Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Institución Universitaria Digital de Antioquia

Dirección de Tecnología

2025

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA

Historial de cambios

Versión	Fecha	Descripción del cambio
01	31-01-2023	No aplica para la primera versión
02	26-01-2024	Se adecuaron las metas e indicadores al Plan de Desarrollo 2022-2026. Se actualizaron todos los componentes del plan.
03	05-12-2024	Se actualizaron las metas e indicadores al Plan de Desarrollo 2022-2026. Se actualizaron todos los componentes del plan

Contenido

1. Introducción

La Institución Universitaria Digital de Antioquia presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, en el cual se establece un conjunto de actividades y estrategias para garantizar el uso confiable de la información en un entorno digital e híbrido.

Este plan se fundamenta en un enfoque basado en la gestión de riesgos, con el objetivo de proteger los principios de confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad, reduciendo los riesgos que puedan afectar los activos fundamentales para la operación institucional.

El análisis de riesgos aplicado a los activos de información permite a la IU Digital identificar, evaluar y mitigar de manera eficaz los riesgos relacionados con la pérdida de confidencialidad, integridad y disponibilidad de los datos.

Este enfoque integral asegura que la institución esté mejor preparada para gestionar las amenazas cibernéticas y otros factores externos que puedan comprometer la estabilidad de los procesos institucionales y la protección de la información.

Además, la gestión de riesgos se orienta a fortalecer la confianza de las partes interesadas, demostrando el compromiso de la IU Digital de Antioquia con la protección de la información y la capacidad de respuesta ante los desafíos digitales, asegurando la continuidad operativa y el cumplimiento de los estándares de seguridad en todos los ámbitos institucionales.

2. Objetivos

2.1. Objetivo general

Definir e implementar las actividades necesarias para asegurar la integridad, confidencialidad, disponibilidad y privacidad de la información, mediante una gestión integral de los riesgos relacionados con la seguridad digital y la continuidad operativa, alineadas con los objetivos estratégicos de la Institución Universitaria Digital de Antioquia.

2.2. Objetivos específicos

- Involucrar a la alta dirección en la gestión proactiva, eficiente y oportuna de los riesgos asociados con la seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad operativa, para garantizar el cumplimiento de los objetivos estratégicos de la Institución.
- Identificar, evaluar y gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad operativa de manera integrada con los riesgos institucionales, conforme al Modelo Integrado de Planeación y Gestión (MIPG), promoviendo un enfoque holístico en la gestión de riesgos.
- Monitorear y asegurar la implementación efectiva de los controles y planes de tratamiento definidos, realizando un seguimiento detallado de las evidencias y resultados obtenidos, para garantizar la mejora continua en la gestión de los riesgos.

3. Generalidades

3.1. Contexto estratégico

El presente plan está alineado con los objetivos estratégicos de la Institución Universitaria Digital de Antioquia, contribuyendo al cumplimiento de su misión y visión, y respaldando las iniciativas claves definidas en el Plan Estratégico de tecnologías de la información Institucional (PETI) y el Plan de Seguridad y privacidad de la Información.

Este enfoque asegura que las actividades de gestión de riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad operativa estén directamente relacionadas con los objetivos institucionales.

Articulación con el contexto estratégico - MIPG	
Objetivo Estratégico al que aporta	**Política y marco de gestión**
Fortalecer análisis y divulgación de información relevante para grupos de interés.	• Política de Gobierno Digital • Política de Transparencia, acceso a la información pública y lucha contra la corrupción
Mejorar los procesos administrativos	• Política de Gestión Documental
Generar una cultura de calidad e innovación en todos los niveles de la organización.	• Gestión del conocimiento y la innovación.
Fortalecer el uso de la tecnología	• Política de Seguridad Informática
Optimizar la gestión y desempeño institucional	• MIPG (Modelo Integrado de Planeación y Gestión)

4. Alcance

El presente plan se aplica a todos los procesos de la IU Digital de Antioquia que involucran el almacenamiento, procesamiento, recolección, intercambio, recuperación y consulta de información, tanto en entornos físicos como digitales. Este plan abarca la protección de los activos de información de la Institución, garantizando su seguridad y privacidad, y es fundamental para el desarrollo de la misión institucional, así como para el cumplimiento de los objetivos estratégicos y la mejora continua de los procesos organizacionales.

