2026

UNIPAZ®
Instituto Universitario de la Paz

Plan de tratamiento de riesgos 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

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

En el marco del fortalecimiento institucional y dando continuidad a las acciones desarrolladas en la vigencia 2025, el Instituto Universitario de la Paz – UNIPAZ establece para la vigencia 2026 el presente Plan de Gestión y Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información, orientado a consolidar una gestión integral, sistemática y sostenible de los riesgos asociados a los activos de información de la entidad.

La gestión de los riesgos de seguridad digital constituye un componente fundamental para garantizar la continuidad, confiabilidad y calidad de los servicios académicos, administrativos y tecnológicos que presta UNIPAZ, en un contexto caracterizado por el aumento del uso de plataformas digitales, la interconexión de sistemas de información, el manejo de datos personales y académicos, y la creciente exposición a amenazas cibernéticas. En este sentido, la institución reconoce la necesidad de fortalecer sus capacidades de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.

Este plan se formula de conformidad con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la Secretaría de Transparencia de la Presidencia de la República, y en articulación con el Modelo Integrado de Planeación y Gestión – MIPG, especialmente en su Dimensión 7 – Control Interno, así como con el Modelo de Seguridad y Privacidad de la Información – MSPI. De igual forma, se fundamenta en buenas prácticas y estándares internacionales tales como la NTC ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27701 e ISO 22301, y en la normatividad vigente aplicable, entre la que se destacan el Decreto 1008 de 2018, la Resolución 500 de 2021, la Resolución 746 de 2022 y la Resolución 1519 de 2022, relacionadas con Gobierno Digital, seguridad digital, acceso a la información pública y protección de datos.

Para la vigencia 2026, UNIPAZ orienta su gestión hacia la actualización del contexto de riesgos, la re-identificación y reevaluación de los riesgos de seguridad digital, el fortalecimiento del tratamiento de los riesgos críticos y altos, la implementación y maduración de controles, así como la medición del desempeño mediante indicadores, todo ello soportado en una hoja de ruta y una matriz de Plan de Acción que permiten realizar seguimiento, monitoreo y evaluación permanente.

El presente Plan inicia con la definición y actualización del contexto institucional y tecnológico, abarcando los procesos estratégicos, misionales, de apoyo y de evaluación, e incorpora los aprendizajes derivados de la gestión de incidentes y auditorías previas. Finalmente, se articula con un Plan de Acción 2026, a través del cual se desarrollarán las actividades de tratamiento, monitoreo, revisión y mejora continua de los riesgos de seguridad digital, contribuyendo al cumplimiento de los objetivos institucionales y a la generación de confianza en el entorno digital 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

1. OBJETIVO GENERAL

Consolidar un marco integral de gestión de riesgos de seguridad digital y privacidad de la información para el Instituto Universitario de la Paz – UNIPAZ, que permita identificar, evaluar, tratar y monitorear de manera sistemática las vulnerabilidades y amenazas asociadas a los activos de información, con el fin de mantener los riesgos en niveles aceptables y garantizar la disponibilidad, integridad, confidencialidad y privacidad de la información, así como la continuidad de los servicios institucionales durante la vigencia 2026.

1.1. Objetivos específicos

- fortalecer la gestión de seguridad digital y privacidad de la información en UNIPAZ, articulándola con los objetivos estratégicos institucionales, el Modelo Integrado de Planeación y Gestión – MIPG y el Modelo de Seguridad y Privacidad de la Información – MSPI.
- Priorizar los riesgos de seguridad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica, considerando el contexto institucional, tecnológico y normativo vigente, así como los riesgos emergentes.
- Actualizar el inventario de activos de información, incluyendo activos críticos, servicios digitales y sistemas de información, asegurando su adecuada protección conforme a su nivel de criticidad.
- Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y normativos en materia de seguridad de la información, seguridad digital, protección de datos personales y acceso a la información pública, establecidos por las disposiciones nacionales y los estándares técnicos aplicables.
- Fortalecer la cultura organizacional en seguridad digital, mediante procesos de sensibilización, capacitación y apropiación dirigidos al personal directivo, administrativo, docente y demás colaboradores, promoviendo buenas prácticas y la corresponsabilidad en la protección de la información.
- Desarrollar estrategias de continuidad de los servicios tecnológicos, que permitan a la institución responder de manera efectiva ante situaciones adversas que puedan afectar la operación, garantizando la disponibilidad de los servicios misionales y de apoyo.

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. ALCANCE

El presente Plan de Gestión y Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información define el alcance de las actividades que desarrollará el Instituto Universitario de la Paz – UNIPAZ durante la vigencia 2026, orientadas a la actualización, consolidación y fortalecimiento de la gestión de los riesgos asociados a los activos de información y a los servicios digitales institucionales.

El Plan comprende la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información, considerando el contexto organizacional, tecnológico y normativo vigente, así como los riesgos emergentes derivados del uso de plataformas tecnológicas, sistemas de información y servicios digitales.

El alcance del Plan cubre los procesos estratégicos, misionales, de apoyo y de evaluación de la institución, e involucra a todas las dependencias, líderes de proceso y colaboradores que intervienen en la gestión, uso, administración y protección de los activos de información de UNIPAZ, conforme a las tres líneas de defensa definidas en el Modelo Integrado de Planeación y Gestión – MIPG.

