidez técnica, soporte normativo y alineación estratégica.

6. DIAGNÓSTICO DEL ESTADO ACTUAL DEL SGSI

El diagnóstico inicial constituye el punto de partida para la planificación y ejecución del Plan de Seguridad y Privacidad de la Información – vigencia 2026. Su propósito es identificar el estado actual de la Seguridad de la Información en la ETITC, determinar el nivel de madurez alcanzado según el Modelo de Seguridad y Privacidad de la Información (MSPI) y establecer las brechas existentes frente a los requisitos de la NTC ISO/IEC 27001:2022 y sus controles del Anexo A. Este análisis permite orientar la priorización de actividades, recursos y controles durante el año 2026.

6.1 Resultados del Autodiagnóstico

La Escuela Tecnológica Instituto Técnico Central (ETITC) ha alcanzado un nivel de madurez OPTIMIZADO en su Sistema de Gestión de Seguridad de la Información, con una calificación global de 82/100 puntos y un avance del 92% en la implementación del ciclo PHVA (Planificar-Hacer-Verificar-Actuar). En el diagnóstico detallado de los controles de seguridad según ISO 27001:2022 Anexo A, se identifica brechas críticas y establece las bases para el desarrollo del Plan de Seguridad y Privacidad de la Información institucional.

- Fortaleza institucional en controles organizacionales (83/100) y físicos (89/100)
- Brecha crítica en controles tecnológicos (76/100) - déficit de 24 puntos
- Oportunidad de mejora en controles de personas (80/100) - déficit de 20 puntos
- Implementación del SGSI con certificación ICONTEC con respecto a los requisitos especificados en la norma ISO/IEC 27001:2022 (92% de avance)

6.2 Evaluación Detallada Por Dominios De Control

CONTROLES ORGANIZACIONALES A.5

Calificación: 83/100
Nivel de Madurez: OPTIMIZADO
Brecha: 17 puntos

Análisis:

Los controles organizacionales de la ETITC muestran un alto grado de formalización y aplicación sistemática. La Escuela cuenta con políticas documentadas, estructura de gobierno de seguridad de la información y procedimientos de gestión de riesgos establecidos.

Fortalezas Identificadas:

- Políticas de seguridad de la información aprobadas y comunicadas
- Asignación clara de roles y responsabilidades
- Procesos de gestión de riesgos operativos
- Contratos con terceros incluyen cláusulas de seguridad

Oportunidades de Mejora:

- Actualización periódica de políticas
- Documentación de procedimientos específicos por áreas
- Integración de seguridad en la gestión de proyectos institucionales

CONTROLES DE PERSONAS - A.6

Calificación: 80/100
Nivel de Madurez: GESTIONADO
Brecha: 20 puntos

Análisis:

Aunque existe gestión de los controles relacionados con el personal, este dominio presenta la segunda brecha más significativa. La cultura de seguridad requiere fortalecimiento mediante programas de sensibilización continuos.

Fortalezas Identificadas:

- Proceso de vinculación incluye verificación de antecedentes
- Acuerdos de confidencialidad con servidores públicos y contratistas
- Procedimiento disciplinario para incidentes de seguridad

Oportunidades de Mejora

- Capacitación continua: programa estructurado de formación en seguridad
- Concienciación: campañas periódicas sobre amenazas actuales (phishing, ingeniería social)
- Evaluación de competencias: medición de conocimientos en seguridad del personal
- Gestión de salida: proceso formal de desvinculación y revocación de accesos

CONTROLES FÍSICOS A.7

Calificación: 89/100
Nivel de Madurez: OPTIMIZADO
Brecha: 11 puntos

Análisis:

Este es el dominio con mejor desempeño en la ETITC. Los controles físicos de acceso, protección de instalaciones y gestión de equipos están bien establecidos y funcionan de manera efectiva.

