PLAN DE ACCIÓN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DIGITAL

vigencia (2026)

Oficina de Riesgos
19 de noviembre 2025

Versión 1

Tabla de Contenido

1. Introducción

El ICETEX, en su compromiso con la mejora continua, implementa un enfoque sistemático para la gestión de los riesgos de seguridad digital que permite identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional, con el propósito de prevenir impactos significativos sobre esta.

En concordancia con lo anterior, y en cumplimiento de los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), se establece el Plan de Acción de Tratamiento de Riesgos de Seguridad Digital del ICETEX para la vigencia 2026. Este plan define la estrategia de gestión de riesgos de seguridad digital de la Entidad, incorporando la revisión de los controles establecidos en la norma ISO/IEC 27001 y las medidas de seguridad de la información aplicables al entorno operativo, mediante metodologías que aseguren la protección de los activos de información en cuanto a confidencialidad, integridad, disponibilidad y privacidad.

Asimismo, el documento garantiza el cumplimiento de los requisitos normativos vigentes, los lineamientos del Sistema de Gestión de Seguridad Digital y del Programa Integral de Protección de Datos Personales, e integra las oportunidades de mejora identificadas en la gestión correspondiente a la vigencia 2025.

Este Plan se articula con el Plan de Acción de Seguridad y Privacidad de la Información y se desarrolla en alineación con el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

2. Información general

Nombre del Plan de acción o estrategia institucional	Plan de Acción de Tratamiento de Riesgo de Seguridad Digital
Nombre y código rubro presupuestal asociado	
Presupuesto asignado ($)	
Área responsable	Oficina de Riesgos
Política asociada y otros lineamientos	8. Seguridad digital
Proceso	Gestión de Riesgos No Financieros
Fecha de inicio	02/02/2026
Fecha de finalización	19/12/2026

3. Objetivo Estratégico

Optimizar los procesos a través del mejoramiento tecnológico, de la cultura organizacional y del gobierno corporativo para atender las necesidades de los grupos de incidencia.

4. Objetivo General

Fortalecer la gestión de los riesgos de seguridad digital del ICETEX mediante la implementación de acciones planificadas que permitan identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional, garantizando la protección de la confidencialidad, integridad, disponibilidad y privacidad de los activos de información, en cumplimiento de los lineamientos normativos, el Sistema de Gestión de Seguridad Digital y el Modelo Integrado de Planeación y Gestión (MIPG).

4.1 Objetivos Específicos

- Identificar y analizar los riesgos de seguridad digital asociados a los procesos de la Entidad.
- Evaluar los riesgos detectados para establecer su nivel de impacto y probabilidad, de acuerdo con los criterios definidos en el Sistema de Gestión de Seguridad Digital.
- Definir e Implementar acciones y controles de tratamiento con las áreas que permitan reducir los niveles de riesgo residual.
- Monitorear de manera continua la eficacia de las medidas de tratamiento de riesgo y actualizar el plan según los resultados obtenidos.
- Fortalecer la cultura institucional de seguridad digital mediante la comunicación oportuna de riesgos y la sensibilización del personal sobre prácticas seguras en el manejo de la información.
- Alinear la gestión de riesgos de seguridad digital con los requisitos normativos, el Programa Integral de Protección de Datos Personales y el Modelo Integrado de Planeación y Gestión (MIPG).
- Incorporar las oportunidades de mejora identificadas en la vigencia anterior para optimizar la prevención y respuesta ante incidentes de seguridad digital.

5. Alcance

El Plan de Acción de Tratamiento de Riesgos de Seguridad Digital del ICETEX para la vigencia 2026 abarca todos los procesos de la institución, orientando la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información. Su aplicación involucra a las dependencias relacionadas con la gestión de seguridad digital y se articula con el Sistema de Gestión de Seguridad Digital, el Programa Integral de Protección de Datos Personales y el Modelo Integrado de Planeación y Gestión (MIPG), en coherencia con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

6. Normatividad

El presente Plan de Acción de Tratamiento de Riesgos de Seguridad Digital se basa en el cumplimiento de la normatividad vigente, los lineamientos emitidos por las autoridades competentes y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP). Entre las principales disposiciones legales, reglamentarias, técnicas y orientativas que sustentan este plan, se incluyen:

- Ley 1581 de 2012 – Protección de Datos Personales, sujeta a actualización conforme a proyecto de ley radicado en 2025 para modernización del marco normativo.
- Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública.
- Ley 2088 de 2021 – Regulación del trabajo en casa y disposiciones relacionadas.
- Decreto 1074 de 2015 – Decreto Único Reglamentario Sector Comercio, Industria y Turismo (artículos 25 y 26 sobre Registro Nacional de Bases de Datos).
- Decreto 1078 de 2015 – Decreto Único Reglamentario Sector Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 – Decreto Único Reglamentario Sector Función Pública, con políticas de Gobierno Digital y Seguridad Digital.
- Decreto 612 de 2018 – Directrices para integración de planes institucionales en los planes de acción de las entidades públicas.
- Decreto 2106 de 2019 – Estrategia de seguridad digital alineada con lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Decreto 338 de 2022 – Lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- Resolución 500 de 2021 – Lineamientos y estándares para la estrategia de seguridad digital, adopción del modelo de seguridad y privacidad.

