2026

UNIPAZ®
Instituto Universitario de la Paz

Plan de Seguridad y Privacidad de la Información

Tabla de contenido

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

INTRODUCCIÓN

El uso intensivo y estratégico de las Tecnologías de la Información y las Comunicaciones (TIC) se ha consolidado como un factor determinante para la generación de valor público, la modernización institucional y el cumplimiento de los objetivos misionales en las entidades del Estado. No obstante, dicho aprovechamiento implica desafíos crecientes asociados a la protección de la información, la gestión de los riesgos digitales, la privacidad de los datos y la continuidad de los servicios tecnológicos, los cuales deben ser abordados de manera integral, sistemática y alineada con la planeación institucional.

En el Instituto Universitario de la Paz – UNIPAZ, las Tecnologías de la Información y las Comunicaciones se conciben como habilitadores estratégicos para el cumplimiento de los planes, programas y objetivos institucionales, en coherencia con su misión académica, administrativa y social. En este sentido, la Alta Dirección ha dispuesto la incorporación de la gestión de las TIC, la seguridad digital y la protección de la información como componentes transversales de la planeación estratégica institucional, articulados al Plan de Desarrollo Institucional, al Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2026 y al Modelo Integrado de Planeación y Gestión – MIPG.

La información constituye uno de los activos más críticos de UNIPAZ, en la medida en que soporta los procesos estratégicos, misionales, de apoyo y de evaluación, así como la toma de decisiones, la prestación de servicios académicos y administrativos, la rendición de cuentas y el cumplimiento de los requerimientos normativos. Por ello, la seguridad y privacidad de la información deben ser gestionadas bajo un enfoque de riesgo, garantizando la confidencialidad, integridad, disponibilidad y privacidad de los datos, en un entorno caracterizado por la digitalización de procesos, la interoperabilidad de sistemas y el incremento de amenazas cibernéticas.

El Rector, como máxima autoridad institucional, lidera la planeación estratégica de las Tecnologías de la Información y la Seguridad Digital, asegurando su alineación con la Misión y Visión institucionales, y promoviendo una gestión orientada a la mejora continua, la eficiencia administrativa y la generación de confianza en el entorno digital. Este liderazgo se materializa en la adopción de políticas, planes y mecanismos de gobierno que permiten integrar la seguridad de la información y la privacidad de los datos en la gestión institucional.

El presente Plan de Seguridad y Privacidad de la Información tiene como propósito establecer y consolidar el Sistema de Gestión de Seguridad y Privacidad de la Información de UNIPAZ, tomando como referencia el Modelo de Seguridad y Privacidad de la Información – MSPI, la Política de Gobierno Digital, la Política de Seguridad Digital, y los estándares internacionales ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 27701, entre otros. Estos marcos proporcionan un enfoque metodológico basado en buenas prácticas para la gestión de riesgos, la implementación de controles y la protección integral de los activos de información.

Para la vigencia 2026, el Plan se orienta a fortalecer la gestión de los riesgos de seguridad digital y privacidad de la información, mediante la actualización del contexto institucional y tecnológico, la identificación y priorización de riesgos, la implementación y maduración de controles, el monitoreo permanente y la mejora continua. Así mismo, se articula con los ciclos de planeación,

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

seguimiento y evaluación definidos en el MIPG y con las tres líneas de defensa, asegurando su sostenibilidad, trazabilidad y efectividad en el tiempo.

De esta manera, el Plan de Seguridad y Privacidad de la Información de UNIPAZ se consolida como un instrumento estratégico que contribuye a la protección de la información institucional, la continuidad de los servicios tecnológicos, el cumplimiento normativo y la generación de confianza en la comunidad universitaria y los grupos de interés, apoyando de forma directa los objetivos definidos en el PETI UNIPAZ 2026 y la transformación digital de la institución.