Fortalezas Identificadas:

- Perímetros de seguridad definidos
- Control de acceso físico principal con carnet digital
- Áreas seguras para servidores y equipos críticos
- Protección contra amenazas ambientales (incendio, inundación)

Oportunidades de Mejora

- Actualización tecnológica de sistemas de videovigilancia
- Implementación de controles de acceso en más puntos críticos
- Fortalecimiento del mantenimiento preventivo de infraestructura

CONTROLES TECNOLÓGICOS A.8

Calificación: 76/100
Nivel de Madurez: GESTIONADO
Brecha: 24 puntos

Análisis:

Los controles tecnológicos presentan la brecha más significativa del SGSI. Aunque existen capacidades básicas de protección, se requiere inversión y modernización para alcanzar niveles de seguridad avanzados acordes con las amenazas actuales.

Fortalezas Identificadas:

- Firewall perimetral implementado
- Software Antivirus instalado en estaciones de trabajo
- Respaldos periódicos de información crítica
- Segregación de red

Oportunidades de Mejora

- Gestión de identidad y acceso: implementación de autenticación multifactor (MFA)
- Protección de datos: cifrado de información sensible en reposo y en tránsito
- Monitoreo y detección: sistema SEM para análisis de eventos de seguridad, alineado un SOC e inteligencia de amenazas
- Gestión de vulnerabilidades: escaneo periódico, parches de seguridad y seguimiento a planes de mejoramiento
- Seguridad en la nube: controles para servicios cloud utilizados
- Gestión de logs: centralización y retención de registros de auditoría

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	83	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	80	100	GESTIONADO
A.7	CONTROLES FÍSICOS	89	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	76	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		82	100	OPTIMIZADO

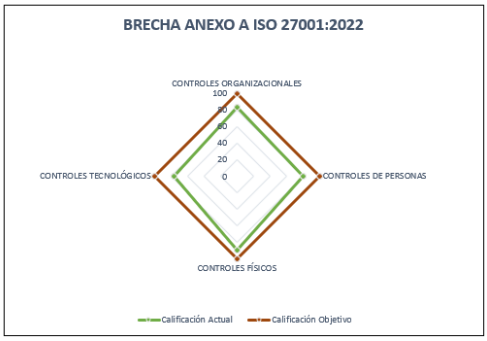

Ilustración 1. Pantallazo Autodiagnóstico MSPI

6.3 Brechas MSPI por fase del modelo

Fase MSPI	Hallazgos
Diagnóstico	Existe evaluación general, pero se requiere mayor profundidad en clasificación de información y fortalecimiento del marco institucional.
Planificación	No se evidencia una integración de seguridad en la planeación y gestión de proyectos institucionales.
Operación	Algunos procesos (gestión de incidentes, vulnerabilidades, riesgos) presentan implementación parcial o no uniforme.
Evaluación y Mejora	La auditoría no está plenamente integrada al SGSI, lo que limita la mejora continua.

7. PLAN DE ACCIÓN

El Plan de Acción define las **metas, estrategias, actividades, responsables, recursos e indicadores** necesarios para avanzar en la consolidación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) de la ETITC durante la vigencia 2026. Su formulación se basa en:

- Las brechas identificadas en el **autodiagnóstico MSPI 2025 y el SGSI**.
- Los requisitos de la **NTC ISO/IEC 27001:2022** (controles del Anexo A).
- La metodología de **gestión de riesgos DAFP – MSPI**.
- La articulación con el **PDI 2025–2032** y sus seis ejes estratégicos.
- Las prioridades institucionales para fortalecer la confiabilidad y seguridad de los servicios y procesos académicos, administrativos, investigativos y de extensión.

7.1 Objetivos Específicos del Plan

1. **Revisar, actualizar y formalizar el marco institucional de seguridad y privacidad**, incluyendo Políticas de Seguridad de la Información y el resto de los documentos base del SGSI.
2. **Fortalecer el proceso de gestión de riesgos** conforme a la Guía DAFP y MSPI, integrando riesgos, vulnerabilidades, controles y SoA.
3. **Implementar de forma** completa, homogénea y funcional los procesos **de gestión de incidentes de seguridad digital y gestión de vulnerabilidades**.
4. **Elevar la cultura institucional de seguridad y privacidad**, fortaleciendo competencias, comportamientos seguros y apropiación de responsabilidades.

7.2 Plan de Acción 2026 – Estrategias, Actividades y Responsables

A continuación, se presenta el plan organizado por los objetivos específicos del plan, cada una con sus actividades anuales.