En el marco del tratamiento de los riesgos identificados, UNIPAZ aplicará las siguientes opciones de tratamiento del riesgo, de acuerdo con los criterios establecidos y el apetito de riesgo institucional:

Aceptar el riesgo:

La institución podrá decidir, previo análisis técnico y aprobación de la instancia correspondiente, no adoptar medidas adicionales cuando el nivel de riesgo se encuentre dentro de los rangos de tolerancia establecidos. Esta opción se aplicará principalmente a riesgos con nivel bajo; no obstante, podrá considerarse para otros niveles cuando no sea viable implementar controles adicionales. La aceptación del riesgo no exime de su seguimiento, monitoreo y revisión periódica.

Reducir el riesgo:

Se implementarán controles técnicos, administrativos y organizacionales, así como planes de mejora, orientados a disminuir la probabilidad y/o el impacto de los riesgos identificados. Estos controles estarán alineados con las buenas prácticas establecidas en la ISO/IEC 27002, el Modelo de Seguridad y Privacidad de la Información – MSPI y los lineamientos de Gobierno Digital, priorizando la reducción de los riesgos críticos y altos.

Evitar el riesgo:

Cuando se determine que un riesgo no es aceptable y no es posible reducirlo a niveles tolerables, la institución podrá optar por eliminar o modificar las actividades, procesos o servicios que dan origen al riesgo, garantizando la protección de la información y la continuidad institucional.

Compartir el riesgo:

UNIPAZ podrá compartir determinados riesgos mediante la tercerización de servicios tecnológicos, la suscripción de acuerdos con terceros o la adquisición de mecanismos de aseguramiento, sin que ello implique la transferencia total de la responsabilidad sobre la gestión del riesgo, la cual continuará siendo 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

El presente alcance permite asegurar que las actividades definidas en el Plan de Acción 2026 se desarrollen de manera coherente, articulada y medible, facilitando el seguimiento por parte de la Alta Dirección, el Comité CIGDAC y la Oficina de Control Interno, y contribuyendo a la mejora continua de la gestión de riesgos de seguridad digital en UNIPAZ.

3. DEFINICIONES Y SIGLAS

Para la adecuada implementación, seguimiento y consolidación de la gestión de riesgos de seguridad digital y privacidad de la información durante la vigencia 2026, el Instituto Universitario de la Paz – UNIPAZ adopta las siguientes definiciones, las cuales se encuentran alineadas con las normas técnicas colombianas, estándares internacionales y lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI.

Activo:
De acuerdo con la ISO/IEC 27000, se refiere a cualquier recurso que tenga valor para la institución en relación con la seguridad de la información, incluyendo información, datos, sistemas de información, infraestructura tecnológica, plataformas digitales, servicios, personas, instalaciones físicas y otros elementos que soportan los procesos institucionales.

Amenaza:
Causa potencial de un incidente no deseado que puede explotar una vulnerabilidad y generar impactos negativos sobre los activos de información, los servicios digitales o la operación institucional.

Análisis del riesgo:
Proceso sistemático mediante el cual se comprende la naturaleza del riesgo y se determina su nivel, a partir del análisis de la probabilidad de ocurrencia y el impacto potencial sobre los objetivos institucionales.

Apetito de riesgo:
Nivel máximo de riesgo que UNIPAZ está dispuesta a aceptar, definido por la Alta Dirección, teniendo en cuenta su contexto institucional, estratégico, normativo y operativo.

Consecuencia:
Resultado o impacto derivado de la materialización de un riesgo, el cual puede afectar el cumplimiento de los objetivos institucionales, la prestación de los servicios, la reputación, el cumplimiento normativo o la continuidad de la operación.

Controles:
Conjunto de políticas, procedimientos, prácticas, medidas técnicas y organizativas implementadas para modificar el riesgo, reduciendo su probabilidad y/o impacto, y mantenerlo dentro de los niveles de tolerancia establecidos. Los controles pueden ser preventivos, detectivos o correctivos.

CSIRT (Computer Security Incident Response Team):
Equipo responsable de coordinar la atención, gestión y respuesta a incidentes de seguridad digital, tanto a nivel institucional como en articulación con instancias externas cuando aplique.

Criterios del riesgo:

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

Términos de referencia frente a los cuales se evalúa la importancia y aceptabilidad de un riesgo, considerando el apetito y la tolerancia al riesgo definidos por la institución.

Evaluación del riesgo:
Proceso mediante el cual se comparan los resultados del análisis del riesgo con los criterios establecidos, con el fin de determinar si el riesgo es aceptable, tolerable o requiere tratamiento adicional.

Identificación del riesgo:
Proceso orientado a reconocer, describir y documentar los riesgos que pueden afectar los activos de información, los servicios digitales y los procesos institucionales.

Impacto:
Consecuencia que puede generar un incidente de seguridad digital sobre la institución, la cual puede manifestarse en términos financieros, operativos, legales, reputacionales o académicos.

Inventario de activos de información:
Relación estructurada y actualizada de todos los activos de información que se encuentran dentro del alcance de la gestión de riesgos de seguridad digital, incluyendo su clasificación, nivel de criticidad, responsable y controles asociados.

