PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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 23 de enero del 2026.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Escuela Tecnológica Instituto Técnico Central (ETITC), como institución pública de educación superior, reconoce la importancia de gestionar de manera integral los riesgos que puedan afectar la seguridad y privacidad de la información en todos sus procesos, sedes y sistemas. Este Plan de Tratamiento de Riesgos se formula en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) actualizado en 2025 por el Ministerio TIC, la norma técnica NTC ISO/IEC 27001:2022 y su Anexo A, así como la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP) para la administración del riesgo en el marco del Modelo Integrado de Planeación y Gestión (MIPG).

La metodología utilizada para la valoración de riesgos corresponde a la versión 7 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, basada en la combinación de probabilidad e impacto, con representación en mapa de calor y opciones estándar de tratamiento (evitar, mitigar, transferir, aceptar), complementada con el detalle y profundidad que aporta y exige el MSPI, específicamente en los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

Este documento es de alto nivel y se encuentra alineado con:

- Los seis 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, y (6) Cuidado por el bienestar y la vida.
- La misión y visión institucional, la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (Acuerdo 012 de julio del 2024) y el Plan de Desarrollo Institucional 2025–2032, asegurando que el tratamiento de riesgos aporte valor a los servicios y fortalezca la confianza digital.

La ETITC reafirma su compromiso institucional con la gestión de riesgos de seguridad y privacidad de la información, garantizando la asignación de recursos humanos, tecnológicos y financieros adecuados para su desarrollo. Este compromiso busca respaldar a los responsables en la implementación efectiva de los controles definidos, así como en el seguimiento y monitoreo continuo de los riesgos, asegurando la sostenibilidad del Sistema de Gestión de Seguridad de la Información y la protección integral de los activos de información.

El Plan adopta los controles del Anexo A de la ISO/IEC 27001:2022, organizados en categorías organizativas, de personas, físicas y tecnológicas, y define su Declaración de Aplicabilidad (SoA) en función de los riesgos identificados. Asimismo, establece criterios para la aceptación de riesgos, responsables, recursos, cronogramas y mecanismos de seguimiento y mejora continua.

La aprobación del Plan corresponde al Comité Institucional de Gestión y Desempeño (CIGD), en tanto que su elaboración es responsabilidad del líder del Sistema de Gestión de Seguridad de la Información (SGSI), quien coordina la implementación con las dependencias académicas y administrativas, garantizando el cumplimiento normativo y la privacidad de los datos sensibles.

Este Plan constituye un instrumento estratégico que integra y articula la gestión de riesgos de seguridad de la información con la planeación institucional, contribuyendo a la resiliencia organizacional, la gestión segura de la información en la prestación del servicio educativo y la consolidación de una cultura de seguridad y privacidad en la ETITC.

2. OBJETIVO

Establecer y ejecutar, durante la vigencia 2026, un conjunto integral de acciones para el tratamiento de riesgos de seguridad y privacidad de la información en todos los procesos, sedes y sistemas de la ETITC, mediante la implementación y fortalecimiento de controles alineados al MSPI, la norma

NTC ISO/IEC 27001:2022 y la guía del DAFP, asegurando la reducción del riesgo residual a niveles aceptables, el seguimiento continuo y la sostenibilidad del Sistema de Gestión de Seguridad de la Información, en coherencia con los seis ejes estratégicos institucionales y el Plan de Desarrollo Institucional 2025–2032.

3. ALCANCE

El alcance del presente Plan cubre toda la institución y sedes, garantizando que las acciones de tratamiento se apliquen de manera transversal adoptando un enfoque a procesos y sus interacciones, así como a la infraestructura tecnológica y física.

4. TERMINOS Y DEFINICIONES

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

ACTIVO CRÍTICO: Son aquellos elementos o componentes que hacen parte de la infraestructura crítica.

ACEPTACIÓN DE RIESGO: Decisión de asumir un riesgo.

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

EVALUACIÓN DEL RIESGO: Definir el riesgo estimado contra criterios de riesgo para determinar su importancia y nivel de criticidad.

IMPACTO: Se entiende como las consecuencias que puede ocasionar a la ETITC la materialización del riesgo.

NIVEL DE RIESGO: Da el resultado en donde se ubica el riesgo por cada activo de información.

PROBABILIDAD: Se entiende como la posibilidad de ocurrencia del riesgo.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).

RIESGO INHERENTE: Nivel de riesgo existente en un proceso, sistema o actividad antes de aplicar cualquier medida de control o tratamiento. Representa la exposición natural al riesgo considerando las amenazas y vulnerabilidades asociadas al activo, sin mitigación ni salvaguardas implementadas.

RIESGO RESIDUAL: Nivel restante de riesgo después del tratamiento del riesgo.

TRATAMIENTO DEL RIESGO: Implementación de acciones de mejora que permitan mitigar el riesgo.