Estrategia 1: Actualización del Marco Institucional de Seguridad
Objetivo asociado: OE1
Responsable: Líder del SGSI
Corresponsables: Oficina de Planeación, Jurídica, Proceso TIC

Actividad 2026	Descripción	Responsables	Productos / Evidencias
1.1 Revisar la Política de	Revisión con base en la armonización	Líder SGSI – Jurídica –	Política Revisada o actualizada con

Actividad 2026	Descripción	Responsables	Productos / Evidencias
Seguridad de la Información	con MSPI, ISO/IEC 27001:2022, DAFP y PDI	Planeación – Comité de Gestión y Desempeño	aprobación; acuerdo ETITC.
1.2 Actualizar documentos base del SGSI	Procedimientos, normas internas, lineamientos, roles	Líder SGSI – Proceso de gestión TI	Documentos versionados; matriz documental
1.3 Integrar la seguridad en la gestión de proyectos institucionales	Delimitar dentro de la gestión de proyectos institucionales el rol de la seguridad de la información.	SGSI - Planeación	Documentación formal.

Estrategia 2: Fortalecimiento de la Gestión de Riesgos
Objetivo asociado: OE2
Responsable líder: Líder SGSI

Actividad 2026	Descripción	Productos / Evidencias
2.1 Ejecutar el plan de tratamiento de riesgos	De acuerdo con la documentación del plan	De acuerdo con el Plan
2.2 Integrar riesgos con controles del Anexo A 2022	Riesgo → Control → Evidencia	Matriz riesgos–controles

Estrategia 3: Implementación del proceso para gestión de incidentes de seguridad digital y gestión de vulnerabilidades.
Objetivo asociado: OE3
Responsable líder: Proceso Gestión TI
Corresponsables: SGSI, proveedores, líderes de proceso

Controles priorizados según diagnóstico:

- A.5.7 Inteligencia de amenazas
- A.5.23 Seguridad en la nube
- A.8.9 Gestión de configuración
- A.8.16 Monitoreo
- A.8.28 Codificación segura

Actividad 2026	Descripción	Productos / Evidencias
3.1 Implementar centro de operaciones de seguridad (SOC)	Establecer un centro de operaciones de seguridad cibernética que permita el monitoreo 24/7 x 365 de eventos de seguridad y su gestión acompañada con una respuesta de primer nivel a incidentes confirmados	SOC de la ETITC
3.2 Implementar la gestión de vulnerabilidades técnicas en la infraestructura de TI	Gestión de vulnerabilidades técnicas de la infraestructura de TI y Sistemas de Información de forma permanente	Evidencia de la gestión de vulnerabilidades
3.3 Implementar la gestión de identidad y acceso seguro	Implementar la autenticación multi factor (MFA) para aquellos sistemas con tal capacidad (Obligatoria usuarios directivos, administrativos, docentes y contratistas).	Autenticación MFA implementada

Estrategia 4: Cultura Institucional y Capacitación
Objetivo asociado: OE4
Responsable líder: SGSI y Talento Humano

Actividad 2026	Descripción	Productos / Evidencias
4.1 Campaña trimestral de cultura digital	Sitio web, material audiovisual, correos educativos	Registros de difusión
4.2 Capacitación por rol	Docentes, administrativos, TIC, contratistas	Registros, listas de asistencia

10.3 Indicadores del Plan

Algunos indicadores clave para 2026:

- % de implementación de actividades del plan.
- % de funcionarios capacitados según rol.
- Tiempo promedio de respuesta a incidentes.
- Tasa de remediación de vulnerabilidades.

10.4 Cronograma General

- **Enero–Abril:** Diagnóstico complementario, política, documentos y planificación.
- **Marzo–Diciembre:** Implementación de SOC, formación, cultura, riesgos.
- **Marzo - Diciembre:** Indicadores, revisión por el comité de Gestión y Desempeño, cierre anual.

8. 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
23/01/2026	4	Actualización integral del Plan de Seguridad y Privacidad de acuerdo con los lineamientos de la resolución 02277 de junio del 2025 (MinTIC)

ELABORÓ	REVISÓ	APROBÓ
JORGE A. TAMAYO R. Líder de Gestión de Seguridad de la Información	**JAVIER A. DIAZ M.** Administrador de la Documentación	**COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**