Nivel de riesgo:
Magnitud del riesgo expresada como la combinación de la probabilidad de ocurrencia y el impacto de sus consecuencias, utilizada para priorizar el tratamiento de los riesgos.

Perfil de riesgo:
Descripción consolidada del conjunto de riesgos identificados para un proceso, activo o servicio, que permite visualizar su comportamiento y evolución en el tiempo.

Política:
Declaración formal de la Alta Dirección que establece las intenciones, principios y lineamientos generales que orientan la gestión de la seguridad digital y la privacidad de la información en UNIPAZ.

Política de gestión del riesgo:
Declaración mediante la cual la Alta Dirección define su enfoque, compromisos y responsabilidades frente a la gestión de los riesgos institucionales, incluyendo los riesgos de seguridad digital.

Reducción del riesgo:
Acciones orientadas a disminuir la probabilidad de ocurrencia y/o el impacto de un riesgo, mediante la implementación de controles y planes de tratamiento.

Riesgo:
Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre un activo de información, un servicio digital o la operación institucional.

Riesgo residual:
Nivel de riesgo que permanece una vez aplicados los controles y ejecutados los planes de tratamiento definidos por 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

Vulnerabilidad:
Debilidad de un activo, proceso o control que puede ser explotada por una amenaza y dar lugar a un incidente 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

4. MARCO NORMATIVO

El Plan de Gestión y Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información del Instituto Universitario de la Paz – UNIPAZ para la vigencia 2026 se fundamenta en el marco normativo vigente que regula la gestión de riesgos, la seguridad digital, la protección de la información, el acceso a la información pública y la implementación de la Política de Gobierno Digital en las entidades del Estado.

Este marco normativo orienta la definición, implementación, seguimiento y mejora continua de los controles de seguridad digital, en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo de Seguridad y Privacidad de la Información – MSPI, y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, garantizando el cumplimiento de los principios de legalidad, transparencia, responsabilidad y protección de la información institucional.

Las disposiciones normativas que se relacionan a continuación constituyen el soporte legal y técnico para el desarrollo de las actividades definidas en el Plan de Acción 2026, así como para el fortalecimiento de la gobernanza, la gestión del riesgo y la toma de decisiones en materia de seguridad digital en UNIPAZ.

Norma	Fecha	Contexto
Directiva Presidencial 02	24 de febrero de 2022	Lineamientos para garantizar la implementación segura de la Política de Gobierno Digital liderada por MinTIC.
Decreto 338	8 de marzo de 2022	Fortalece la gobernanza de la seguridad digital y crea el Modelo e instancias de Gobernanza de Seguridad Digital.
Resolución 746 de 2022	11 de marzo de 2022	Fortalece el Modelo de Seguridad y Privacidad de la Información y complementa la Resolución 500 de 2021.
Decreto 767 de 2022	16 de mayo de 2022	Actualiza los lineamientos generales de la Política de Gobierno Digital y subroga disposiciones del Decreto 1078 de 2015.
Directiva Presidencial 03	15 de marzo de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Resolución 500 de 2021	10 de marzo de 2021	Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el MSPI.

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

Norma	Fecha	Contexto
CONPES 3995	1 de julio de 2020	Política Nacional de Confianza y Seguridad Digital.
Resolución 1519 de 2020	24 de agosto de 2020	Define estándares de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V5	Diciembre de 2020	Define la metodología oficial para la gestión del riesgo en entidades públicas.
Decreto 612 de 2018	4 de abril de 2018	Establece la integración de los planes institucionales y estratégicos al Plan de Acción.
Decreto 1008 de 2018	14 de junio de 2018	Lineamientos generales de la Política de Gobierno Digital.
Ley 1915 de 2018	12 de julio de 2018	Modifica la Ley 23 de 1982 en materia de derechos de autor y derechos conexos.
Resolución 2140 de 2017	19 de octubre de 2017	Adopta el Modelo Integrado de Planeación y Gestión – MIPG.
CONPES 3854	11 de abril de 2016	Política Nacional de Seguridad Digital.
Decreto 103 de 2015	20 de enero de 2015	Reglamenta parcialmente la Ley 1712 de 2014.
Decreto 1068 de 2015	26 de mayo de 2015	Reglamenta parcialmente la Ley 1581 de 2012 y el Registro Nacional de Bases de Datos.
Ley 1712 de 2014	6 de marzo de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública.
Decreto 886 de 2014	13 de mayo de 2014	Reglamenta el artículo 25 de la Ley 1581 de 2012.
Decreto 1377 de 2013	23 de junio de 2013	Reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581 de 2012	17 de octubre de 2012	Establece disposiciones generales para la 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

Norma	Fecha	Contexto
Ley 1273 de 2009	5 de enero de 2009	Crea el bien jurídico de protección de la información y los datos en el Código Penal.