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

1. OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información para el Instituto Universitario de la Paz – UNIPAZ, que oriente la implementación y fortalecimiento de la Política de Seguridad Digital y Privacidad de la Información, en coherencia con el Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital, los objetivos estratégicos institucionales, el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2026, y en cumplimiento del marco legal y normativo vigente, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

1.1. Objetivos específicos

- Estructurar las etapas del Plan de Seguridad y Privacidad de la Información de UNIPAZ, a partir del análisis del contexto institucional y tecnológico y del autodiagnóstico de madurez en seguridad digital, con el fin de establecer una estrategia integral de seguridad de la información alineada con el MSPI, el MIPG y la Política de Gobierno Digital.
- Implementar los controles técnicos, administrativos y organizacionales de seguridad y privacidad de la información, priorizados mediante la gestión de riesgos, a través de un cronograma y un plan de acción definidos para la vigencia 2026, que permitan mitigar las amenazas y vulnerabilidades asociadas a los activos de información y servicios digitales institucionales.
- Evaluar el nivel de implementación y madurez de la Política de Seguridad y Privacidad de la Información en UNIPAZ, mediante mecanismos de seguimiento, indicadores y revisión periódica durante la vigencia 2026, con el propósito de identificar brechas, verificar la efectividad de los controles y definir acciones de mejora continua.

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

2. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información del Instituto Universitario de la Paz – UNIPAZ se fundamenta en el marco constitucional, legal, reglamentario y de política pública que regula la protección de la información, la seguridad digital, la privacidad de los datos, la transparencia, el uso de las Tecnologías de la Información y las Comunicaciones y la gestión del riesgo en las entidades públicas del Estado colombiano.
Este marco normativo orienta la formulación, implementación, seguimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, en coherencia con el Modelo de Seguridad y Privacidad de la Información – MSPI, la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión – MIPG.

2.1. Marco constitucional

Constitución Política de Colombia (1991)

- Artículo 15: Derecho a la intimidad, al buen nombre y a la protección de los datos personales (hábeas data).
- Artículo 20: Libertad de expresión y acceso a la información.
- Artículo 23: Derecho fundamental de petición.
- Artículo 74: Derecho de acceso a documentos públicos.

2.2. Marco legal

- Ley 23 de 1982 – Régimen general de derechos de autor.
- Ley 44 de 1993 – Modifica y adiciona la Ley 23 de 1982 en materia de derechos de autor.
- Decisión Andina 351 de 1993 – Régimen común sobre derecho de autor y derechos conexos.
- Ley 527 de 1999 – Mensajes de datos, comercio electrónico y firmas digitales.
- Ley 594 de 2000 – Ley General de Archivos.
- Ley 850 de 2003 – Regulación de las veedurías ciudadanas.
- Ley 962 de 2005 – Racionalización de trámites administrativos.
- Ley 1221 de 2008 – Regulación del teletrabajo.
- Ley 1266 de 2008 – Régimen de hábeas data financiero y crediticio.
- Ley 1273 de 2009 – Protección penal de la información y los datos.
- Ley 1341 de 2009 – Principios de la sociedad de la información y las TIC.
- Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1450 de 2011 – Plan Nacional de Desarrollo 2010–2014.
- Ley 1474 de 2011 – Estatuto Anticorrupción.
- Ley 1581 de 2012 – Régimen general de protección de datos personales.

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Ley 1753 de 2015 – Plan Nacional de Desarrollo 2014–2018.
- Ley 1755 de 2015 – Derecho Fundamental de Petición.
- Ley 1915 de 2018 – Derechos de autor y derechos conexos.
- Ley 2052 de 2020 – Código General Disciplinario.
- Ley 2088 de 2021 – Regulación del trabajo en casa.