- Resolución 460 de 2022 – Plan Nacional de Infraestructura de Datos y hoja de ruta para la Política de Gobierno Digital.
- Resolución 1519 de 2020 – Estándares y directrices para acceso a información pública, accesibilidad web, seguridad digital y datos abiertos.
- Proyecto de ley para actualización de la Ley 1581 de 2012 (2025), que fortalecerá la protección de datos personales ante tecnologías emergentes.
- Circular Externa 002 de 2024 (Superintendencia de Industria y Comercio) – Lineamientos específicos para tratamiento de datos en sistemas de inteligencia artificial.
- Modelo de Seguridad y Privacidad Digital (MSPI) – Estrategia de Gobierno Digital del MinTIC.
- Normas técnicas NTC ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información actualizado.
- Modelo Integrado de Planeación y Gestión (MIPG) – Dimensión Seguridad Digital.
- CONPES 3701 de 2011 – Estrategia de Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
- Directiva Presidencial 03 de 2021 – Lineamientos para uso seguro de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva Presidencial 02 de 2022 – Lineamientos para actualización de catálogos, sistemas, bases de datos y estrategia de seguridad digital institucional.
- Circulares de la Superintendencia Financiera de Colombia (029 de 2014 y Circular Externa 033 de 2020) – Gestión del riesgo de ciberseguridad, calidad en manejo de información y reporte de incidentes.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP), que establece los lineamientos técnicos y metodológicos para la identificación, evaluación, tratamiento y monitoreo de riesgos institucionales, con un enfoque integral y acorde a la normatividad vigente.

Este marco normativo garantiza que el Plan de Acción esté alineado con los requerimientos legales actuales y las mejores prácticas internacionales para la protección, control y gestión de los riesgos de seguridad digital y la protección de datos personales.

7. Formulación del plan de acción o estrategia institucional

7.1 Generalidades del plan

Para definir las actividades del presente Plan de Acción de Tratamiento de Riesgos de Seguridad Digital para el año 2026, se realizó un análisis detallado de la situación actual frente a la situación deseada, buscando siempre una estricta alineación con la normatividad vigente en materia de seguridad y privacidad de la información. Este ejercicio, coordinado por la Oficina de Riesgos, rectora en la gestión y seguimiento del plan, garantiza que las actividades propuestas respondan tanto a las brechas identificadas como a los objetivos estratégicos institucionales.

Situación actual

Las revisiones realizadas a controles específicos definidos en la norma ISO/IEC 27001:2022 han evidenciado necesidades de fortalecimiento en su diseño y efectividad, a fin de asegurar una protección adecuada de la información institucional. Se ha identificado la necesidad de continuar con verificaciones y revisiones periódicas a todo el Sistema de Gestión de Seguridad Digital, para implementar medidas correctivas y mitigantes eficaces ante los riesgos detectados. Esta situación refleja demandantes retos en materia de cierre de brechas y adaptación a un entorno de amenazas dinámicas y crecientes.

Situación deseada

Se aspira a que el Sistema de Gestión de Seguridad Digital sea un proceso transversal sólido que respalde activamente el logro de las metas institucionales, aportando una gestión integral de la seguridad de la información en todos los procesos y proyectos institucionales. Esto implica contar con controles efectivos que garanticen la confidencialidad, integridad, disponibilidad y privacidad de la información, respaldados por un esquema riguroso de verificación de controles basados en ISO/IEC 27001:2022, con énfasis en el diseño y efectividad comprobados. Se prevé el cierre definitivo de las brechas halladas en auditorías internas y externas, fortaleciendo la resiliencia digital de la Entidad.

Además, se proyecta la consolidación de un esquema robusto de monitoreo y respuesta ágil a incidentes de seguridad digital, que minimice impactos y facilite la continuidad operativa. Paralelamente, se busca la implementación sistemática de controles para garantizar la protección de la privacidad en todas las dependencias, de acuerdo con los lineamientos del Programa Integral de Protección de Datos Personales.

La Oficina de Riesgos, como área encargada de coordinar este plan, garantiza la gestión integral del mismo, promoviendo el compromiso interinstitucional, la actualización continua de las políticas y procedimientos, y el seguimiento riguroso a la ejecución del plan, asegurando la mejora continua y alineación con la normativa vigente y las mejores prácticas internacionales.