5. Contexto normativo

La formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información está respaldada por el siguiente marco normativo y legal:

- Ley 527 de 1999: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establece las entidades de certificación y se dictan otras disposiciones".
- Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado 'protección de la información y de los datos', y se preservan integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones".
- CONPES 3854 de 2016: "Política de Seguridad Digital del Estado Colombiano".

- Decreto 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado".
- Dirección de Gestión y Desempeño Institucional, (diciembre de 2020): Guía para la administración del riesgo y el diseño de controles en entidades públicas.
- NTC-ISO/IEC 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- NTC-ISO/IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- NTC-ISO/IEC 27005:2018: Tecnología de la información. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.
- NTC-ISO 31000:2018: Gestión del riesgo. Directrices.
- Ley 2195 de 2022: "Por medio de la cual se modifica la Ley 1581 de 2012 y se dictan otras disposiciones sobre la protección de datos personales".
- Resolución 2420 de 2021: "Por la cual se regula el manejo de la información clasificada y se dictan otras disposiciones".

6. Definiciones

- **Vulnerabilidad:** Es una debilidad o deficiencia inherente a los procesos, tecnologías o administración, que puede ser explotada por una amenaza para comprometer la seguridad de los activos de información.
- **Amenaza:** Es cualquier potencial evento o acción que pueda explotar una

vulnerabilidad y resultar en un incidente de seguridad, causando daño o pérdida a los activos de información, la operación de la institución o su reputación.

- **Riesgo residual:** Es el riesgo que permanece después de haber aplicado medidas de control y mitigación sobre un riesgo identificado. Este riesgo es aceptado en función de la tolerancia al riesgo de la institución.
- **Privacidad:** Es la capacidad de un individuo o entidad para controlar la recolección, el acceso, el uso y la divulgación de su información personal. Implica también el derecho a que se respete la confidencialidad y el tratamiento adecuado de los datos personales.
- **Confidencialidad:** Es la propiedad de la información que garantiza que solo las personas, procesos o sistemas autorizados tengan acceso a la información. Implica protección contra la divulgación no autorizada.
- **Consecuencia:** Son los efectos directos o indirectos que resultan de la materialización de un riesgo. Pueden ser negativos o positivos, y afectan tanto a los procesos de la organización como a los grupos de interés involucrados.
- **Control:** Son las medidas, acciones o procedimientos implementados para mitigar, reducir o eliminar los riesgos identificados, o para cambiar el nivel de riesgo hacia una aceptabilidad predefinida.
- **Disponibilidad:** Es la propiedad de la información que asegura que esta sea accesible y utilizable cuando sea necesario, de manera eficiente y confiable, por las personas y sistemas autorizados.
- **Gestión de riesgos:** Es el proceso de identificar, evaluar, controlar y monitorear los riesgos que afectan la seguridad, privacidad y operación de los activos de información de la organización. Incluye la valoración de los riesgos y la implementación de estrategias de mitigación.
- **Incidente de seguridad de la información:** Cualquier evento que comprometa la confidencialidad, integridad, o disponibilidad de los activos de información, ya sea

por acción maliciosa o por error, que afecte la seguridad de la información.