2.3. Marco reglamentario

- Decreto 2364 de 2012 – Firma electrónica.
- Decreto 2609 de 2012 – Gestión documental en entidades públicas.
- Decreto 1377 de 2013 – Reglamentación parcial de la Ley 1581 de 2012.
- Decreto 886 de 2014 – Registro Nacional de Bases de Datos.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC.
- Decreto 103 de 2015 – Reglamentación de la Ley de Transparencia.
- Decreto 1074 de 2015 – Reglamentación de la Ley 1581 de 2012 (RNBD).
- Decreto 1499 de 2017 – Adopción del Modelo Integrado de Planeación y Gestión – MIPG.
- Decreto 728 de 2017 – Fortalecimiento del modelo de Gobierno Digital.
- Decreto 1008 de 2018 – Lineamientos generales de la Política de Gobierno Digital.
- Decreto 612 de 2018 – Integración de planes institucionales al Plan de Acción.
- Decreto 2106 de 2019 – Simplificación y digitalización de trámites.
- Decreto 620 de 2020 – Servicios Ciudadanos Digitales.
- Decreto 1287 de 2020 – Seguridad de documentos firmados en trabajo en casa.
- Decreto 338 de 2022 – Gobernanza de la Seguridad Digital y creación del Modelo de Seguridad Digital.
- Decreto 767 de 2022 – Actualización de la Política de Gobierno Digital.
- Decreto 88 de 2022 – Digitalización y automatización de trámites.

2.4. Políticas públicas y documentos CONPES

- CONPES 3701 de 2011 – Lineamientos de política para ciberseguridad y ciberdefensa.
- CONPES 3854 de 2017 – Política Nacional de Seguridad Digital.
- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
- CONPES 4069 de 2022 – Política Nacional de Ciencia, Tecnología e Innovación 2022–2031.

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

3. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DIGITAL

La implementación del Modelo de Seguridad Digital en el Instituto Universitario de la Paz – UNIPAZ se desarrollará mediante un enfoque progresivo, basado en riesgos y orientado a resultados, considerando el nivel actual de madurez institucional identificado en el PETI 2026 y en el Plan de Gestión y Tratamiento de Riesgos de Seguridad Digital 2026.
La metodología integra de manera armónica:

- El Modelo de Seguridad y Privacidad de la Información – MSPI
- El ciclo PHVA (Planear, Hacer, Verificar y Actuar)
- Las tres líneas de defensa del MIPG
- La planeación estratégica institucional (PETI y Plan de Desarrollo)

Este enfoque permite implementar la seguridad digital como un habilitador transversal, articulado a los procesos misionales, académicos y administrativos, y no como un componente aislado o meramente tecnológico.

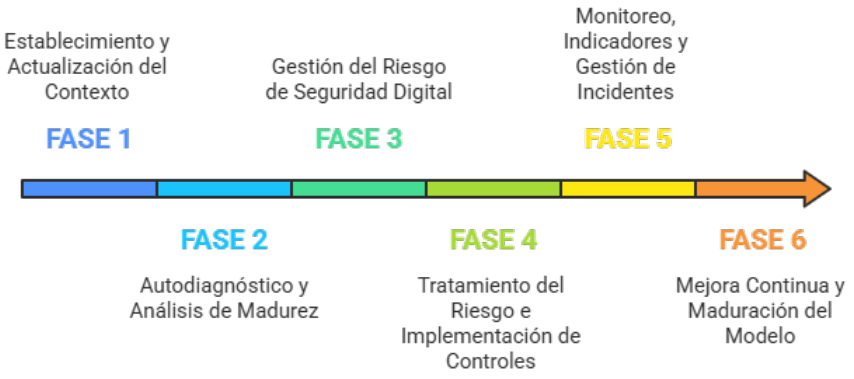

Diagrama de la metodología de implementación
Fuente: Elaboración propia

3.1. Supuesto de implementación

La implementación del Modelo se fundamenta en una comprensión realista de las condiciones actuales de la institución, reconociendo tanto sus capacidades existentes como las limitaciones operativas, técnicas y organizacionales. Estos supuestos orientan el alcance, la priorización de actividades y el ritmo de ejecución de la metodología, garantizando su viabilidad y sostenibilidad durante la vigencia 2026.

3.1.1. Nivel de madurez intermedio-bajo en seguridad digital

UNIPAZ presenta un nivel de madurez intermedio–bajo en la gestión de la seguridad digital, caracterizado por la existencia de prácticas operativas y controles básicos implementados de manera parcial, pero con brechas en su formalización, estandarización y medición. Si bien la institución cuenta con infraestructura tecnológica y mecanismos operativos que permiten la

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

prestación continua de servicios, aún se requiere fortalecer la adopción sistemática del Modelo de Seguridad y Privacidad de la Información – MSPI, especialmente en aspectos relacionados con la gobernanza, la gestión integral del riesgo, la documentación de procesos y la medición del desempeño.

