

**EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E.**  
**RESOLUCIÓN No. 10.15-115-2025**  
(10 de Diciembre de 2025)

**“POR LA CUAL SE ADOPTA LA ACTUALIZACIÓN DE DOCUMENTOS DEL  
SISTEMA DE GESTIÓN INTEGRADO DE LA EMPRESA DE DESARROLLO Y RENOVACIÓN  
URBANA E.I.C.E. – EDRU E.I.C.E.”**

La Gerente General de la EMPRESA DE DESARROLLO Y RENOVACION URBANA E.I.C.E., en uso de sus facultades legales y estatutarias, establecidas en el Decreto Municipal No. 084 bis del 04 de marzo de 2002, modificado por el Acuerdo 0536 de 2022 y en la Resolución de Junta Directiva No. 20.15.1-001-2024 del 18 de julio de 2024, así como las demás normas que las modifiquen, desarrollen o complementen, y

**CONSIDERANDO**

*Que, el Modelo Integrado de Planeación y Gestión (MIPG), adoptado mediante el Decreto 1499 de 2017, integra en un solo Sistema de Gestión el anterior Sistema de Gestión de la Calidad (Ley 872 de 2003) y el Sistema de Desarrollo Administrativo (Ley 489 de 1998), con el propósito de dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas.*

*Que, el Modelo Integrado de Planeación y Gestión (MIPG) se orienta bajo principios rectores como la Excelencia y Calidad y la Orientación a Resultados, reconociendo que la gestión institucional debe enfocarse en la entrega de bienes y servicios públicos que satisfagan las necesidades y expectativas de los grupos de valor, siendo el Sistema de Gestión de la Calidad la herramienta fundamental para asegurar el mejoramiento continuo en el desarrollo de sus procesos.*

*Que, en artículo 6 del Decreto 1499 de 2017 se dispuso que cada una de las entidades “... integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG, el cual sustituirá los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal. (...)”.*

*Que, mediante la Resolución No. 10.15-029-2018 la Empresa Municipal de Renovación Urbana - EMRU E.I.C. adoptó el Modelo Integrado de Planeación y Gestión MIPG, articulado con el Modelo Estándar de Control Interno – MECI 2014 y creó el Comité Institucional de Gestión y Desempeño, según lo estipulado en el Decreto Nacional 1499 de 2017.*

*Que, en virtud de lo anterior, es deber del Comité Institucional de Gestión y Desempeño de la Empresa de Desarrollo y Renovación Urbana E.I.C.E, en el marco de la implementación y mantenimiento del MIPG, garantizar que el Sistema de Gestión de la Calidad opere de manera efectiva, articulándose con las siete (7) dimensiones y las políticas de gestión y desempeño, para lograr una administración pública más eficiente, transparente y orientada al ciudadano.*

*Que, la Ley 1341 de 2009, o la norma que la modifique o sustituya, establece el marco general y los principios orientadores para el desarrollo del sector de las Tecnologías de la* 

**EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E.**  
**RESOLUCIÓN No. 10.15-115-2025**  
(10 de Diciembre de 2025)

**“POR LA CUAL SE ADOPTA LA ACTUALIZACIÓN DE DOCUMENTOS DEL  
SISTEMA DE GESTIÓN INTEGRADO DE LA EMPRESA DE DESARROLLO Y RENOVACIÓN  
URBANA E.I.C.E. – EDRU E.I.C.E.”**

*Información y las Comunicaciones (TIC) en Colombia, buscando el acceso y servicio universal a las mismas, y promoviendo el uso eficiente de las TIC en la gestión pública.*

*Que, la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones estableció lineamientos y estándares para la implementación de la estrategia de seguridad digital en las entidades públicas, los cuales deben ser tenidos en cuenta en la gestión de riesgos tecnológicos y de protección de datos.*

*Que, el Marco de Gobierno Digital (anteriormente Estrategia de Gobierno en Línea), liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), es la política pública que promueve el uso y aprovechamiento de las tecnologías digitales para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, generando valor público en un entorno de confianza digital.*

*Que, la implementación de la Política de Gestión y Desempeño del MIPG denominada "Gestión de la Información y la Seguridad y Privacidad de la Información" establece la obligatoriedad de que las entidades públicas diseñen, implementen y mantengan planes estratégicos de tecnologías y sistemas de información, alineados con el Modelo de Seguridad y Privacidad de la Información y la arquitectura empresarial de la entidad.*

*Que, de conformidad con el Manual Operativo del MIPG, es responsabilidad de cada entidad expedir los instrumentos necesarios para la planeación, organización, ejecución y seguimiento del componente estratégico de TIC, el cual debe ser coherente con los objetivos misionales, las necesidades de los grupos de valor y las políticas de Gobierno Digital.*

*Que, la adopción y el cumplimiento del Plan Estratégico de las Tecnologías de la Información y las Comunicaciones (PETI) y del Plan de Seguridad y Privacidad de la Información (PSPI), son instrumentos esenciales de planeación que garantizan la adecuada gestión de los activos de información, la infraestructura tecnológica y la provisión de servicios digitales de calidad, contribuyendo a la eficiencia administrativa y a la transparencia.*

*Que, el día cinco (5) de diciembre de 2025 se reunió el Comité Institucional de Gestión y Desempeño de la EDRU E.I.C.E., en el cual se puso a consideración de sus miembros, la actualización de los documentos vigentes de los procesos Direccionamiento y Planeación Institucional, Gestión Administrativa, Documental y TIC., Gestión de Talento Humano y Gestión financiera de la EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E – EDRU E.I.C.E. En dicha sesión se tuvo la aprobación de los mismos.*

*Que, en sesión llevada a cabo el 5 de diciembre de 2025, por el Comité Institucional de Gestión y Desempeño se revisaron y se aprobaron las actualizaciones de los documentos relacionados con los macroprocesos:*

**Estratégico:**

- Proceso Direccionamiento y Planeación Institucional – Subproceso Planeación Institucional. *CTE*

**EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E.**  
**RESOLUCIÓN No. 10.15-115-2025**  
(10 de Diciembre de 2025)

**“POR LA CUAL SE ADOPTA LA ACTUALIZACIÓN DE DOCUMENTOS DEL  
SISTEMA DE GESTIÓN INTEGRADO DE LA EMPRESA DE DESARROLLO Y RENOVACIÓN  
URBANA E.I.C.E. – EDRU E.I.C.E.”**

Apoyo:

- Proceso Gestión de Talento Humano – Subproceso Seguridad y Salud en el Trabajo
- Proceso Gestión Administrativa Documental y TIC – Subproceso Tecnologías de la Información y las Comunicaciones
- Proceso Gestión Financiera.

Que, conforme a lo anteriormente expuesto,

**RESUELVE:**

**ARTÍCULO PRIMERO:** Adoptar la actualización de treinta y cuatro (35) documentos que hacen parte del Sistema de Gestión Integrado, clasificados en los Macroprocesos Estratégico – proceso Direccionamiento y Planeación Institucional – Subproceso Planeación Institucional, Macroproceso de Apoyo – Procesos: Gestión Administrativa, Documental y TIC. – Subproceso Tecnologías de la Información y las Comunicaciones, Proceso Gestión de Talento Humano – Subproceso Seguridad y Salud en el Trabajo y Proceso Gestión Financiera, establecidos en el Mapa de Operación por Procesos de la EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E. – EDRU E.I.C.E., los cuales se relacionan como anexo a la presente resolución denominado ANEXO N° 1.

**ARTÍCULO SEGUNDO:** Será responsabilidad de la oficina de planeación, la dirección administrativa y la dirección financiera la revisión, actualización y socialización de los documentos relacionados con los procesos bajo su responsabilidad, establecidos en el Modelo de Operación por Procesos – MOP de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E y que hacen parte del Sistema de Gestión Integrado.