7.2 Cronograma

Teniendo en cuenta que el Modelo Integrado de Planeación y Gestión (MIPG) establece un marco de referencia integral para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión institucional en entidades públicas, y considerando la necesidad de cumplir con los requisitos normativos que incluyen la gestión de riesgos que puedan afectar cualquier activo de información en cuanto a confidencialidad, integridad, disponibilidad y privacidad, en el presente plan se incorporan actividades específicas de monitoreo de riesgos de seguridad digital, revisión continua de controles para evaluar su diseño y efectividad, y la gestión integral de incidentes de seguridad digital desde su prevención hasta su corrección.

Estas actividades se desarrollan en concordancia tanto con el Sistema de Gestión de Seguridad Digital como con el Programa Integral de Protección de Datos Personales, garantizando un enfoque comprometido con la protección efectiva de la información institucional. La Oficina de Riesgos tiene el rol central y responsable de coordinar la ejecución, seguimiento y evaluación de este plan, asegurando la articulación entre las diferentes áreas y el cumplimiento estricto de los lineamientos institucionales y normativos.

El Plan de Acción de Tratamiento de Riesgos para el año 2026 está conformado por las siguientes actividades, cuyo cronograma será elaborado y ajustado de acuerdo con la planificación estratégica institucional y los requerimientos emergentes derivados del análisis de riesgos y auditorías internas.

N°	Etapa o fase / Actividad / Tarea	Fecha Inicio	Fecha Fin
1.	**Monitoreo, análisis y gestión integral de riesgos de seguridad de la información**	**01/02/2026**	**30/11/2026**
1.1	Revisar y actualizar la metodología de riesgos de seguridad de la información	02/03/2026	10/04/2026
1.1.1	**Entregable:** Metodología actualizada	**01/04/2026**	**30/04/2026**
1.2	Monitoreo, identificación y aceptación de riesgos de seguridad de la información	01/06/2026	31/10/2026
1.3	Evaluación de eficacia de controles de la matriz de riesgos de seguridad de la información	01/06/2026	31/10/2026

1.4	Seguimiento planes de acción para mitigación de riesgos de seguridad de la información.	01/02/2026	31/10/2026
1.4.1	**Entregable:** Matriz de riesgos con mapa y plan de tratamiento de seguridad de la información	**01/11/2026**	**30/11/2026**
2.	**Seguimiento y mejora continua del modelo MSPI**	**01/01/2026**	**30/12/2026**
2.1	Seguimiento del MSPI a los procesos	01/01/2026	30/12/2026
2.1.1	**Entregable:** Formato 462 diligenciado por parte de los procesos – Trimestral	01/01/2026	30/12/2026
2.2	Diligenciamiento Autodiagnóstico del MSPI 2026	01/07/2026	30/12/2026
2.3	Presentación en comité de riesgos de resultados del Autodiagnóstico del MSPI	01/10/2026	30/12/2026
2.4.1	**Entregable:** Herramienta diligenciada de MSPI	**01/02/2026**	**19/12/2026**
3.	**Seguimiento a la remediación de Vulnerabilidades**	**01/02/2026**	**30/11/2026**
3.1.	Asistencia y seguimiento a la remediación de vulnerabilidades de acuerdo con las convocatorias realizadas por la VOT - Dirección de Tecnología.	01/02/2026	30/11/2026
3.1.1	**Entregable:** Actas de la reunión de la VOT	**01/02/2026**	**30/11/2026**
4.	**Sensibilización en riesgos de seguridad digital**	**01/03/2026**	**31/10/2026**
4.1	Reuniones con los lideres para sensibilizarlos sobre la gestión de riesgos de seguridad digital	01/03/2026	31/10/2026
4.1.1	**Entregable:** Listado de asistencia	**01/03/2026**	**31/10/2026**
5.	**Pruebas de Controles ISO 27001:2022**	**01/02/2026**	**30/11/2026**
5.1	Reuniones de validación de controles con las áreas del ICETEX	01/02/2026	30/11/2026
5.2	Elaboración y remisión del Informe con observaciones o recomendaciones de la prueba de controles ISO 27001:2022	01/02/2026	30/11/2026
5.3.1	**Entregable:** Informe y Memorando dirigido a las áreas	**01/02/2026**	**30/11/2026**

7.3 Seguimiento y evaluación

1. **Porcentaje de monitoreo y actualización de riesgos en procesos**
   - Fórmula:

$$= \left(\frac{\text{No. de procesos con riesgos identificados o actualizados}}{\text{No. Total procesos de la Entidad}}\right) \times 100$$

   - Fuente: Resultado del monitoreo de riesgos de seguridad
   - Meta: 95%
   - Periodicidad: anual

8. Control de cambios

Versión	Detalle del cambio	CIGD N°	Fecha aprobación
1.	***Aprobación Plan de Acción de Tratamiento de Riesgo de Seguridad Digital***	14	Diciembre 2025