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

5. IMPLEMENTACIÓN DE LA GESTIÓN DE RIESGOS EN SEGURIDAD DIGITAL

La implementación de la gestión de riesgos de seguridad digital se desarrolla como un proceso continuo, sistemático y articulado, orientado a consolidar los avances logrados en vigencias anteriores y a fortalecer la capacidad institucional para prevenir, detectar, responder y recuperarse frente a incidentes de seguridad digital.
En concordancia con el Modelo de Seguridad y Privacidad de la Información – MSPI, el Modelo Integrado de Planeación y Gestión – MIPG y la norma ISO/IEC 27005, la gestión de riesgos de seguridad digital se implementa bajo un enfoque de mejora continua, integrando las actividades de planeación, ejecución, seguimiento, evaluación y ajuste de los controles definidos.

5.1. Comunicación y consulta del riesgo

La comunicación del riesgo constituye un elemento transversal durante todo el ciclo de gestión de riesgos de seguridad digital. UNIPAZ garantiza que la información relacionada con los riesgos identificados, su nivel, tratamiento y evolución sea comunicada de manera oportuna y adecuada a la Alta Dirección, al Comité Institucional de Gestión, Desempeño y Aseguramiento de la Calidad – CIGDAC, a los líderes de proceso y a las demás partes interesadas.
La comunicación efectiva del riesgo facilita la toma de decisiones, fortalece la gestión de incidentes y promueve la apropiación de la seguridad digital como una responsabilidad compartida al interior de la institución.

5.2. Enfoque de implementación 2026

Para la vigencia 2026, la implementación de la gestión de riesgos de seguridad digital se orienta a:

- La actualización del contexto institucional, tecnológico y normativo.
- La re-identificación y reevaluación de los riesgos de seguridad digital, incorporando los aprendizajes derivados de incidentes y auditorías.
- El fortalecimiento del tratamiento de los riesgos críticos y altos, conforme al apetito de riesgo institucional.
- La maduración de los controles técnicos, administrativos y organizacionales.
- La medición del desempeño mediante indicadores definidos en el Plan de Acción 2026.

5.3. Etapas de la implementación de la gestión del riesgo

La gestión de riesgos de seguridad digital en UNIPAZ se implementa a través de las siguientes etapas:

5.3.1. Establecimiento del contexto:

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

Permite definir el entorno interno y externo de la institución, considerando los procesos, activos de información, servicios digitales, partes interesadas, requisitos normativos y factores tecnológicos que inciden en la seguridad digital.

5.3.2. Identificación de los riesgos:

Se identifican los riesgos asociados a los activos de información y servicios digitales, teniendo en cuenta amenazas, vulnerabilidades y posibles impactos sobre la confidencialidad, integridad, disponibilidad y privacidad de la información.

5.3.3. Análisis y evaluación de los riesgos:

Los riesgos identificados son analizados y evaluados para determinar su nivel, priorización y aceptabilidad, utilizando los criterios definidos por la institución y los lineamientos metodológicos vigentes.

5.3.4. Tratamiento de los riesgos:

Se definen e implementan las opciones de tratamiento del riesgo (aceptar, reducir, evitar o compartir), mediante la aplicación de controles y planes de mejora alineados con el MSPI, la ISO/IEC 27002 y el Plan de Acción 2026.

5.3.5. Aceptación del riesgo:

Los riesgos que se encuentren dentro de los niveles de tolerancia establecidos podrán ser aceptados, previa validación y aprobación de la instancia correspondiente, garantizando su seguimiento y revisión periódica.

5.4. Articulación con el ciclo PHVA y MIPG

La implementación de la gestión de riesgos de seguridad digital se enmarca en el ciclo Planear, Hacer, Verificar y Actuar (PHVA), lo que permite asegurar la mejora continua del proceso y su articulación con las tres líneas de defensa definidas en el MIPG:

- **Primera línea:** Líderes de proceso y dependencias responsables de la gestión diaria de los riesgos.
- **Segunda línea:** Asesor TIC y Comité CIGDAC, encargados de orientar, monitorear y consolidar la gestión del riesgo.
- **Tercera línea:** Oficina de Evaluación y Control de la Gestión, responsable de la evaluación independiente y el aseguramiento.

5.5. Resultados esperados de la implementación 2026

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

Como resultado de la implementación de la gestión de riesgos de seguridad digital durante la vigencia 2026, UNIPAZ espera:

- Disminuir el nivel de los riesgos críticos y altos identificados.
- Fortalecer la capacidad institucional de respuesta ante incidentes de seguridad digital.

- Contar con información actualizada y confiable para la toma de decisiones.
- Consolidar una cultura organizacional orientada a la protección de la información y la continuidad de los servicios.

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

6. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La identificación y valoración de los riesgos de seguridad digital se concibe como un proceso estructurado, periódico y participativo, orientado a consolidar la gestión del riesgo y a fortalecer la toma de decisiones frente a la protección de los activos de información y los servicios digitales institucionales.
Este proceso se desarrolla en concordancia con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 5, el Modelo de Seguridad y Privacidad de la Información – MSPI, la norma ISO/IEC 27005 y el Modelo Integrado de Planeación y Gestión – MIPG, considerando el contexto institucional, tecnológico y normativo vigente, así como los riesgos emergentes y los incidentes de seguridad digital materializados en vigencias anteriores.