**ARTÍCULO TERCERO:** CONTINUIDAD DOCUMENTAL. Los manuales, procesos, procedimientos, guías, formatos, caracterizaciones y demás documentos que integran el Sistema de Gestión Integrado (SGI), que no hayan sido objeto de modificaciones o derogatoria expresa en la presente Resolución o en el Anexo 1, mantendrán su vigencia y aplicación obligatoria hasta que se disponga formalmente su actualización o eliminación mediante los canales institucionales establecidos.

**ARTÍCULO CUARTO:** Anexos. Los documentos relacionados en la presente resolución se encuentra contenido en el Anexo 1. El cual hace parte integral de la presente resolución.

La presente Resolución rige a partir de su fecha de expedición y modifica todas las disposiciones que le sean contrarias, expedidas por la Gerencia General de la EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E. - EDRU E.I.C.E.

VTF

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E.  
RESOLUCIÓN No. 10.15-115-2025  
(10 de Diciembre de 2025)

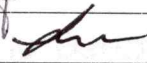
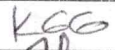
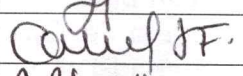
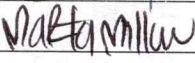
“POR LA CUAL SE ADOPTA LA ACTUALIZACIÓN DE DOCUMENTOS DEL  
SISTEMA DE GESTIÓN INTEGRADO DE LA EMPRESA DE DESARROLLO Y RENOVACIÓN  
URBANA E.I.C.E. – EDRU E.I.C.E.”

COMUNÍQUESE Y CÚMPLASE

Se expide en Santiago de Cali, el diez (10) del mes de Diciembre de 2025.

  
MARIA ALEXANDRA PACHECO MUÑOZ  
Gerente General EDRU E.I.C.E.

Empresa de Desarrollo y Renovación Urbana - EDRU E.I.C.E.

|                                                                                                                                                                                                                  | nombre                          | Cargo / Actividad                                                         | Firma                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Proyectó                                                                                                                                                                                                         | Adriana Millán Azcárate         | Contratista – Oficina de Planeación – Sistema Aseguramiento de la Calidad |  |
| Proyectó                                                                                                                                                                                                         | Julian Gomez Alarcón            | Contratista – Oficina de Planeación                                       |  |
| Revisó                                                                                                                                                                                                           | Karelyn García Gómez            | Contratista – Oficina de Planeación                                       |  |
| Revisó                                                                                                                                                                                                           | Jorge Andrés Martínez Zambrano  | Jefe Oficina de Planeación                                                |  |
| Revisó                                                                                                                                                                                                           | Carolina Soto Flórez            | Jefe Oficina Jurídica                                                     |  |
| Aprobó                                                                                                                                                                                                           | Martha Alexandra Millán Córdoba | Secretaria General                                                        |  |
| Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma. |                                 |                                                                           |                                                                                       |



ANEXO 1: POLÍTICAS DE  
SEGURIDAD Y PRIVACIDAD  
DE LA INFORMACIÓN  
2025

---

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

## TABLA DE CONTENIDO

|                                                                               | Pág. |
|-------------------------------------------------------------------------------|------|
| 1 OBJETIVO.....                                                               | 4    |
| 2 ALCANCE .....                                                               | 4    |
| 3 RESPONSABILIDAD .....                                                       | 5    |
| 4 TERMINOS Y DEFINICIONES .....                                               | 5    |
| 4.1 Clasificación de las Políticas: Institucionales Vs. De Proceso .....      | 6    |
| 5 CONTENIDO .....                                                             | 7    |
| 5.1 POLÍTICAS.....                                                            | 7    |
| 5.1.1 Política de Seguridad de la Información. ....                           | 7    |
| 5.1.2 Política de Clasificación y Manejo de la Información. ....              | 9    |
| 5.1.3 Política de Control de Acceso.....                                      | 11   |
| 5.1.4 Política de Gestión de Incidentes de Seguridad.....                     | 13   |
| 5.1.5 Política de Seguridad Física y Ambiental. ....                          | 14   |
| 5.1.6 Política de Uso Aceptable de Recursos. ....                             | 16   |
| 5.1.7 Política de Protección de Datos Personales. ....                        | 18   |
| 5.1.8 Política de Backup y Recuperación ante Desastres.....                   | 19   |
| 5.1.9 Política de Seguridad en Proveedores y Terceros. ....                   | 22   |
| 5.1.10 Política General de Seguridad y Privacidad de la Información. ....     | 23   |
| 5.1.11 Política de Derecho de Autor y Autorización de Uso de Contenidos. .... | 25   |
| 6 DOCUMENTOS Y REGISTROS.....                                                 | 26   |
| 7 NORMATIVIDAD, DOCUMENTOS Y/O REGISTROS RERERENCIADOS .....                  | 27   |
| 8 Control de cambios .....                                                    | 28   |

|                                                                                                                                                              |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
| <br>Gestión Administrativa,<br>Documental y TIC<br>Dirección Administrativa | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                              |                                                              | Versión:<br>01                               |
|                                                                                                                                                              | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

## INTRODUCCIÓN

Las Políticas de Seguridad y Privacidad de la Información constituyen el marco normativo interno que regula, orienta y armoniza las acciones para la protección de los activos de información de la Empresa de Desarrollo y Renovación Urbana – EDRU E.I.C.E.

Estas políticas establecen los principios, directrices, responsabilidades y normas que deben ser observadas por todos los servidores públicos, contratistas y terceros que accedan, administren o procesen información institucional.

El marco está compuesto por dos niveles complementarios:

- Políticas institucionales, que definen la postura, objetivos y compromisos organizacionales frente a la seguridad y privacidad de la información.
- Políticas de proceso, que desarrollan los procedimientos específicos y acciones técnicas u operativas para dar cumplimiento a los lineamientos institucionales.

El propósito principal de este conjunto normativo es salvaguardar la confidencialidad, integridad y disponibilidad de la información, garantizar la continuidad operativa de la entidad y asegurar el cumplimiento de las disposiciones legales y normativas aplicables, tales como la Ley 1581 de 2012, el Decreto 1377 de 2013, la Ley 1712 de 2014, y los lineamientos de la Política de Gobierno Digital y la ISO/IEC 27001:2022.

En total:

- 7 políticas son institucionales puras, porque definen la posición y compromiso global de la organización.

|                                                                                                                                                              |                                                              |                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------------------------------|
| <br>Gestión Administrativa,<br>Documental y TIC<br>Dirección Administrativa | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br><b>POL-DPI-01-03</b>                                                  |
|                                                                                                                                                              | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Versión:<br><b>01</b><br><br>Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

- 3 son de proceso, porque detallan actividades técnicas y operativas (backup, incidentes, accesos).
- 1 híbrida (institucionales con componentes de proceso), ya que establecen postura general y a la vez procedimientos específicos (proveedores, clasificación).

## 1 OBJETIVO

Establecer los lineamientos que orientan la gestión de la seguridad y privacidad de la información en la EDRU E.I.C.E., con el fin de proteger los activos de información institucional, garantizar su confidencialidad, integridad y disponibilidad, y asegurar el cumplimiento de las disposiciones legales y normativas aplicables.

## 2 ALCANCE

Las Políticas de Seguridad y Privacidad de la Información aplican a todas las áreas, procesos, sistemas, aplicaciones, infraestructuras tecnológicas, servicios en la nube y equipos que conforman el entorno operativo de la EDRU E.I.C.E., así como a todas las personas que accedan, administren, custodien o procesen información de carácter institucional, sin importar su tipo de vinculación.

Estas políticas son de cumplimiento obligatorio para:

- Servidores públicos y contratistas de la EDRU E.I.C.E.
- Proveedores y terceros que presten servicios tecnológicos o manejen información institucional.
- Usuarios internos y externos que interactúan con los sistemas de información de la Entidad.