Este nivel de madurez implica que la metodología priorice el fortalecimiento de los fundamentos del modelo (políticas, roles, inventarios, riesgos y controles básicos), evitando enfoques de alta complejidad que no se ajusten a la capacidad institucional actual.

3.1.2. Función de las TIC con enfoque asesor y articulador

La función de Tecnologías de la Información y las Comunicaciones en UNIPAZ se encuentra concentrada principalmente en un rol asesor y articulador, responsable de orientar, coordinar y acompañar a los procesos institucionales en el uso seguro de las tecnologías, más que en una estructura robusta de operación especializada en seguridad digital.
En este contexto, la metodología reconoce que la implementación del Modelo de Seguridad Digital no puede recaer exclusivamente en el área de TI, sino que debe desarrollarse de manera transversal, involucrando activamente a los líderes de proceso, dependencias misionales, administrativas y de apoyo, en coherencia con las tres líneas de defensa del MIPG. Por tanto, se prioriza un modelo de corresponsabilidad institucional, donde la seguridad digital se integre en la gestión diaria de los procesos y no se limite a un enfoque tecnológico.

3.1.3. Infraestructura tecnológica funcional con brechas en continuidad y formalización

UNIPAZ dispone de una infraestructura tecnológica funcional que soporta los procesos académicos, administrativos y de gestión institucional; sin embargo, se identifican brechas en la formalización de controles asociados a la continuidad de los servicios, la gestión de respaldos, la recuperación ante incidentes, la documentación de procedimientos y la estandarización de prácticas de seguridad.
Este supuesto implica que la metodología se enfoque en fortalecer progresivamente los mecanismos de continuidad operativa, respaldo de información y respuesta ante incidentes, priorizando soluciones prácticas y sostenibles que puedan ser implementadas con los recursos disponibles, antes de adoptar esquemas avanzados o altamente especializados.

3.1.4. Priorización de controles críticos y de alto impacto

Dadas las limitaciones de recursos humanos, técnicos y financieros, la implementación del Modelo de Seguridad Digital en UNIPAZ se basa en la priorización de controles críticos y de alto impacto, definidos a partir de la gestión de riesgos de seguridad digital y del apetito de riesgo institucional.
La metodología asume que no todos los controles del MSPI o de los estándares internacionales pueden ser implementados de manera simultánea; por ello, se priorizan aquellos controles que

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

contribuyen directamente a mitigar riesgos críticos y altos, proteger activos de información esenciales, garantizar la continuidad de los servicios y cumplir con los requisitos normativos obligatorios.
Esta priorización permite optimizar los recursos disponibles y generar resultados visibles y medibles durante la vigencia 2026.

3.1.5. Implementación gradual y mejora progresiva durante la vigencia 2026

La implementación del Modelo de Seguridad Digital en UNIPAZ se concibe como un proceso gradual y evolutivo, alineado con el ciclo PHVA y los instrumentos de planeación institucional. Durante la vigencia 2026, la metodología se orienta a consolidar las bases del modelo, cerrar brechas prioritarias y fortalecer la cultura organizacional en seguridad digital.
Este enfoque reconoce que la madurez en seguridad digital se alcanza de manera progresiva y sostenida en el tiempo, por lo cual la metodología establece mecanismos de seguimiento, evaluación y ajuste continuo, que permiten incorporar lecciones aprendidas, mejorar los controles existentes y preparar a la institución para niveles superiores de madurez en vigencias posteriores.

3.2. Principios rectores

Los principios rectores orientan la toma de decisiones, la priorización de actividades, la asignación de recursos y la evaluación de resultados. Estos principios garantizan que la gestión de la seguridad digital se desarrolle de manera coherente con la realidad institucional, los lineamientos normativos vigentes y los objetivos estratégicos definidos para la vigencia 2026.