- **Información:** Conjunto organizado de datos que tienen un significado particular y que pueden ser utilizados para tomar decisiones o generar conocimiento. La información puede ser creada, almacenada, compartida y procesada por los sistemas de la organización.
- **Integridad:** Es la propiedad de la información que asegura que esta es precisa, completa y está protegida contra modificaciones no autorizadas. Garantiza que la información no ha sido alterada o destruida de manera inapropiada.
- **Impacto:** Es el efecto o consecuencia, positivo o negativo, que puede ocurrir si un riesgo se materializa. Se refiere a los resultados directos de un incidente de seguridad ya las implicaciones que tiene para la organización.
- **Nivel de riesgo:** Es la magnitud de un riesgo, que se determina por la combinación de la probabilidad de que un riesgo se materialice y el impacto que tendría si ocurriera. Se expresa en términos de probabilidad y consecuencias.
- **Activo de información:** Cualquier recurso relacionado con la información, como datos, documentos, sistemas informáticos, hardware, software, servicios y personas, que es esencial para la operación de la organización. Los activos de información deben ser protegidos adecuadamente como parte de la gestión de seguridad.
- **Probabilidad:** Es la posibilidad de que un evento no deseado (riesgo) ocurra. Se puede medir en términos de frecuencia, recurrencia o factibilidad, y se utiliza para estimar el nivel de exposición al riesgo.
- **Riesgo:** Es la posibilidad de que un evento no deseado, que afecte los objetivos de la organización o de un proceso, ocurra. El riesgo se evalúa en términos de su probabilidad de ocurrir y el impacto que tendría en la organización.
- **Riesgo Inherente:** Es el nivel de riesgo antes de aplicar controles o medidas de mitigación. Es el riesgo natural asociado a una vulnerabilidad y una amenaza sin

intervención.

- **Riesgo de seguridad y privacidad:** Es el potencial de que una amenaza explote una vulnerabilidad en un activo de información, lo que podría resultar en daño o pérdida a la organización, incluyendo afectaciones a la confidencialidad, integridad, disponibilidad o privacidad de la información. Se mide en términos de probabilidad y consecuencias.

7. Desarrollo del Plan de Seguridad y Privacidad de la Información

La metodología utilizada para la evaluación y gestión de riesgos en los sistemas de gestión de la IU Digital de Antioquia se fundamenta en las mejores prácticas internacionales, específicamente en la NTC-ISO 31000, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP), con especial énfasis en su Anexo 4 - Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. Estos lineamientos se encuentran en total concordancia con las políticas de gestión de riesgos establecidas por la entidad.

El objetivo principal del Plan de gestión de riesgos es proporcionar un marco claro para la identificación, evaluación, tratamiento y monitoreo de los riesgos, que permita a la IU Digital de Antioquia cumplir con sus objetivos institucionales, fortalecer la transparencia y el desempeño de los procesos, y garantizar la mejora continua en la gestión. Este plan se aplica a todos los procesos institucionales, incluyendo tanto riesgos operacionales como aquellos relacionados con la seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad.

Para asegurar la eficacia de este enfoque, la gestión de riesgos se lleva a cabo en colaboración con los líderes de cada proceso, quienes son responsables de los activos de

información. Estos líderes deben garantizar que los custodios de la información implementen y mantengan los controles necesarios para salvar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional.

La identificación y análisis de los riesgos se realiza en un marco de colaboración continua con los responsables de los procesos, quienes deben asegurar que los controles sean adecuados para proteger la información. El proceso de análisis se orienta a identificar los riesgos de manera integral, evaluando la pertinencia de los controles existentes y determinando el tratamiento adecuado para reducir los riesgos a un nivel aceptable. Este proceso sigue el siguiente orden:

1. **Identificación de riesgos:** Se identifican todas las amenazas y vulnerabilidades que pueden afectar los activos de información, incluyendo tanto los riesgos internos como los externos.

2. **Evaluación de riesgos:** Se evalúa la probabilidad de ocurrencia de los riesgos identificados y su impacto potencial sobre los procesos y objetivos institucionales. Esta evaluación también tiene en cuenta la legislación vigente y las mejores prácticas en ciberseguridad y protección de datos.

3. **Determinación de controles:** Se evalúa la efectividad de los controles existentes y se determina las mejoras necesarias. Los controles deben ser específicos, alcanzables y diseñados para mitigar los riesgos a un nivel tolerable según la política de gestión de riesgos de la IU Digital de Antioquia.