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

El alcance abarca tanto la información física como digital, incluyendo los activos tecnológicos, las bases de datos institucionales, la infraestructura de red, los sistemas corporativos, los servicios Cloud, los dispositivos móviles y de respaldo, así como los procesos de soporte y administración asociados a la gestión de la información.

Estas políticas son aplicables en todas las etapas del ciclo de vida de la información y su cumplimiento se encuentra bajo la supervisión del Área de Sistemas de la Dirección Administrativa, en coordinación con la Oficina de Planeación y Control Interno.

### 3 RESPONSABILIDAD

Los responsables de la implementación, seguimiento y cumplimiento de las políticas de seguridad y privacidad de la información se encuentran definidos en cada una de las políticas específicas que integran el presente Plan.

La asignación de roles y responsabilidades (responsable, Aprobador, Consultado e Informado – RACI) se consolida en el Anexo 1: Matriz RACI de Seguridad y Privacidad de la Información, la cual forma parte integral de este documento y sirve como instrumento de trazabilidad para las auditorías internas y externas.

### 4 TERMINOS Y DEFINICIONES

Para efectos de esta política, se aplican las definiciones establecidas en el documento Institucional de Seguridad y Privacidad de la Información, el cual recoge los conceptos adoptados de la norma ISO/IEC 27701 y la Política de Gobierno Digital.

|                                                                                   |                                                              |  |                                              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------|--|----------------------------------------------|
|  | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br>POL-DPI-01-03                     |
|                                                                                   |                                                              |  | Versión:<br>01                               |
|                                                                                   | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br>10-dic-2025 |

En caso de no requerirse términos adicionales específicos para esta política, se registrará la expresión “No aplica”.

#### 4.1 Clasificación de las Políticas: Institucionales Vs. De Proceso

| Nombre de la Política                                        | Tipo                                | Descripción / Justificación                                                                        | Responsable                                                                                | Versión |
|--------------------------------------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------|
| Política General de Seguridad y Privacidad de la Información | Institucional                       | Define los principios y compromisos generales en materia de seguridad y privacidad.                | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0     |
| Política de Seguridad de la Información                      | Institucional                       | Establece lineamientos globales para la protección de la información institucional.                | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0     |
| Política de Gestión de Riesgos de Seguridad y Privacidad     | Institucional                       | Define la postura institucional frente al riesgo y su tratamiento.                                 | Jefe oficina de planeación, Comité institucional de gestión y desempeño                    | 1.0     |
| Política de Tratamiento y Protección de Datos Personales     | Institucional                       | Cumple la Ley 1581 de 2012 y regula el manejo de datos personales.                                 | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0     |
| Política de Seguridad Física y Ambiental                     | Institucional con enfoque operativo | Regula medidas físicas y ambientales para protección de activos.                                   | Jefe oficina de planeación, Comité institucional de gestión y desempeño                    | 1.0     |
| Política de Uso Aceptable de Recursos TIC                    | Institucional                       | Establece las normas de comportamiento y uso responsable de los recursos tecnológicos.             | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0     |
| Política de Backup y Recuperación ante Desastres             | De Proceso                          | Detalla las acciones específicas para asegurar la continuidad operativa y respaldo de información. | Jefe oficina de planeación, Comité institucional de gestión y desempeño                    | 1.0     |

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

|                                                                          |                                          |                                                                               |                                                                                            |     |
|--------------------------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----|
| Política de Seguridad en Proveedores y Terceros                          | Institucional con componentes de proceso | Regula las relaciones externas y define controles mínimos de seguridad.       | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0 |
| Política de Gestión de Incidentes de Seguridad de la Información (PGISI) | De Proceso                               | Define el procedimiento para notificación, análisis y respuesta a incidentes. | Jefe oficina de planeación, Comité institucional de gestión y desempeño                    | 1.0 |
| Política de Control de Accesos                                           | De Proceso                               | Regula la gestión de usuarios, contraseñas y accesos físicos o lógicos.       | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0 |
| Política de Derechos de Autor y Autorización de Uso de Contenidos        | Institucional                            | Define la postura organizacional sobre el uso ético y legal de contenidos.    | Líder del proceso, Jefe oficina de planeación, Comité institucional de gestión y desempeño | 1.0 |

## 5 CONTENIDO

### 5.1 POLÍTICAS

Actualizar las políticas del Plan de Seguridad y Privacidad para fortalecer la protección de los activos de información, garantizar el cumplimiento normativo y mejorar la gestión de riesgos.

#### 5.1.1 Política de Seguridad de la Información.

|                     |                                              |
|---------------------|----------------------------------------------|
| Versión             | 1.0                                          |
| Fecha de aprobación | 28-nov-2025                                  |
| Aprobado por        | Comité Institucional de Gestión y Desempeño. |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Responsable              | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                        |
| Propósito                | Establece el compromiso de la empresa con la protección de la información.                                                                                                                                                                                                                                                                                                                                                               |
| Alineación               | ISO/IEC 27001:2022 (Cláusula 5.2)                                                                                                                                                                                                                                                                                                                                                                                                        |
| Incluye                  | Objetivos de seguridad, roles y responsabilidades, principios de confidencialidad, integridad y disponibilidad.                                                                                                                                                                                                                                                                                                                          |
| Objetivo                 | Establecer las directrices generales para proteger los activos de información de la EDRU E.I.C.E frente a amenazas internas y externas, garantizando su confidencialidad, integridad y disponibilidad.                                                                                                                                                                                                                                   |
| Alcance                  | Esta política aplica a los funcionarios de planta, contratistas internos y externos que tengan acceso a la información de la EDRU E.I.C.E, sin importar el medio o ubicación donde se procese o almacene la información.                                                                                                                                                                                                                 |
| Principios Rectores      | 1. Confidencialidad: La información solo debe ser accesible por personas autorizadas.<br>2. Integridad: La información debe mantenerse completa, exacta y sin alteraciones no autorizadas.<br>3. Disponibilidad: La información debe estar disponible cuando se necesite.<br>4. Legalidad: Cumplimiento de las leyes locales (Ley 1581 de 2012), internacionales (GDPR, si aplica), y estándares como ISO/IEC 27001.                     |
| Directrices Generales    | 1. Toda información debe clasificarse según su sensibilidad.<br>2. Se debe implementar control de accesos a la información.<br>3. Todo incidente de seguridad debe ser reportado y gestionado.<br>4. Se deben realizar respaldos periódicos y pruebas de restauración.<br>5. Se debe capacitar continuamente al personal en temas de seguridad.<br>6. Los contratos con terceros deben incluir cláusulas de seguridad de la información. |
| Cumplimiento             | El incumplimiento de esta política puede dar lugar a sanciones disciplinarias, contractuales y/o legales, según lo determine la normativa interna o externa correspondiente.                                                                                                                                                                                                                                                             |
| Revisión y Actualización | Esta política será revisada anualmente o cuando se presenten cambios significativos en la legislación, estructura organizacional o riesgos tecnológicos. Toda modificación deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.                                                                                                                                                                                       |

|     |                 |
|-----|-----------------|
| Rol | Responsabilidad |
|-----|-----------------|

|                                                                                   |                                                              |                                              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                   |                                                              | Versión:<br>01                               |
|                                                                                   | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comité Institucional de Gestión y Desempeño | Aprobar la política, asegurar los recursos necesarios y hacer seguimiento a la implementación del Plan de Seguridad y Privacidad de la Información.                                                                                                                                                                                                                                              |
| Gestión Administrativa, Documental y TIC    | Implementar, monitorear y revisar la aplicación de la política, garantizando la ejecución de controles técnicos, administrativos y organizativos.                                                                                                                                                                                                                                                |
| Oficina de Planeación                       | Administrar el componente de seguimiento a la implementación de los controles definidos, consolidar los informes trimestrales de avance de las políticas institucionales y verificar su articulación con las siete dimensiones del Modelo Integrado de Planeación y Gestión (MIPG). Además, identificar oportunidades de mejora y coordinar las acciones correctivas con las áreas responsables. |
| Personal TIC                                | Aplicar controles técnicos de seguridad, realizar mantenimientos, respaldos y atender incidentes reportados según los procedimientos establecidos.                                                                                                                                                                                                                                               |
| Todos los colaboradores                     | Cumplir con las políticas de seguridad y privacidad de la información, participar en las capacitaciones institucionales y reportar oportunamente los incidentes o vulnerabilidades detectadas.                                                                                                                                                                                                   |