6.1. Programación y planeación de la identificación de riesgos

Durante la vigencia 2026 se realizará la planeación de las actividades de identificación y valoración de riesgos, definiendo los procesos, dependencias y activos de información que hacen parte del alcance, así como el cronograma y los responsables de su ejecución, de conformidad con lo establecido en el Plan de Acción 2026.
Esta planeación permitirá priorizar los procesos críticos y asegurar la participación de los líderes de proceso y actores clave en la gestión del riesgo.

6.2. Entrevistas y talleres con los líderes de proceso

Se desarrollarán entrevistas, mesas de trabajo o talleres con los líderes de los procesos estratégicos, misionales, de apoyo y de evaluación, con el fin de:

- Actualizar el contexto de los procesos.
- Identificar activos de información y servicios digitales asociados.
- Reconocer amenazas, vulnerabilidades y posibles impactos.
- Incorporar los aprendizajes derivados de incidentes y auditorías.
- Los resultados de estas actividades serán documentados en la Matriz de Riesgos de Seguridad Digital.

6.3. Identificación y análisis de los riesgos

A partir de la información recopilada, se procederá a la identificación de los riesgos de seguridad digital, considerando como mínimo:

- Las amenazas internas y externas.
- Las vulnerabilidades técnicas, organizacionales y humanas.
- Los impactos potenciales sobre la confidencialidad, integridad, disponibilidad y privacidad de la información.
- Los activos críticos y los servicios digitales institucionales.

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

Cada riesgo será analizado en términos de probabilidad e impacto, de acuerdo con los criterios definidos por la institución.

6.4. Valoración del riesgo inherente y residual

En esta etapa se realizará la valoración del riesgo inherente, identificando el nivel inicial del riesgo antes de la aplicación de controles, y posteriormente la valoración del riesgo residual, considerando la eficacia de los controles existentes o implementados.
La valoración permitirá:

- Determinar la aceptabilidad del riesgo.
- Priorizar los riesgos críticos y altos.
- Definir las opciones de tratamiento más adecuadas.

6.5. Elaboración y análisis de mapas de calor

Los riesgos identificados y valorados serán representados mediante mapas de calor, los cuales permitirán visualizar la distribución y evolución de los riesgos antes y después del tratamiento, facilitando la toma de decisiones por parte de la Alta Dirección y el Comité CIGDAC.
Los mapas de calor se utilizarán como insumo para el seguimiento, monitoreo y evaluación del Plan de Acción 2026.

6.6. Revisión y actualización periódica de los riesgos

La identificación y valoración de riesgos no constituye una actividad aislada, sino un proceso dinámico. Durante la vigencia 2026, los riesgos serán revisados y actualizados cuando se presenten, entre otros, los siguientes eventos:

- Cambios significativos en los procesos o en la estructura organizacional.
- Incorporación de nuevos sistemas de información o servicios digitales.
- Materialización de incidentes de seguridad digital.
- Resultados de auditorías internas o externas.

Esta revisión garantizará que la gestión de riesgos se mantenga alineada con la realidad institucional y contribuya de manera efectiva a la 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

7. METODOLOGÍA

La metodología se fundamenta en un enfoque sistemático, integral y orientado a la mejora continua, que permite identificar, analizar, evaluar, tratar y monitorear los riesgos asociados a los activos de información y a los servicios digitales institucionales.
Esta metodología se encuentra alineada con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 5, el Modelo de Seguridad y Privacidad de la Información – MSPI, la norma ISO/IEC 27005, y el Modelo Integrado de Planeación y Gestión – MIPG, garantizando coherencia entre la planeación, la ejecución y el seguimiento de la gestión del riesgo.

7.1. Enfoque metodológico para la vigencia 2026

Para la vigencia 2026, UNIPAZ orienta su metodología hacia la consolidación del proceso de gestión del riesgo, priorizando:

- La actualización periódica del contexto institucional, tecnológico y normativo.
- La integración de la gestión de riesgos de seguridad digital con la planeación institucional.
- La priorización de los riesgos críticos y altos conforme al apetito de riesgo.
- El uso de indicadores para medir la eficacia y efectividad de los controles implementados.
- La incorporación de los resultados de incidentes y auditorías como insumos para la mejora continua.

7.2. Etapas de la metodología de gestión del riesgo

La metodología adoptada por UNIPAZ se estructura en las siguientes etapas:

7.2.1. Establecimiento del contexto:

Comprende la identificación y análisis del entorno interno y externo de la institución, los procesos, los activos de información, los servicios digitales, las partes interesadas y los requisitos normativos aplicables, como base para una adecuada gestión del riesgo.

7.2.2. Identificación de riesgos:

Se identifican los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información, considerando amenazas, vulnerabilidades y eventos potenciales asociados a los activos y servicios institucionales.

7.2.3. Análisis del riesgo:

Consiste en el análisis de cada riesgo identificado, evaluando la probabilidad de ocurrencia y el impacto potencial, con el fin de determinar su nivel y priorización.

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

7.2.4. Evaluación del riesgo:

Se comparan los resultados del análisis con los criterios de aceptación definidos por la institución, determinando la necesidad de tratamiento, aceptación o priorización de los riesgos.