4. **Tratamiento de riesgos:** Se implementan acciones para reducir el nivel de los riesgos, ya sea mediante la mitigación, transferencia o aceptación de los mismos. Cada tratamiento debe ser documentado y debe estar alineado con las necesidades operativas y estratégicas de la institución.

5. **Monitoreo y seguimiento:** Se establece un proceso de monitoreo constante para verificar la efectividad de los controles implementados y para hacer ajustes cuando sea necesario. La supervisión debe ser continua y debe involucrar a todas las partes interesadas para garantizar el cumplimiento y la mejora continua.

7.1. Establecimiento de contexto

Para el desarrollo adecuado y gestión del Plan de riesgos de Seguridad y Privacidad de la Información, se establece un contexto del proceso tomando en cuenta los siguientes aspectos esenciales:

1. **Contexto del proceso:** Se identifican y detallan las características fundamentales del proceso, así como sus interrelaciones con otros procesos y actores dentro de la institución. Este análisis permite comprender cómo el proceso se integra y contribuye a los objetivos globales de la IU Digital de Antioquia.

2. **Diseño del proceso:** Se describe claramente el alcance y los objetivos del proceso, asegurando que todas las actividades y tareas estén alineadas con las metas estratégicas de la institución. El diseño debe ser flexible y permitir ajustes conforme a las necesidades emergentes.

3. **Interrelación con otros procesos:** Se identifican las relaciones del proceso con otros procesos dentro de la institución, considerando los insumos, proveedores, productos, usuarios o clientes que influyen o son influenciados por este. Esto asegura que todas las partes estén coordinadas y que la información fluya de manera adecuada entre procesos interdependientes.

4. **Transversalidad:** Se identifican los procesos clave que proporcionan los lineamientos necesarios para el desarrollo y éxito de todos los demás procesos en la entidad. La transversalidad asegura que el proceso de seguridad y privacidad de la información sea compatible y colaborativo con otras áreas, estableciendo un enfoque integral en la organización.

5. **Procedimientos asociados:** Se evalúa la pertinencia y coherencia de los procedimientos asociados que desarrollan cada proceso. Es crucial que estos procedimientos sean apropiados y estén alineados con las políticas de

seguridad, privacidad y eficiencia operativa de la institución.

6. **Responsables del proceso:** Se establece claramente el grado de autoridad y responsabilidad de los funcionarios frente al proceso. Esto incluye la designación de roles específicos para la gestión de riesgos, controles de seguridad y privacidad de la información, asegurando la correcta implementación y supervisión de las actividades.

7. **Comunicación entre los procesos:** Se asegura que existe una comunicación efectiva y eficiente entre los procesos. Los flujos de información deben ser claros y definidos, permitiendo la interacción fluida entre los distintos actores y facilitando la toma de decisiones informadas.

Tipo de proceso: Los procesos se clasifican de acuerdo con su impacto y función en la Institución:

- **Procesos Misionales:** Aquellos directamente relacionados con el cumplimiento de la misión y visión de la Institución, que afectan directamente el propósito central de la Institución.
- **Procesos Estratégicos:** Procesos que contribuyen al logro de los objetivos estratégicos de la Institución.
- **Procesos de Apoyo:** Aquellos que facilitan y respaldan los procesos misionales y estratégicos.
- **Procesos de Evaluación y Control:** Procesos destinados a monitorear, evaluar y garantizar la eficacia de los controles y las políticas implementadas.

7.2. Valoración y análisis del riesgo

El proceso de valoración y análisis del riesgo se enfoca en identificar, analizar y evaluar los riesgos que pueden afectar los activos de información de la IU Digital de Antioquia. Este proceso se lleva a cabo mediante las siguientes actividades:

1. **Identificación de riesgos:** Se identifican todos los riesgos potenciales que podrían impactar los activos de información. Esta identificación se realiza mediante la revisión de procesos, amenazas, vulnerabilidades y situaciones internas y externas que pueden comprometer la seguridad y privacidad de la información.