3.2.1. Gestión basada en riesgos *(plan de gestión y tratamiento de riesgos 2026)*

La gestión de la seguridad digital en UNIPAZ se orienta por un enfoque basado en riesgos, mediante el cual se identifican, analizan, evalúan y priorizan los riesgos que afectan a los activos de información, los servicios digitales y los procesos institucionales. Este principio permite focalizar los esfuerzos de seguridad en aquellos riesgos que representan un mayor impacto para la confidencialidad, integridad, disponibilidad y privacidad de la información.
En coherencia con el Plan de Gestión y Tratamiento de Riesgos de Seguridad Digital 2026, las decisiones relacionadas con la implementación de controles, la asignación de recursos y la definición de planes de acción se fundamentan en la criticidad de los riesgos identificados y en el apetito de riesgo institucional, evitando la adopción de medidas genéricas o desalineadas con el contexto real de UNIPAZ.

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

3.2.2. Proporcionalidad y viabilidad *(PETI Unipaz 2026)*

La implementación del Modelo se rige por el principio de proporcionalidad y viabilidad, garantizando que las acciones, controles y mecanismos adoptados sean coherentes con la capacidad operativa, técnica, financiera y organizacional de UNIPAZ.
Este principio reconoce que la institución no requiere ni está obligada a implementar controles de alta complejidad tecnológica cuando estos no resultan viables o necesarios para su contexto. En consecuencia, la metodología prioriza soluciones prácticas, sostenibles y ajustadas a la infraestructura existente, conforme a los lineamientos definidos en el PETI UNIPAZ 2026, permitiendo avanzar de manera gradual en la madurez del modelo sin comprometer la continuidad de los servicios ni la gestión institucional.

3.2.3. Integración institucional *(MIPG)*

La seguridad digital en UNIPAZ se concibe como un componente transversal de la gestión institucional, integrado de manera armónica a los procesos estratégicos, misionales, de apoyo y de evaluación. Este principio asegura que el Modelo de Seguridad Digital no opere de forma aislada, sino que se articule con los sistemas de planeación, control interno, gestión del riesgo, evaluación del desempeño y mejora continua definidos en el MIPG.
En este sentido, la metodología promueve la alineación de la seguridad digital con el Plan de Desarrollo Institucional, el PETI, el Plan de Acción anual, el FURAG y los mecanismos de seguimiento y control, fortaleciendo la coherencia institucional y evitando la duplicidad de esfuerzos.

3.2.4. Responsabilidad compartida *(Líneas de defensa MIPG)*

El modelo se fundamenta en el principio de responsabilidad compartida, según el cual la protección de la información y la gestión de los riesgos digitales no es exclusiva del área de Tecnologías de la Información, sino un compromiso de toda la institución.
Este principio se materializa a través de las tres líneas de defensa del MIPG:

- Primera línea: líderes de proceso y dependencias, responsables de la gestión cotidiana de los riesgos y la aplicación de controles en sus actividades.
- Segunda línea: Asesor TIC y Comité CIGDAC, encargados de orientar, monitorear y consolidar la gestión de la seguridad digital.
- Tercera línea: Oficina de Evaluación y Control de la Gestión, responsable de la evaluación independiente y el aseguramiento del modelo.

La aplicación de este principio fortalece la corresponsabilidad institucional y contribuye a la construcción de una cultura organizacional orientada a la seguridad digital.

3.2.5. Mejora continua (PHVA)

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

Este principio garantiza que la seguridad digital sea un proceso dinámico, sujeto a evaluación permanente y ajustes progresivos conforme evolucionan los riesgos, las tecnologías y el contexto institucional.
A través del PHVA, UNIPAZ asegura la revisión periódica del contexto de riesgos, la evaluación de la efectividad de los controles implementados, la incorporación de lecciones aprendidas derivadas de incidentes y auditorías, y la definición de acciones de mejora que fortalezcan la sostenibilidad y madurez del Modelo de Seguridad Digital en el tiempo.