7.2.5. Tratamiento del riesgo:

Se definen e implementan las opciones de tratamiento del riesgo (aceptar, reducir, evitar o compartir), mediante controles técnicos, administrativos y organizacionales, alineados con la ISO/IEC 27002, el MSPI y el Plan de Acción 2026.

7.2.6. Aceptación del riesgo:

Los riesgos que se encuentren dentro de los niveles de tolerancia establecidos podrán ser aceptados formalmente, garantizando su seguimiento y revisión periódica.

7.2.7. Monitoreo y revisión:

Se realiza el seguimiento continuo de los riesgos, controles e indicadores, verificando su eficacia y efectividad, y ajustando la gestión del riesgo cuando sea necesario.

7.3. Articulación con el ciclo PHVA

La metodología de gestión de riesgos de seguridad digital se desarrolla bajo el ciclo Planear, Hacer, Verificar y Actuar (PHVA), lo que permite:

- Planear: Definir el contexto, identificar riesgos y planear su tratamiento.
- Hacer: Implementar controles y ejecutar el Plan de Acción 2026.
- Verificar: Medir el desempeño mediante indicadores, auditorías y seguimiento.
- Actuar: Implementar acciones de mejora y ajustar la gestión del riesgo.

Este enfoque asegura la mejora continua y la sostenibilidad del proceso.

7.4. Roles y responsabilidades en la aplicación de la metodología

La aplicación de la metodología se articula con las tres líneas de defensa del MIPG, de la siguiente manera:

- Primera línea: Líderes de proceso y dependencias, responsables de identificar y gestionar los riesgos en sus actividades.
- Segunda línea: Asesor TIC y Comité CIGDAC, encargados de orientar, consolidar y monitorear la gestión del riesgo.
- Tercera línea: Oficina de Control y Evaluación de la Gestión, responsable de la evaluación independiente y el aseguramiento del proceso.

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

8. MONITOREO Y REVISIÓN

El Instituto Universitario de la Paz – UNIPAZ realizará el monitoreo y la revisión de la gestión de riesgos de seguridad digital de manera permanente, sistemática y documentada durante la vigencia 2026, con el propósito de verificar la eficacia y efectividad de los planes de tratamiento, los controles implementados y el cumplimiento de las actividades definidas en el Plan de Acción 2026.
Este proceso se desarrollará en el marco de las tres líneas de defensa definidas en el Modelo Integrado de Planeación y Gestión – MIPG, Dimensión 7 – Control Interno, asegurando la articulación entre la gestión operativa, el seguimiento técnico y la evaluación independiente.

8.1. Seguimiento al Plan de Acción y a los planes de tratamiento

UNIPAZ efectuará el seguimiento periódico al Plan de Acción 2026 y a los planes de tratamiento de riesgos de seguridad digital, con el fin de:

- Verificar el avance y cumplimiento de las actividades programadas.
- Evaluar la implementación oportuna de los controles definidos.
- Identificar desviaciones, retrasos o dificultades en la ejecución.
- Definir acciones correctivas y de mejora cuando sea necesario.

El seguimiento se realizará tanto durante la etapa de implementación como al cierre de las actividades, garantizando la trazabilidad entre riesgos, controles, responsables e indicadores.

8.2. Revisión de actividades de control y monitoreo de riesgos

La institución revisará periódicamente las actividades de control con el fin de determinar su vigencia, pertinencia y efectividad, procediendo a su actualización cuando el contexto institucional, tecnológico o normativo así lo requiera.
De igual forma, se realizará el monitoreo continuo de los riesgos de seguridad digital y de los controles tecnológicos, considerando especialmente los riesgos críticos, los activos de información priorizados y los servicios digitales institucionales.

8.3. Reevaluación de riesgos y análisis del riesgo residual

Una vez ejecutados los planes de tratamiento conforme a los tiempos y recursos establecidos, UNIPAZ realizará una nueva valoración de los riesgos de seguridad digital, con el objetivo de:

- Verificar la disminución del nivel de riesgo.
- Analizar el desplazamiento de los riesgos en los mapas de calor.
- Comparar los resultados con el nivel de riesgo residual previamente definido.
- Determinar la necesidad de ajustes adicionales en los controles o planes de tratamiento.

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

La evaluación periódica de los riesgos residuales permitirá validar la efectividad de las medidas implementadas y apoyar la toma de decisiones por parte de la Alta Dirección.

8.4. Registro y gestión de incidentes de seguridad digital

UNIPAZ mantendrá un registro actualizado de los eventos e incidentes de seguridad digital materializados durante la vigencia 2026, el cual permitirá:

- Analizar las causas y consecuencias de los incidentes.
- Identificar deficiencias en los controles existentes.
- Implementar acciones de respuesta, mitigación y recuperación.
- Retroalimentar el proceso de identificación y valoración de riesgos.

Así mismo, los incidentes de seguridad de la información serán reportados a los entes de control, autoridades competentes y demás instancias que correspondan, conforme a la normatividad vigente y a las buenas prácticas en seguridad digital.