2. **Causas y vulnerabilidades:** Se analizan las causas fundamentales que pueden dar origen a los riesgos y las vulnerabilidades asociadas a los sistemas, procesos o controles existentes. Esto permite identificar puntos débiles dentro de la infraestructura y los procedimientos que podrían ser explotados.

3. **Amenazas:** Se describen las amenazas potenciales, clasificándolas por tipo (internas, externas, tecnológicas, humanas, etc.), y se evalúa su impacto en caso de que se materialicen.

4. **Consecuencias:** Se determinarán las posibles consecuencias de la materialización de los riesgos, considerando los impactos sobre la confidencialidad, integridad, disponibilidad y privacidad de la información, así como sobre los procesos y objetivos institucionales.

5. **Clasificación del riesgo:** Se clasifica cada riesgo según su probabilidad de ocurrencia y su impacto potencial en los activos de información. Esta clasificación determina la prioridad en la gestión de los riesgos, permitiendo la asignación de recursos de manera eficiente.

El objetivo de esta etapa es obtener una comprensión profunda de los riesgos para poder tomar decisiones informadas en las siguientes fases del tratamiento de riesgos.

7.3. Tratamiento del riesgo

El tratamiento del riesgo implica la selección y aplicación de medidas adecuadas para mitigar, transferir, evitar o aceptar el riesgo, dependiendo de su naturaleza y nivel de impacto. Las acciones incluyen:

7.3.1. Medidas de respuesta ante los riesgos

Se definen las siguientes estrategias de respuesta, según el análisis realizado:

- **Aceptar:** Cuando el riesgo es bajo y no se justifica una acción inmediata.
- **Reducir:** Implementación de controles para reducir la probabilidad o el impacto del riesgo.
- **Compartir:** Transferencia del riesgo mediante mecanismos como seguros o subcontratación.
- **Transferir:** Externalización de la responsabilidad del riesgo a terceros mediante contratos o acuerdos.
- **Evitar:** Eliminación de la causa del riesgo o cambio en los procesos para evitar su materialización.

7.3.2. Acciones de mitigación de riesgos

Para cada riesgo identificado y clasificado, se definen acciones de mitigación detalladas que incluyen:

- **Actividades o tareas específicas:** Acciones concretas que deben llevarse a cabo para gestionar el riesgo.
- **Responsables:** Asignación de responsabilidades a los funcionarios encargados de implementar las medidas de mitigación.
- **Plazo de ejecución:** Establecimiento de plazos claros para la implementación de

cada acción.

- **Seguimiento:** Monitoreo continuo del avance de las medidas y su efectividad para ajustar el tratamiento de los riesgos si es necesario.

El tratamiento de riesgos debe estar alineado con los objetivos estratégicos de la institución y contribuir al fortalecimiento de los controles internos, garantizando la protección de los activos de información.

7.3.3. Comunicación de riesgos

La comunicación de riesgos es un proceso continuo que involucra a todos los niveles de la organización. Se lleva a cabo mediante las siguientes prácticas:

1. **Colaboración y participación:** Todos los procesos de la IU Digital de Antioquia participan activamente en la identificación y tratamiento de los riesgos, con especial énfasis en la colaboración de los responsables de los procesos clave y expertos en áreas específicas.

2. **Levantamiento de mapas de riesgo:** A través de talleres, reuniones y sesiones de trabajo, se elaboran mapas de riesgo detallados acciones que permiten visualizar los riesgos identificados y las implementadas para mitigarlos.

3. **Diálogo y transparencia:** Cuando se identifica un riesgo, la institución proporciona información relevante a todas las partes interesadas (internas y externas) a través de mecanismos de comunicación eficaces. La información incluye la naturaleza, probabilidad, impacto y estrategias de tratamiento del riesgo.

4. **Proceso continuo:** La comunicación de riesgos no se limita a un único evento o momento, sino que debe ser un proceso continuo durante todo el ciclo de vida del riesgo. Esto garantiza que todos los involucrados estén al tanto de los cambios en la evaluación y tratamiento de los riesgos.