3.3. Desarrollo de la metodología

3.3.1. FASE 1: Establecimiento y actualización del contexto

Objetivo
Actualizar el contexto institucional, tecnológico y normativo de la seguridad digital, conforme al PETI 2026 y al Plan de Tratamiento de Riesgos.
Actividades:
Definir el alcance del Modelo de Seguridad Digital (procesos estratégicos, misionales, de apoyo y evaluación).

- Actualizar el inventario de activos de información (alineado con Gestión de la Información – PETI).
- Identificar activos críticos TI/TO y servicios digitales institucionales.
- Analizar el contexto organizacional:
  - Estructura de TI
  - Capacidades humanas y técnicas
  - Dependencias críticas
- Analizar el contexto normativo vigente (Gobierno Digital, MSPI, Decreto 338 de 2022).

Responsables:
Asesor TIC – Seguridad Digital
Líderes de Proceso
Productos:
Contexto de seguridad digital actualizado
Inventario de activos de información

3.3.2. FASE 2: Autodiagnóstico y análisis de madurez

Objetivo:
Determinar el estado real de implementación del Modelo de Seguridad Digital en UNIPAZ.
Actividades:

- Aplicar el autodiagnóstico MSPI – MinTIC.
- Revisar resultados FURAG relacionados con:
  - Seguridad digital

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

  - Gobierno Digital
  - Control Interno
- Identificar brechas frente a:
  - Gobernanza
  - Gestión del riesgo
  - Controles
  - Gestión de incidentes
  - Continuidad del servicio
- Priorizar brechas según impacto institucional y capacidad de cierre en 2026.

Responsables:
Asesor TIC
Comité CIGDAC
Oficina de Evaluación y Control de la Gestión
Productos:
Informe de madurez en seguridad digital
Matriz de brechas priorizadas

3.3.3. FASE 3: Gestión del riesgo de seguridad digital

Objetivo:
Identificar, analizar y priorizar los riesgos de seguridad digital, conforme al Plan de Tratamiento de Riesgos 2026.
Actividades:

- Identificación de riesgos por proceso y activo.
- Identificación de amenazas y vulnerabilidades técnicas, humanas y organizacionales.
- Análisis de impacto:
  - Operativo
  - Legal
  - Reputacional
  - Académico
- Valoración del riesgo inherente y residual.
- Elaboración de mapas de calor.
- Priorización de riesgos críticos y altos para tratamiento.

Responsables:
Asesor TIC
Líderes de Proceso
Productos:
Matriz de riesgos de seguridad digital

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

Mapas de calor
Riesgos priorizados

3.3.4. FASE 4: Tratamiento del riesgos e implementación de controles

Objetivo:
Implementar controles de seguridad digital alineados con MSPI, priorizados por riesgo y viabilidad institucional.
Actividades:

- Definir el Plan de Tratamiento de Riesgos (alineado con el plan 2026).
- Seleccionar controles técnicos, administrativos y organizacionales (ISO 27002 / MSPI).
- Implementar controles prioritarios:
  - Políticas y lineamientos de seguridad
  - Gestión de accesos
  - Copias de seguridad
  - Protección de infraestructura
  - Gestión documental segura
  - Seguridad en trabajo remoto
- Formalizar controles mediante actos administrativos cuando aplique.
- Sensibilización básica a usuarios clave.

Responsables:
Asesor TIC
Secretaría General
Productos:
Plan de Tratamiento ejecutado
Controles implementados
Políticas y procedimientos formalizados

3.3.5. FASE 5: Monitoreo, indicadores y gestión de incidentes

Objetivo:
Evaluar la efectividad del Modelo de Seguridad Digital y gestionar incidentes.
Actividades:

- Definir e implementar indicadores de seguridad digital (Plan 2026).
- Seguimiento al avance del Plan de Tratamiento.
- Registro, gestión y análisis de incidentes de seguridad digital.
- Reportes periódicos a:
  - Alta Dirección
  - Comité CIGDAC

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

- Oficina de Evaluación y Control de la Gestión

Responsables:
Asesor TIC
Comité CIGDAC
Productos:
Indicadores de desempeño
Registro de incidentes
Informes de seguimiento

3.3.6. FASE 6: Mejora continua y maduración del modelo

Objetivo:
Asegurar la sostenibilidad y mejora progresiva del Modelo de Seguridad Digital.
Actividades:

- Reevaluación periódica de riesgos.
- Ajuste de controles y planes de tratamiento.
- Incorporación de lecciones aprendidas.
- Actualización anual del Plan de Seguridad Digital.
- Articulación con la planeación institucional siguiente.