8.5. Reporte de la gestión del riesgo

El responsable de la seguridad digital consolidará y presentará reportes periódicos a la Línea Estratégica (Alta Dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas, los cuales incluirán, como mínimo:

- Estado y evolución de los riesgos críticos.
- Matriz actualizada de riesgos de seguridad digital.
- Listado de activos de información críticos TI/TO e Infraestructuras Críticas Cibernéticas – ICC, cuando aplique.
- Avance y resultados de los planes de tratamiento.
- Modificaciones al apetito y tolerancia al riesgo, cuando se presenten.
- Impactos potenciales y estimaciones de impacto económico asociados a los riesgos.

8.6. Reporte a autoridades o entidades especiales

Cuando corresponda, UNIPAZ consolidará la información derivada de la gestión de riesgos de seguridad digital para su reporte a las autoridades o instancias competentes, con el propósito de contribuir a la construcción de un panorama nacional de riesgos de seguridad digital y apoyar la formulación de políticas públicas, la generación de capacidades y la asignación de recursos.
Estos reportes podrán incluir información relacionada con:

- Riesgos, amenazas y vulnerabilidades críticas.
- Tipos de activos afectados por los riesgos críticos.
- Servicios digitales críticos para la institución.
- Estado de ejecución de los planes de tratamiento.

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

- Infraestructuras Críticas Cibernéticas – ICC identificadas, cuando aplique.

El reporte de información no implica la transferencia de la responsabilidad sobre la gestión del riesgo, la cual continúa siendo responsabilidad de UNIPAZ.

8.7. Auditorías internas y externas

La Oficina de Evaluación y Control, en su rol de tercera línea de defensa, realizará evaluaciones independientes y auditorías internas y externas sobre la gestión de riesgos de seguridad digital, de acuerdo con el Plan Anual de Auditoría aprobado por el Comité Institucional.
Los resultados de estas auditorías serán gestionados mediante planes de mejora, los cuales harán parte del proceso de seguimiento y mejora continua.

8.8. Medición del desempeño e indicadores

UNIPAZ utilizará indicadores de desempeño para medir la gestión de los riesgos de seguridad digital, los cuales reflejarán el cumplimiento de los objetivos definidos para la vigencia 2026 y serán evaluados periódicamente por la línea estratégica.

8.8.1. Indicadores de la gestión del riesgo de seguridad digital

La entidad definirá, como mínimo, dos (2) indicadores por proceso, así:

- Indicador de eficacia: mide el grado de cumplimiento de las actividades definidas para la gestión del riesgo de seguridad digital.
- Indicador de efectividad: mide el impacto de los planes de tratamiento en la reducción de los riesgos de seguridad digital, asociados a la confidencialidad, integridad y disponibilidad de la información.

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

9. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

Una vez identificados, analizados y valorados los riesgos de seguridad digital, y definidos los controles y planes de tratamiento correspondientes, el Instituto Universitario de la Paz – UNIPAZ establecerá y aplicará acciones claras, oportunas y coordinadas para la atención de los riesgos que se materialicen durante la vigencia 2026.
Estas acciones se desarrollarán en el marco de las tres líneas de defensa del Modelo Integrado de Planeación y Gestión – MIPG, garantizando una respuesta efectiva que permita mitigar el impacto, restablecer la operación y fortalecer la gestión del riesgo.

9.1. Activación de las líneas de defensa

Ante la materialización de un riesgo de seguridad digital, UNIPAZ activará las siguientes líneas de defensa:

Primera línea de defensa:
Los líderes de proceso y las dependencias responsables deberán ejecutar de manera inmediata las acciones de contención, mitigación y notificación del evento, de acuerdo con los procedimientos establecidos.

Segunda línea de defensa:
El Asesor de Tecnologías de la Información y las Comunicaciones y el Comité CIGDAC coordinarán la gestión del incidente, evaluarán la efectividad de los controles existentes y definirán acciones adicionales de tratamiento, cuando sea necesario.

Tercera línea de defensa:
La Oficina de Evaluación y Control realizará la verificación posterior de la gestión del evento, evaluando la oportunidad y efectividad de las acciones ejecutadas y formulando recomendaciones de mejora.

9.2. Gestión y respuesta ante el riesgo materializado

Cuando un riesgo se materialice, la institución deberá:

- Registrar el evento o incidente de seguridad digital.
- Evaluar el impacto generado sobre los activos de información, los servicios digitales y la operación institucional.
- Activar los controles de respuesta, recuperación y continuidad definidos.
- Adoptar medidas correctivas para reducir la probabilidad de recurrencia.
- Realizar los reportes internos y externos que correspondan, conforme a la normatividad vigente.

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

9.3. Reevaluación del riesgo y fortalecimiento de controles

Una vez gestionado el riesgo materializado, UNIPAZ realizará la reevaluación del riesgo, con el propósito de:

- Determinar la efectividad de los controles implementados.
- Identificar fallas o debilidades en los controles existentes.
- Actualizar la matriz de riesgos y los mapas de calor.
- Definir e implementar controles adicionales o ajustes a los planes de tratamiento.

Esta reevaluación permitirá prevenir la ocurrencia de eventos similares en el futuro y fortalecer de manera continua la gestión de riesgos de seguridad digital.

9.4. Incorporación de lecciones aprendidas y mejora continua

Las lecciones aprendidas derivadas de la materialización de los riesgos serán documentadas e incorporadas como insumo para:

- La actualización del contexto de riesgos.
- El ajuste del apetito y la tolerancia al riesgo.
- El fortalecimiento de los controles y procedimientos.
- La mejora de la capacidad institucional de respuesta ante incidentes.