7.3.4. Información de riesgos y revisión

La gestión de riesgos es un proceso dinámico que requiere monitoreo, revisión y retroalimentación constante. Para ello, se da cuenta de lo siguiente:

1. **Monitoreo de controles:** Se lleva a cabo un monitoreo continuo para garantizar que los controles implementados sean efectivos tanto en su diseño como en su ejecución. Este monitoreo permite detectar cualquier brecha de seguridad o ineficiencia en los controles existentes.

2. **Obtención de información adicional:** El monitoreo proporciona datos adicionales que son cruciales para ajustar la valoración de los riesgos, identificar nuevos riesgos emergentes o evaluar la efectividad de las medidas implementadas.

3. **Lecciones aprendidas:** A partir de los eventos de riesgo que se materializan, la institución analiza y extrae lecciones aprendidas para mejorar la gestión de riesgos y la implementación de controles en el futuro.

4. **Detección de cambios:** El entorno interno y externo está en constante cambio. Por lo tanto, se debe monitorear cualquier modificación en el contexto institucional, en las amenazas y vulnerabilidades, así como en las prioridades estratégicas que puedan afectar la gestión de riesgos. Estos cambios pueden requerir una revisión de las estrategias de tratamiento y la revalorización de los riesgos.

El objetivo de esta fase es mantener un ciclo de mejora continua en la gestión de riesgos, garantizando que los controles sean siempre adecuados y que la organización esté preparada para adaptarse a nuevos desafíos.

8. Mapa de ruta y seguimiento

La implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se lleva a cabo a través de un conjunto de actividades y esfuerzos alineados

con los objetivos de la organización, con el fin de mitigar los riesgos identificados. Este proceso incluye la definición de indicadores clave que facilitan la medición continua del avance y la efectividad de las acciones implementadas.

El mapa de ruta para el tratamiento de riesgos se organiza a través de actividades específicas medidas por indicadores. Además, se realiza un seguimiento de los resultados alcanzados, comparándolos con los resultados esperados para garantizar que los objetivos del plan se estén cumpliendo de manera eficiente.

Los indicadores de seguimiento permiten evaluar el desempeño de las medidas de mitigación, su impacto en la reducción de riesgos y la efectividad de los controles implementados.

A través de este enfoque, se asegura que todas las actividades relacionadas con la gestión de riesgos sean ejecutadas de manera efectiva, con un enfoque claro en la mejora continua y en la obtención de resultados concretos que contribuyan a la seguridad y privacidad de la información institucional.

#	ACTIVIDAD	META ESTABLECIDA	UNIDAD DE MEDIDA	PRODUCTO O RESULTADO ESPERADO
1	Socialización de la estrategia para el análisis de riesgos, ciberseguridad y seguridad informática.	100%	(Número de actividades realizadas / Número de actividades planificadas) * 100	Evidencias de campañas de sensibilización
2	Actualización de la matriz de riesgos de seguridad y privacidad de la información	1	Unidad	Matriz de riesgos actualizada

3	Publicación de riesgos, ciberseguridad y seguridad informática	1	Unidad	Portal Web Institucional, sección de transparencia
4	Informe de seguimiento y gestión de riesgos, ciberseguridad y seguridad informática	1	Unidad	Informe final de la gestión de riesgos

En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información será objeto de un seguimiento semestral, de acuerdo con los formatos establecidos en el Modelo de Operación por Procesos de la institución, con el fin de garantizar su correcta implementación. evaluación y ajuste conforme a los cambios y necesidades que puedan surgir.

Acción	Nombre	Fecha
Proyectó y Elaboró:	César Alexander Zapata Jiménez	20/01/2025
Revisó:	César Luis Vásquez Suárez Mónica Andrea Santa Escobar	22/01/2025
Revisó y Aprobó:	Jhonatan Arroyave Jaramillo	23/01/2025
Los anteriores, declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por lo tanto, bajo nuestra responsabilidad presentamos para firma.		

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA
DIGITAL DE ANTIOQUIA