### 5.1.2 Política de Clasificación y Manejo de la Información.

|                     |                                                                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión             | 1.0                                                                                                                                                                                                   |
| Fecha de aprobación | 10-dic-2025                                                                                                                                                                                           |
| Aprobado por        | Comité Institucional de Gestión y Desempeño                                                                                                                                                           |
| Responsable         | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución     |
| Propósito           | Define cómo clasificar y proteger la información según su nivel de sensibilidad.                                                                                                                      |
| Alineación          | ISO/IEC 27001:2022 (Anexo A.8)                                                                                                                                                                        |
| Incluye             | Niveles de clasificación (pública, interna, confidencial, restringida), tratamiento, retención y destrucción.                                                                                         |
| Objetivo            | Establecer directrices claras para clasificar y manejar la información de acuerdo con su nivel de sensibilidad, permitiendo su protección y uso apropiado dentro del ciclo de vida de la información. |
| Alcance             | Aplica a toda la información generada, recibida, procesada, almacenada o transmitida por la entidad, sin importar su formato (físico o digital) o medio.                                              |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                    |                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principios Rectores                | 1. La clasificación es obligatoria para todos los activos de información.<br>2. La información debe manejarse según su nivel de sensibilidad.<br>3. Los cambios en el contexto (organizacional, normativo, operativo) pueden modificar su clasificación.                                                                                     |
| Manejo de la Información por Nivel | 1. Etiquetado: Cada documento físico o digital debe estar rotulado con su nivel.<br>2. Transmisión: La información “Confidencial” y “Restringida” debe enviarse encriptada.<br>3. Almacenamiento: Debe hacerse en medios seguros y/o cifrados.<br>4. Eliminación: Según su nivel, puede requerirse destrucción segura o borrado certificado. |
| Cumplimiento                       | El manejo incorrecto de información clasificada puede acarrear sanciones disciplinarias y legales según la normativa vigente y los contratos firmados.                                                                                                                                                                                       |
| Revisión y Actualización           | Esta política será revisada anualmente o cuando se presenten cambios significativos en la legislación, estructura organizacional o riesgos tecnológicos. Toda modificación deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.                                                                                           |

| Categorías de Clasificación |                                                                           |                                                      |                  |
|-----------------------------|---------------------------------------------------------------------------|------------------------------------------------------|------------------|
| Nivel                       | Descripción                                                               | Ejemplos                                             | Acceso           |
| Pública                     | Puede divulgarse sin autorización previa.                                 | Comunicados externos, publicaciones web              | Libre acceso     |
| Interna                     | Solo para uso dentro de la EDRU E.I.C.E.                                  | Manuales internos, instructivos, boletines internos. | Colaboradores    |
| Confidencial                | Divulgación no autorizada podría causar daño a la EDRU E.I.C.E.           | Estados financieros, contratos, información personal | Autorizados      |
| Restringida                 | Su exposición podría causar daños graves. Acceso extremadamente limitado. | Claves, secretos industriales, estrategia ejecutiva  | Gerencia general |

| Rol                                   | Responsabilidad                                                                                                                                                                                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Todos los colaboradores               | Clasificar correctamente la información que generan o reciben, cumplir con las políticas institucionales de seguridad y privacidad y reportar oportunamente los incidentes o vulnerabilidades detectadas.                                                                       |
| Jefes de Oficina y Directores de Área | Supervisar la aplicación y cumplimiento de la política dentro de su área, garantizar que los colaboradores conozcan y apliquen los lineamientos establecidos, y remitir los reportes de seguimiento a la Oficina de Planeación y a la Gestión Administrativa, Documental y TIC. |

|                                                                                   |                                                              |                                              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                   |                                                              | Versión:<br>01                               |
|                                                                                   | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                          |                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestión Administrativa, Documental y TIC | Capacitar, monitorear y auditar el cumplimiento de la política; coordinar las acciones técnicas y administrativas necesarias para fortalecer la seguridad y privacidad de la información institucional.                                                                                                                                     |
| Oficina de Planeación                    | Consolidar los seguimientos trimestrales de las políticas institucionales de seguridad y privacidad, verificar su cumplimiento frente a las siete dimensiones del Modelo Integrado de Planeación y Gestión (MIPG), e identificar las oportunidades de mejora que deben ser presentadas ante el Comité Institucional de Gestión y Desempeño. |

### 5.1.3 Política de Control de Acceso.

|                         |                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión                 | 1.0                                                                                                                                                                                                                                                                                                                                                                  |
| Fecha de aprobación     | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                          |
| Aprobado por            | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                          |
| Responsable             | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                    |
| Propósito               | Establece reglas para controlar el acceso a los sistemas y datos.                                                                                                                                                                                                                                                                                                    |
| Alineación              | ISO/IEC 27001:2022 (Anexo A.9)                                                                                                                                                                                                                                                                                                                                       |
| Incluye                 | Control basado en roles (RBAC), privilegios mínimos, autenticación multifactor.                                                                                                                                                                                                                                                                                      |
| Objetivo                | Establecer controles adecuados para garantizar que solo las personas autorizadas tengan acceso a los activos de información, en concordancia con sus funciones, responsabilidades y niveles jerárquicos.                                                                                                                                                             |
| Alcance                 | Esta política aplica a todos los usuarios (funcionarios de planta, contratistas internos y externos), recursos informáticos, sistemas de información, redes y aplicaciones gestionadas por la EDRU E.I.C.E.                                                                                                                                                          |
| Principios Rectores     | 1. Mínimo privilegio: Se otorgan solo los accesos estrictamente necesarios.<br>2. Necesidad de saber: Acceso a información sensible sólo para quienes la requieren.<br>3. Segregación de funciones: Se evita que una persona tenga control total sobre procesos críticos.<br>4. Autenticación robusta: Requiere contraseña segura y autenticación multifactor (MFA). |
| Directrices y Controles | 5. Asignación de accesos: Mediante solicitud formal aprobada por el jefe de área.                                                                                                                                                                                                                                                                                    |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | 6. Revisión periódica: Los accesos serán revisados cada 6 meses o al cambiar el rol del usuario.<br>7. Revocación inmediata: Cuando un usuario finaliza su relación laboral o contractual.<br>8. Registro y monitoreo: Toda actividad se debe auditar y registrar.                                                                                                                                                                                                                                                                                                                                            |
| Cumplimiento             | El acceso no autorizado o uso indebido puede ser sancionado conforme al reglamento interno y la ley.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Revisión y Actualización | Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.<br><br>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.<br><br>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación. |

| Tipos de Acceso Controlado |                                       |                                         |
|----------------------------|---------------------------------------|-----------------------------------------|
| Tipo                       | Descripción                           | Ejemplo                                 |
| Físico                     | Acceso a espacios físicos sensibles   | Salas de servidores, oficinas cerradas. |
| Lógico                     | Acceso a sistemas, datos, plataformas | Aplicativos, bases de datos, cloud.     |
| Administrativo             | Accesos con privilegios elevados      | Usuarios root, admin., super usuarios.  |

| Responsabilidades                        |                                                                              |
|------------------------------------------|------------------------------------------------------------------------------|
| Rol                                      | Responsabilidad                                                              |
| Usuario final                            | Proteger sus credenciales y no compartirlas.                                 |
| Gestión Administrativa, Documental y TIC | Gestionar y auditar el acceso físico y lógico.                               |
| Líder de área                            | Solicitar y aprobar accesos pertinentes para su personal.                    |
| Personal TIC                             | Validar cumplimiento de controles, revisar logs y responder ante incidentes. |

|                                                                                                                                                              |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
| <br>Gestión Administrativa,<br>Documental y TIC<br>Dirección Administrativa | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                              |                                                              | Versión:<br>01                               |
|                                                                                                                                                              | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