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

10. MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

UNIPAZ garantizará la mejora continua de la gestión de riesgos de seguridad digital durante la vigencia 2026, como un proceso permanente orientado a fortalecer la eficacia, eficiencia y sostenibilidad de los controles implementados, así como a reducir de manera progresiva los niveles de riesgo asociados a los activos de información y a los servicios digitales institucionales.
En este sentido, cuando se identifiquen hallazgos, falencias, no conformidades o incidentes de seguridad digital, la institución adoptará de manera oportuna las acciones necesarias para mitigar sus impactos, corregir las causas identificadas y prevenir su recurrencia, en coherencia con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG y el Modelo de Seguridad y Privacidad de la Información – MSPI.
Para el fortalecimiento continuo de la gestión de riesgos de seguridad digital, UNIPAZ desarrollará, como mínimo, las siguientes acciones:

- Revisar y evaluar de manera sistemática los hallazgos derivados de auditorías internas, auditorías externas, informes de la Oficina de Control Interno y pronunciamientos de los entes de control.
- Analizar las causas raíz y las consecuencias asociadas a los hallazgos, incidentes o no conformidades identificadas, con el fin de definir acciones correctivas y preventivas efectivas.
- Identificar la posible existencia de hallazgos similares o riesgos recurrentes en otros procesos o activos, con el propósito de implementar acciones transversales que eviten su materialización.
- Ejecutar acciones de revisión continua y seguimiento, orientadas a gestionar oportunamente los riesgos detectados, disminuir su probabilidad de ocurrencia y mitigar su impacto, así como a identificar nuevos riesgos que puedan afectar el desempeño institucional o la prestación de los servicios.
- Actualizar la matriz de riesgos, los planes de tratamiento y los controles, incorporando las lecciones aprendidas y los resultados del monitoreo y la medición del desempeño.

Adicionalmente, UNIPAZ mantendrá un registro documentado y actualizado de los hallazgos, las acciones de tratamiento implementadas, los responsables, los plazos de ejecución y los resultados obtenidos, el cual servirá como insumo para la toma de decisiones, la rendición de cuentas y la mejora continua del sistema de gestión 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

11. PLAN DE COMUNICACIONES

El Plan de Comunicaciones para la gestión de riesgos de seguridad digital del Instituto Universitario de la Paz – UNIPAZ para la vigencia 2026 tiene como propósito garantizar la participación, articulación y apropiación institucional de la gestión del riesgo, promoviendo una comunicación clara, oportuna y efectiva entre todos los actores involucrados.

En el desarrollo de este plan participan todos los procesos institucionales, involucrando a directivos, líderes de proceso, funcionarios, docentes, contratistas y demás colaboradores, quienes contribuyen de manera activa en la identificación, análisis, tratamiento y seguimiento de los riesgos de seguridad digital, de acuerdo con sus roles y responsabilidades.

Cuando se identifique un riesgo de seguridad digital, la institución asegurará el intercambio permanente de información mediante espacios de diálogo y mecanismos de comunicación definidos, que permitan suministrar, compartir y obtener información relevante entre las partes interesadas. Esta información estará relacionada, entre otros aspectos, con:

- La existencia y descripción del riesgo.
- Su naturaleza, causas y posibles consecuencias.
- La probabilidad de ocurrencia y el impacto potencial.
- Los resultados de la evaluación y el nivel de aceptabilidad del riesgo.
- Las opciones de tratamiento definidas y los controles implementados.
- La evolución del riesgo y los resultados del seguimiento.

El Plan de Comunicaciones apoyará además el fortalecimiento de la cultura organizacional en seguridad digital, mediante actividades de sensibilización, divulgación y capacitación, orientadas a generar conciencia sobre la importancia de la protección de la información, la gestión de incidentes y la corresponsabilidad en la gestión del riesgo.

Así mismo, la comunicación efectiva de los riesgos de seguridad digital facilitará la toma de decisiones por parte de la Alta Dirección y los comités institucionales, contribuirá al cumplimiento del Plan de Acción 2026 y servirá como insumo para el monitoreo, la revisión y la mejora continua de la gestión de riesgos en 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

12. HOJA DE RUTA

Objetivo Asociado	Responsable	Indicador	Meta 2026	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Formalizar la planeación de seguridad digital	Comité CIGDAC	% aprobación	100%	•											
Alinear la gestión del riesgo al contexto institucional	Asesor TIC	% actualización	100%	•	•										
Mantener inventario actualizado y clasificado	Asesor TIC / Dependencia	% activos actualizados	100%		•	•	•								
Actualizar la matriz de riesgos 2026	Asesor TIC / Dependencia	% riesgos evaluados	100%			•	•	•							
Reducir riesgos críticos y altos	Asesor TIC	% reducción riesgos críticos	≥30%					•	•	•	•				
Responder oportunamente a incidentes	Asesor TIC	% incidentes gestionados	100%					•	•	•	•	•	•	•	•
Verificar efectividad del modelo	Control Interno	% acciones de mejora ejecutadas	100%									•	•		

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