VALORACIÓN DEL RIESGO: Es el proceso de análisis y evaluación del riesgo.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

5. IDENTIFICACIÓN, GESTIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se describen los lineamientos generales mediante el cual la ETITC identifica, analiza, evalúa, gestiona y trata los riesgos que puedan

afectar la seguridad y privacidad de la información, asegurando la protección de los activos críticos y el cumplimiento normativo, en concordancia con el MSPI, la NTC ISO/IEC 27001:2022, la guía del DAFP y el Procedimiento para administración de riesgos GSI-CA-PC-06.

5.1 Identificación de riesgos

Inventario de activos de información (hardware, software, datos, servicios, infraestructura).
Identificación de amenazas y vulnerabilidades asociadas.
Relación de riesgos con procesos estratégicos y ejes institucionales.

5.2 Análisis y evaluación

Aplicación de la matriz DAFP (probabilidad × impacto) con mapa de calor a través del formato GSI-CA-FO-9.
Clasificación del nivel de riesgo: bajo, medio, alto, extremo.
Priorización de riesgos críticos que afectan la continuidad institucional.

5.3 Opciones de tratamiento

Evitar: eliminar la causa del riesgo.
Mitigar: implementar controles para reducir probabilidad o impacto.
Transferir: delegar el riesgo (p. ej., seguros, contratos).
Aceptar: asumir el riesgo residual dentro de niveles tolerables.

5.4 Selección de controles

Basada en el Anexo A de la ISO/IEC 27001:2022 y lineamientos MSPI.
Controles organizativos, humanos, físicos y tecnológicos.
Definición de la Declaración de Aplicabilidad (SoA).

5.5 Seguimiento y mejora continua

Monitoreo periódico del avance de las acciones.

Reporte al Comité Institucional de Gestión y Desempeño (CIGD).
Integración con el Mapa de Riesgos Institucional y el MIPG.

A continuación, se determinan las actividades del plan de tratamiento de riesgos de la ETITC:

Estrategia	Actividades	Evidencia	Responsable	Fecha de Programación de Tareas	
				Fecha Inicial	Fecha Final
Implementar un enfoque integral que combine la identificación, análisis y priorización de riesgos con la aplicación de controles preventivos, detectivos y correctivos alineados al MSPI y la ISO/IEC 27001:2022	Actualizar el inventario de activos de información y clasificar la criticidad de los activos de acuerdo con la metodología GSI-ME-01	Formato actualizado con el inventario y clasificación	Profesional de Gestión de Informática y Telecomunicaciones Líderes de procesos Líder SGSI	01/02/2026	15/04/2026
	Actualizar y evaluar riesgos aplicando el formato GSI-CA-FO-9	Mapa de riesgos diligenciado y validado	Líder SGSI	15/04/2026	30/04/2026
	Revisar y aprobar la Declaración de Aplicabilidad (SoA) con controles ISO/IEC 27001:2022 (Dominios Organizacional, Personas, físicos y Tecnológico)	Documento SoA validado por el SIACET	Líder SIACET Líder SGSI	02/05/2026	30/08/2026
	Implementar controles priorizados para riesgos inherentes críticos	Reportes de implementación y evidencias técnicas	Líderes de procesos Profesional de Gestión de Informática y Telecomunicaciones	01/06/2026	30/09/2026
	Realizar seguimiento y validación a la implementación de controles y reporte al CIGD sobre el avance del Plan	Mapa de riesgos actualizado Actas o reportes de seguimiento	Líder SGSI Comité Institucional de Gestión y Desempeño	01/10/2026	15/12/2026

Instrumentos relacionados:
GSI-CA-FO-09 MAPA Y PLAN DE TRATAMIENTO DE RIESGOS
GSI-ME-01 METODOLOGÍA PARA IDENTIFICAR, CLASIFICAR Y VALORAR LOS ACTIVOS DE INFORMACIÓN DE LA ETITC

6. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
26/01/2024	1	Adopción del Documento
27/01/2024	2	Actualización del Plan De Tratamiento de Riesgos de Seguridad y Privacidad de la Información 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 al nuevo formato GSI-CA-FO-09 Mapa y Plan de Tratamiento de Riesgos.
10/11/2025	3	Actualización de codificación del Documento
23/01/2026	4	Actualización integral y sustancial del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, hacia un enfoque más completo, riguroso y alineado con marcos y normas nacionales y mejores prácticas internacionales, fortaleciendo claramente la gestión de riesgos de seguridad y privacidad en la ETITC. Incorpora un compromiso institucional de asignación de recursos humanos, tecnológicos y financieros, alineando gobernanza y sostenibilidad del SGSI. Se actualiza la tabla de actividades que detalla Estrategia con cinco principales acciones, cada una con evidencia, responsables, fechas de inicio y fin, lo que garantiza un nivel concreto de gestión y seguimiento. Se define claramente la Declaración de Aplicabilidad (SoA) como componente crucial, con referencia a controles organizativos, físicos, tecnológicos y de personas. Se actualiza objetivo a uno integral y cuantificable. Se expande el alcance institucional: ahora cubre explícitamente todos los procesos, sedes y sistemas.

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**