#### 5.1.4 Política de Gestión de Incidentes de Seguridad.

|                                      |                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión                              | 1.0                                                                                                                                                                                                                                                                                                                                                    |
| Fecha de aprobación                  | 10-dic-2025                                                                                                                                                                                                                                                                                                                                            |
| Aprobado por                         | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                            |
| Responsable                          | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                      |
| Propósito                            | Establece el proceso para detectar, responder y recuperarse ante incidentes de seguridad.                                                                                                                                                                                                                                                              |
| Alineación                           | ISO/IEC 27035:2023, NIST 800-61r2:2025                                                                                                                                                                                                                                                                                                                 |
| Incluye                              | Definición de incidente, canal de reporte, tiempo de respuesta, roles del equipo CSIRT o similar.                                                                                                                                                                                                                                                      |
| Objetivo                             | Establecer un marco que permita identificar, reportar, responder, analizar y aprender de los incidentes de seguridad de la información que puedan afectar la confidencialidad, integridad o disponibilidad de los activos informáticos.                                                                                                                |
| Alcance                              | Aplica a todos los usuarios, sistemas, aplicaciones, infraestructuras tecnológicas, procesos y servicios que estén bajo el control de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E.                                                                                                                                                       |
| Definición de Incidente de Seguridad | Cualquier evento que afecte o tenga el potencial de afectar negativamente los activos de información, tales como:<br><br>1. Pérdida o filtración de información.<br>2. Acceso no autorizado a sistemas.<br>3. Malware, ransomware, phishing u otros ciberataques.<br>4. Fallas de disponibilidad del sistema.<br>5. Vulneraciones de datos personales. |
| Canales de Reporte                   | Correo: mesadeayuda@edru.gov.co.<br>WhatsApp Institucional: +57 317 258 0210.<br>Reporte directo al líder del área.                                                                                                                                                                                                                                    |
| Cumplimiento                         | El no reporte de incidentes, la omisión deliberada de información o la manipulación indebida del proceso, se considera falta grave.                                                                                                                                                                                                                    |

|                                                                                                                                                                    |                                                              |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revisión y Actualización | <p>Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.</p> <p>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.</p> <p>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación.</p> |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| <b>Fases del Proceso de Gestión de Incidentes</b> |                                                                                         |
|---------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Fase</b>                                       | <b>Descripción</b>                                                                      |
| Detección                                         | Identificación temprana del incidente por parte del usuario, monitoreo u otras fuentes. |
| Reporte                                           | Registro inmediato al canal establecido. Ver anexo (Registro y Gestión de Incidentes).  |
| Evaluación                                        | Clasificación del incidente según su impacto, urgencia y criticidad.                    |
| Respuesta                                         | Activación del plan de respuesta. Aislamiento, contención y resolución.                 |
| Documentación                                     | Registro detallado del incidente y acciones tomadas.                                    |
| Lecciones aprendidas                              | Revisión post-mortem para evitar recurrencias.                                          |

| <b>Clasificación de Incidentes</b> |                                                      |                                                    |
|------------------------------------|------------------------------------------------------|----------------------------------------------------|
| <b>Nivel</b>                       | <b>Impacto estimado</b>                              | <b>Ejemplo</b>                                     |
| Crítico                            | Riesgo grave a operaciones, legales o reputacionales | Pérdida de base de datos con información personal. |
| Alto                               | Afectación relevante a procesos o usuarios           | Acceso no autorizado a información sensible.       |
| Medio                              | Incidentes contenibles sin impacto severo            | Infección de malware contenida localmente.         |
| Bajo                               | Afectación menor y sin consecuencias                 | Intento de acceso fallido, falso positivo.         |

### 5.1.5 Política de Seguridad Física y Ambiental.

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión                         | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Fecha de aprobación             | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Aprobado por                    | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Responsable                     | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Propósito                       | Protege la infraestructura física contra accesos no autorizados, desastres y daños ambientales.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Alineación                      | ISO/IEC 27001:2025 (Anexo A.11)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Incluye                         | Control de accesos físicos, cámaras, climatización, UPS, extintores, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Objetivo                        | Establecer las directrices para proteger los activos físicos y tecnológicos de la entidad contra accesos no autorizados, daños, pérdida o interferencia derivada de factores ambientales o humanos.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Alcance                         | Esta política aplica a todas las instalaciones físicas donde se procesen, almacenen o transmitan datos institucionales, incluyendo oficinas, centros de datos, espacios de trabajo remoto y áreas restringidas.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Principios Rectores             | <ol style="list-style-type: none"> <li>Defensa en profundidad: Se aplicarán múltiples capas de protección física.</li> <li>Acceso controlado: Solo personal autorizado podrá ingresar a zonas sensibles.</li> <li>Prevención de incidentes ambientales: Medidas para evitar daños por fuego, agua, temperatura u otros riesgos físicos.</li> <li>Continuidad del negocio: Infraestructura física diseñada para soportar fallos y emergencias.</li> </ol>                                                                                                                                                                                       |
| Controles Físicos y Ambientales | <ol style="list-style-type: none"> <li>Accesos <ul style="list-style-type: none"> <li>Registro de entradas y salidas en zonas críticas.</li> <li>Monitoreo por cámaras de videovigilancia (CCTV)</li> </ul> </li> <li>Seguridad perimetral. <ul style="list-style-type: none"> <li>Puertas reforzadas y señalización en áreas críticas.</li> <li>Supervisión, seguridad o vigilancia por cámaras de Videovigilancia.</li> </ul> </li> <li>Protección ambiental. <ul style="list-style-type: none"> <li>Sistemas de detección y extinción de incendios.</li> <li>Controles de temperatura y humedad en centros de datos.</li> </ul> </li> </ol> |

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <ul style="list-style-type: none"> <li>• Respaldo eléctrico (UPS).</li> <li>• Evacuación señalizada y simulacros periódicos.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cumplimiento             | El incumplimiento de esta política podrá dar lugar a sanciones disciplinarias conforme al reglamento interno de trabajo y los contratos suscritos, incluyendo acciones legales si se identifica negligencia o daño intencionado. El personal debe cumplir con las disposiciones establecidas en esta política, y cualquier excepción deberá ser autorizada por la Dirección Administrativa.                                                                                                                                                                                                                          |
| Revisión y Actualización | <p>Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.</p> <p>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.</p> <p>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación.</p> |

| <b>Zonas de Seguridad</b>                                        |                            |                             |
|------------------------------------------------------------------|----------------------------|-----------------------------|
| <b>Zona</b>                                                      | <b>Requisito de acceso</b> | <b>Medidas aplicadas</b>    |
| Recepción general                                                | Libre con registro         | Cámaras.                    |
| Dirección Administrativa, Dirección Financiera, Oficina Jurídica | Libre                      | Cámaras.                    |
| Centro de datos                                                  | Solo personal autorizado   | CCTV, sensores de incendio. |

| <b>Responsabilidades</b>                  |                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------|
| <b>Rol</b>                                | <b>Funciones</b>                                                                   |
| Gestión Administrativa, Documental y TIC. | Supervisar cumplimiento y revisión periódica.                                      |
| Personal de TIC                           | Controlar accesos y eventos anómalos.<br>Gestión de instalaciones y mantenimiento. |