Responsables:
Asesor TIC
Oficina de Planeación
Oficina de Evaluación y Control de la Gestión
Productos:
Planes de mejora
Modelo de Seguridad Digital actualizado

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias
Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia

4. HOJA DE RUTA

Fase	Actividad detallada	Responsable	Evidencia	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Fase 1 - Contexto	Definir alcance del Modelo de Seguridad Digital	Asesor TIC / Planeación	Documento de alcance	●	●										
	Actualizar inventario de activos de información	Asesor TIC / Líderes	Inventario actualizado	●	●										
	Identificar activos críticos TI/TO	Asesor TIC	Listado de activos críticos		●										
	Análisis del contexto organizacional	Asesor TIC / Planeación	Informe de contexto		●										
	Análisis normativo vigente	Asesor TIC / Jurídica	Matriz normativa		●										
Fase 2 - Diagnóstico	Aplicar autodiagnóstico MSPI	Asesor TIC	Resultados MSPI			●									
	Revisión resultados FURAG	Asesor TIC / Control Interno	Informe FURAG			●									
	Identificación de brechas	Asesor TIC / CIGDAC	Matriz de brechas			●									
	Priorización de brechas 2026	CIGDAC / Planeación	Brechas priorizadas			●									
Fase 3 - Riesgos	Identificar riesgos por proceso	Asesor TIC / Líderes	Matriz de riesgos				●	●							
	Identificar amenazas y vulnerabilidades	Asesor TIC	Listado amenazas				●	●							
	Análisis de impacto	Asesor TIC	Análisis de impacto					●	●						
	Valoración riesgo inherente y residual	Asesor TIC	Riesgos valorados					●	●						
	Mapas de calor	Asesor TIC	Mapas de calor					●	●						
	Priorización riesgos críticos	CIGDAC	Listado priorizado					●	●						
Fase 4 - Tratamiento	Definir Plan de Tratamiento de Riesgos	Asesor TIC	Plan aprobado						●						
	Seleccionar controles MSPI / ISO 27002	Asesor TIC	Matriz controles						●	●					
	Formalizar políticas de seguridad	Asesor TIC / Jurídica	Actos administrativos							●	●				
	Implementar controles técnicos	Asesor TIC	Evidencias técnicas							●	●	●	●		
	Gestión copias de seguridad y continuidad	Asesor TIC	Pruebas de backup							●	●	●	●		
	Sensibilización usuarios clave	Asesor TIC	Registros capacitación							●	●	●			
Fase 5 - Monitoreo	Definir indicadores seguridad digital	Asesor TIC	Indicadores										●		
	Seguimiento Plan de Tratamiento	Asesor TIC	Informe avance										●	●	
	Registro y análisis de incidentes	Asesor TIC	Registro incidentes										●	●	
	Reportes a Dirección y CIGDAC	Asesor TIC	Actas e informes										●	●	
Fase 6 - Mejora	Reevaluación de riesgos	Asesor TIC	Matriz actualizada												●
	Planes de mejora	Planeación / Control Interno	Planes definidos												●
	Actualización Plan Seguridad Digital	Planeación	Plan 2027												●

atencionalciudadano@unipaz.edu.co
Página Web: www.unipaz.edu.co
Teléfono: PBX (607) 611 8210
Redes: @unipaznoticias

Decreto Ordenanzal 0331 de 1987 Gobernación de Santander
Cod. SNIES 2207 Vigilada Min Educación NIT. 800-024-581-3
Centro de Invest. Santa Lucía, km 14 vía Bucaramanga
Barrancabermeja, Santander, Colombia