### 5.1.6 Política de Uso Aceptable de Recursos.

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión                       | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Fecha de aprobación           | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Aprobado por                  | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Responsable                   | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Propósito                     | Establece las condiciones de uso de los activos tecnológicos de la empresa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Alineación                    | ISO/IEC 27001;2022 (A.6.1.1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Incluye                       | Uso permitido de internet, correo electrónico, dispositivos, BYOD, descargas, redes sociales.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Objetivo                      | Establecer las normas de uso adecuado de los recursos tecnológicos e informáticos de la EDRU E.I.C.E para asegurar su correcta utilización, prevenir abusos y proteger la integridad de la información corporativa.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Alcance                       | Aplica a todos los funcionarios de planta, contratistas internos y externos que accedan a los recursos tecnológicos de la EDRU E.I.C.E, incluyendo, pero no limitado a: computadores, redes, sistemas, correo electrónico, aplicaciones, dispositivos móviles, almacenamiento en la nube y cuentas institucionales.                                                                                                                                                                                                                                                                                                                                  |
| Principios Rectores           | <ol style="list-style-type: none"> <li>1. Responsabilidad individual: Cada usuario es responsable del uso que les dé a los recursos asignados.</li> <li>2. Uso corporativo: Los recursos deben utilizarse prioritariamente para fines laborales.</li> <li>3. Privacidad limitada: La organización podrá auditar el uso de los recursos cuando lo considere necesario.</li> <li>4. Cumplimiento legal: El uso debe ajustarse a leyes de propiedad intelectual, protección de datos y seguridad de la información.</li> </ol>                                                                                                                          |
| Lineamientos generales de uso | <ol style="list-style-type: none"> <li>1. Está prohibido el uso de los recursos para actividades ilícitas, ofensivas, discriminatorias o que comprometan la reputación de la organización.</li> <li>2. El acceso a contenidos no relacionados con el trabajo (pornografía, apuestas, redes sociales excesivas, etc.) está restringido.</li> <li>3. No se permite instalar software sin autorización del área de Gestión Administrativa, Documental y TIC.</li> <li>4. Las contraseñas deben mantenerse confidenciales y no compartirse.</li> <li>5. El correo electrónico institucional no debe usarse para fines personales o políticos.</li> </ol> |
| Monitoreo y control           | La entidad se reserva el derecho de auditar, registrar y monitorear el uso de todos los recursos tecnológicos con fines de seguridad, cumplimiento normativo y operatividad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cumplimiento             | El incumplimiento de esta política podrá conllevar sanciones disciplinarias conforme al reglamento interno y a la gravedad de la falta, incluyendo posibles acciones legales cuando corresponda.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Revisión y Actualización | <p>Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.</p> <p>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.</p> <p>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación.</p> |

### 5.1.7 Política de Protección de Datos Personales.

|                     |                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión             | 1.0                                                                                                                                                                                                                                          |
| Fecha de aprobación | 10-dic-2025                                                                                                                                                                                                                                  |
| Aprobado por        | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                  |
| Responsable         | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                            |
| Propósito           | Garantiza el cumplimiento de las leyes de protección de datos personales.                                                                                                                                                                    |
| Alineación          | Ley 1581 de 2012 (Colombia), ISO/IEC 27701:2022                                                                                                                                                                                              |
| Incluye             | Consentimiento, derechos del titular, finalidades del tratamiento, transferencia internacional.                                                                                                                                              |
| Objetivo            | Establecer los lineamientos para el tratamiento, recolección, uso, almacenamiento, transmisión y supresión de datos personales, garantizando los derechos de los titulares y el cumplimiento de la normatividad aplicable.                   |
| Alcance             | Aplica a todos los procesos que involucren tratamiento de datos personales de funcionarios de planta, contratistas internos y externos en medios físicos o digitales, realizados por la EDRU E.I.C.E o por terceros que actúen en su nombre. |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principios Rectores                         | <ol style="list-style-type: none"> <li>1. Legalidad: El tratamiento se realizará conforme a la ley.</li> <li>2. Finalidad: El uso de los datos debe tener un propósito claro, legítimo e informado.</li> <li>3. Libertad: El tratamiento sólo puede realizarse con consentimiento previo del titular.</li> <li>4. Veracidad: La información debe ser veraz y actualizada.</li> <li>5. Transparencia: El titular puede acceder a su información en cualquier momento.</li> <li>6. Seguridad: Los datos deben ser protegidos frente a accesos no autorizados o fraudulentos.</li> <li>7. Confidencialidad: Toda persona que intervenga en el tratamiento debe garantizar reserva.</li> </ol> |
| Derechos de los titulares                   | <ol style="list-style-type: none"> <li>1. Conocer, actualizar y rectificar sus datos.</li> <li>2. Solicitar prueba de autorización para el tratamiento.</li> <li>3. Ser informado sobre el uso que se le ha dado a sus datos.</li> <li>4. Presentar quejas ante la Superintendencia de Industria y Comercio.</li> <li>5. Revocar la autorización y/o solicitar la supresión de los datos.</li> <li>6. Acceder gratuitamente a sus datos.</li> </ol>                                                                                                                                                                                                                                        |
| Obligaciones de la EDRU E.I.C.E.            | <ol style="list-style-type: none"> <li>1. Solicitar autorización previa e informada.</li> <li>2. Informar la finalidad del tratamiento.</li> <li>3. Conservar copia de las autorizaciones.</li> <li>4. Garantizar los derechos de los titulares.</li> <li>5. Adoptar medidas de seguridad técnica, humana y administrativa.</li> <li>6. Notificar incidentes de seguridad que comprometan datos personales.</li> <li>7. Responder a las consultas y reclamos en los términos de ley.</li> </ol>                                                                                                                                                                                            |
| Tratamiento de Datos Sensibles y de Menores | <ol style="list-style-type: none"> <li>1. Solo se tratarán cuando exista autorización explícita y sea estrictamente necesario.</li> <li>2. Se tomarán medidas reforzadas de seguridad y confidencialidad.</li> <li>3. En el caso de menores, se requerirá el consentimiento de los representantes legales.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                      |
| Cumplimiento                                | El incumplimiento de esta política podrá conllevar a sanciones internas, así como responsabilidades administrativas y legales frente a la Superintendencia de Industria y Comercio o entes competentes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Revisión y Actualización                    | Esta política será revisada anualmente o cuando haya cambios regulatorios o tecnológicos que lo requieran. Su actualización será responsabilidad de la Oficina Jurídica, Oficina de Planeación y la Dirección Administrativa, toda modificación deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.                                                                                                                                                                                                                                                                                                                                                                    |

### 5.1.8 Política de Backup y Recuperación ante Desastres.

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión                 | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Fecha de aprobación     | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Aprobado por            | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Responsable             | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                                    |
| Propósito               | Asegura la continuidad del negocio y la disponibilidad de la información.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Alineación              | ISO/IEC 22301:2019, ISO/IEC 27031:2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Incluye                 | Respaldos automáticos, frecuencia, pruebas de restauración, RTO, RPO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Objetivo                | Establecer las directrices para realizar copias de seguridad de la información crítica y definir mecanismos de recuperación que aseguren la disponibilidad, integridad y continuidad de los servicios en caso de desastres, incidentes o fallos graves.                                                                                                                                                                                                                                                                              |
| Alcance                 | Esta política aplica a todos los sistemas de información, bases de datos, archivos, aplicaciones y servicios que procesan o almacenan información esencial para la operación de la EDRU E.I.C.E, sin importar su ubicación (on-premise o en la nube).                                                                                                                                                                                                                                                                                |
| Principios Rectores     | <ol style="list-style-type: none"> <li>1. Disponibilidad garantizada: La información crítica debe poder restaurarse en un tiempo aceptable.</li> <li>2. Redundancia: Copias múltiples almacenadas en ubicaciones separadas.</li> <li>3. Integridad: Verificación periódica de que los respaldos son consistentes y utilizables.</li> <li>4. Confidencialidad: Cifrado de respaldos y control de acceso estricto.</li> <li>5. Automatización: Se priorizará el uso de herramientas automáticas de backup.</li> </ol>                  |
| Procedimientos          | <ol style="list-style-type: none"> <li>1. Identificación de activos críticos: Sistemas, datos y aplicaciones esenciales.</li> <li>2. Definición de políticas de retención: Tiempo durante el cual se conservarán las copias.</li> <li>3. Verificación periódica de respaldos: Validación de consistencia y restauración.</li> <li>4. Almacenamiento externo: Se almacenarán respaldos en nube y sitio alterno físico.</li> <li>5. Plan de recuperación ante desastres (DRP): Manual con pasos para restaurar operaciones.</li> </ol> |
| Pruebas de restauración | Se realizarán pruebas semestrales de recuperación para validar los tiempos de recuperación (RTO) y la pérdida máxima tolerable de datos (RPO), ajustando el plan según los resultados.                                                                                                                                                                                                                                                                                                                                               |
| Cumplimiento            | El incumplimiento de esta política pone en riesgo la continuidad operativa y será evaluado como una falta grave conforme al reglamento interno, pudiendo derivar en sanciones y/o correctivos técnicos.                                                                                                                                                                                                                                                                                                                              |

|                                                                                                                                                                    |                                                              |  |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revisión y Actualización | <p>Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.</p> <p>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.</p> <p>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación.</p> |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Tipos de Backup |                     |                                       |
|-----------------|---------------------|---------------------------------------|
| Tipo            | Frecuencia sugerida | Aplicación                            |
| Completo        | Semanal             | Servidores críticos, bases de datos   |
| Incremental     | Diario              | Archivos en modificación constante    |
| Diferencial     | Cada 2 días         | Sistemas operativos o configuraciones |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión             | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fecha de aprobación | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Aprobado por        | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Responsable         | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                |
| Propósito           | Regula los controles de seguridad exigidos a contratistas externos.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Alineación          | I ISO/IEC 27001:2022 (A.15)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Incluye             | SO/IEC 22301:2019, ISO/IEC 27031:2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Objetivo            | Acuerdos de nivel de servicio (SLA), cláusulas contractuales, controles de acceso a contratistas externos.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Alcance             | Establecer las directrices para garantizar que los contratistas externos que acceden procesan o gestionan información de la organización, cumplan con los requisitos de seguridad de la información y protección de datos.                                                                                                                                                                                                                                                                                       |
| Principios Rectores | <ol style="list-style-type: none"> <li>1. Seguridad por contrato: Todo tercero debe aceptar cláusulas de seguridad como parte de sus obligaciones contractuales.</li> <li>2. Evaluación de riesgos: Se realizará un análisis previo de riesgos asociados al servicio externo.</li> <li>3. Supervisión continua: Se monitorea el cumplimiento de los controles acordados.</li> <li>4. Responsabilidad compartida: La seguridad es un compromiso tanto del contratista externo como de la EDRU E.I.C.E.</li> </ol> |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proceso de gestión de seguridad con contratistas externos. | 1. Evaluación previa del contratista externo: Evaluación de riesgos, cumplimiento legal, prácticas de seguridad, certificaciones (ISO 27001, SOC 2, etc.).<br>2. Formalización contractual: Inclusión de cláusulas de confidencialidad, privacidad, medidas de seguridad y derecho de auditoría.<br>3. Monitoreo y seguimiento: Revisiones periódicas, auditorías de cumplimiento y control sobre los accesos otorgados.<br>4. Gestión de finalización de relación: Plan de reversión de datos, revocación de accesos, destrucción segura de información.                                             |
| Cumplimiento                                               | El incumplimiento de esta política puede implicar sanciones contractuales, rescisión del contrato, o acciones legales si compromete la seguridad o privacidad de la EDRU E.I.C.E o sus clientes.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Revisión y Actualización                                   | Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.<br>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.<br>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación. |

### 5.1.9 Política de Seguridad en Proveedores y Terceros.

|                     |                                                                                                                                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión             | 1.0                                                                                                                                                                                                                              |
| Fecha de aprobación | 10-dic-2025                                                                                                                                                                                                                      |
| Aprobado por        | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                      |
| Responsable         | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                |
| Propósito           | Regula los controles de seguridad exigidos a contratistas externos.                                                                                                                                                              |
| Alineación          | I ISO/IEC 27001:2022 (A.15)                                                                                                                                                                                                      |
| Incluye             | SO/IEC 22301:2019, ISO/IEC 27031:2025                                                                                                                                                                                            |
| Objetivo            | Acuerdos de nivel de servicio (SLA), cláusulas contractuales, controles de acceso a contratistas externos.                                                                                                                       |
| Alcance             | Establecer las directrices para garantizar que los contratistas externos que acceden procesan o gestionan información de la organización, cumplan con los requisitos de seguridad de la información y protección de datos.       |
| Principios Rectores | 5. Seguridad por contrato: Todo tercero debe aceptar cláusulas de seguridad como parte de sus obligaciones contractuales.<br>6. Evaluación de riesgos: Se realizará un análisis previo de riesgos asociados al servicio externo. |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | 7. Supervisión continua: Se monitorea el cumplimiento de los controles acordados.<br>8. Responsabilidad compartida: La seguridad es un compromiso tanto del contratista externo como de la EDRU E.I.C.E.                                                                                                                                                                                                                                                                                                                                                                                              |
| Proceso de gestión de seguridad con contratistas externos. | 5. Evaluación previa del contratista externo: Evaluación de riesgos, cumplimiento legal, prácticas de seguridad, certificaciones (ISO 27001:2022, SOC 2, etc.).<br>6. Formalización contractual: Inclusión de cláusulas de confidencialidad, privacidad, medidas de seguridad y derecho de auditoría.<br>7. Monitoreo y seguimiento: Revisiones periódicas, auditorías de cumplimiento y control sobre los accesos otorgados.<br>8. Gestión de finalización de relación: Plan de reversión de datos, revocación de accesos, destrucción segura de información.                                        |
| Cumplimiento                                               | El incumplimiento de esta política puede implicar sanciones contractuales, rescisión del contrato, o acciones legales si compromete la seguridad o privacidad de la EDRU E.I.C.E o sus clientes.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Revisión y Actualización                                   | Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.<br>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.<br>Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación. |

| Requisitos Mínimos para Terceros |                                                                              |
|----------------------------------|------------------------------------------------------------------------------|
| Requisito                        | Descripción                                                                  |
| Acuerdo de confidencialidad      | Obligatorio antes de comenzar cualquier relación contractual.                |
| Política de seguridad            | El contratista externo debe tener una política documentada.                  |
| Protección de datos              | Cumplimiento de la legislación vigente (Ej. Ley 1581 de 2012 en Colombia).   |
| Control de accesos               | Accesos mínimos, temporales y auditables.                                    |
| Notificación de incidentes       | El contratista externo debe informar cualquier incidente en máximo 24 horas. |

### 5.1.10 Política General de Seguridad y Privacidad de la Información.

|                     |             |
|---------------------|-------------|
| Versión             | 1.0         |
| Fecha de aprobación | 10-dic-2025 |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aprobado por                    | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Responsable                     | Revisado por: líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                                   |
| Propósito                       | Definir los lineamientos generales que guían la protección de la información institucional, buscando preservar su confidencialidad, integridad, disponibilidad y privacidad.                                                                                                                                                                                                                                                                                                                                                        |
| Alineación                      | ISO/IEC 27001, Ley 1581 de 2012, Ley 1712 de 2014, Decreto 1377 de 2013, y lineamientos de Gobierno Digital.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Incluye                         | SO/IEC 22301:2019, ISO/IEC 27031:2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Objetivo                        | Establecer los principios, compromisos y directrices generales que orientan la protección de la información en la EDRU E.I.C.E, asegurando la confidencialidad, integridad, disponibilidad, privacidad y cumplimiento normativo, a través de un enfoque basado en riesgos.                                                                                                                                                                                                                                                          |
| Alcance                         | Esta política aplica a todos los procesos, sistemas, funcionarios de planta, contratistas internos y externos que accedan, procesen o administren información en la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E, incluyendo aquellos ubicados en sedes físicas, entornos virtuales y plataformas en la nube.                                                                                                                                                                                                             |
| Principios Rectores             | <ol style="list-style-type: none"> <li>1. Confidencialidad: La información solo debe ser accesible por personas autorizadas.</li> <li>2. Integridad: Garantizar la precisión, consistencia y completitud de la información.</li> <li>3. Disponibilidad: Asegurar el acceso oportuno a la información por usuarios autorizados.</li> <li>4. Legalidad: Cumplimiento estricto de las normas legales y contractuales.</li> <li>5. Privacidad: Protección efectiva de los datos personales de titulares internos y externos.</li> </ol> |
| Compromiso de la Alta Dirección | <ol style="list-style-type: none"> <li>9. Proteger los activos de información como parte estratégica del negocio.</li> <li>10. Asignar los recursos necesarios para implementar, mantener y mejorar el SGSI.</li> <li>11. Alinear el sistema con normas internacionales como ISO/IEC 27001, ISO/IEC 27701, y las leyes colombianas vigentes (Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, entre otras).</li> <li>12. Establecer mecanismos efectivos de reporte, auditoría, formación y mejora continua.</li> </ol>    |
| Cumplimiento                    | El incumplimiento de esta política podrá acarrear medidas disciplinarias, contractuales o legales según lo estipulado en los reglamentos internos de trabajo, contratos laborales o acuerdos de confidencialidad firmados con la EDRU E.I.C.E.                                                                                                                                                                                                                                                                                      |
| Revisión y Actualización        | Esta política será revisada anualmente o cuando se presenten cambios en los procesos, herramientas tecnológicas, normatividad aplicable o estructura organizacional.<br>Cualquier actualización deberá seguir el mismo proceso formal establecido para su aprobación inicial, incluyendo las etapas de revisión técnica, validación jurídica, aprobación por el Comité Institucional de Gestión y Desempeño y publicación oficial en los medios institucionales autorizados.                                                        |

|                                                                                                                                                                    |                                                              |  |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              |  | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br>10-dic-2025 |

|  |                                                                                                                       |
|--|-----------------------------------------------------------------------------------------------------------------------|
|  | Toda modificación deberá ser documentada en el control de versiones y acompañada de la respectiva acta de aprobación. |
|--|-----------------------------------------------------------------------------------------------------------------------|

### 5.1.11 Política de Derecho de Autor y Autorización de Uso de Contenidos.

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versión             | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Fecha de aprobación | 10-dic-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Aprobado por        | Comité Institucional de Gestión y Desempeño                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Responsable         | Revisado por: Líder del proceso<br>Revisado por: Jefe Oficina de Planeación/ Aseguramiento de la calidad<br>Aprobado por: Comité Institucional de Gestión y Desempeño<br>Adoptado por: resolución                                                                                                                                                                                                                                                                                                                                    |
| Propósito           | Garantizar que todos los contenidos generados, adquiridos o utilizados por la Empresa de desarrollo y Renovación Urbana EDRU E.I.C.E. cumplan con la normativa de propiedad intelectual, derechos de autor y licenciamiento, asegurando el uso legal y autorizado de materiales en entornos físicos y digitales, alineados con los principios de seguridad de la información, Gobierno Digital y las leyes colombianas.                                                                                                              |
| Alineación          | 1. ISO/IEC 27001:2022 – Control de cumplimiento legal.<br>2. ISO/IEC 27701:2022 – Extensión de privacidad de la información.<br>3. Ley 23 de 1982 (Régimen de Derecho de Autor en Colombia).<br>4. Ley 1915 de 2018 (Modernización del Régimen de Derecho de Autor).<br>5. Ley 1581 de 2012 (Protección de datos personales).<br>6. Decreto 620 de 2020 – Política de Gobierno Digital.<br>7. Lineamientos de la Función Pública y MinTIC en materia de gestión de información y contenidos digitales.                               |
| Incluye             | 1. Regulación de los derechos patrimoniales y morales de autor en los contenidos institucionales.<br>2. Definición de licenciamiento y autorización de uso de software, bases de datos y recursos digitales.<br>3. Lineamientos para la publicación de contenidos en portales web, redes sociales y plataformas digitales oficiales.<br>4. Establecimiento de cláusulas contractuales con terceros sobre propiedad intelectual y derechos de uso.<br>5. Procedimientos para la gestión de infracciones o uso indebido de contenidos. |
| Objetivo            | Establecer directrices que regulen la creación, adquisición, distribución, publicación y reutilización de contenidos, obras, documentos, software, imágenes, videos y demás recursos digitales o físicos, garantizando el respeto a los derechos de autor y la debida autorización de uso.                                                                                                                                                                                                                                           |
| Alcance             | 1. Todos los funcionarios, contratistas y terceros que generen, gestionen o utilicen contenidos en nombre de la EDRU E.I.C.E.<br>2. Materiales producidos en procesos internos, consultorías externas y alianzas estratégicas.<br>3. Contenidos físicos (documentos, manuales, planos, diseños) y digitales (archivos, imágenes, publicaciones web, software).                                                                                                                                                                       |

|                                                                                                                                                                    |                                                              |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          | Código:<br>POL-DPI-01-03                     |
|                                                                                                                                                                    |                                                              | Versión:<br>01                               |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | Fecha de entrada en vigencia:<br>10-dic-2025 |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cumplimiento             | El incumplimiento de esta política podrá generar:<br>1. Sanciones disciplinarias conforme al reglamento interno de trabajo.<br>2. Acciones legales de responsabilidad civil o penal en los casos que correspondan.<br>3. Revisión de contratos y acuerdos con terceros para garantizar el cumplimiento normativo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Principios rectores      | 1. Legalidad y respeto a la autoría: toda obra se usa y administra conforme a la ley y a sus licencias.<br>2. Titularidad institucional y reconocimiento moral: las obras creadas en cumplimiento de funciones o contratos pertenecen a la entidad, manteniendo el reconocimiento del autor cuando aplique.<br>3. Licenciamiento adecuado: selección, uso y verificación de licencias (comerciales, libres, Creative Commons) conforme a sus términos.<br>4. Transparencia y trazabilidad: registro de licencias, permisos y versiones en inventarios y repositorios institucionales.<br>5. Integridad, autenticidad y disponibilidad: gestión de versiones y controles de cambio para preservar el contenido y su acceso autorizado.<br>6. Confidencialidad y privacidad por diseño: protección de datos personales y secretos institucionales dentro de los contenidos.<br>7. Accesibilidad, inclusión y datos abiertos: adopción de estándares de accesibilidad y publicación como datos abiertos cuando corresponda.<br>8. Seguridad por diseño y por defecto: protección técnica (control de accesos, marcas de agua, metadatos) proporcional al riesgo.<br>9. Rendición de cuentas: aprobaciones, segregación de funciones y evidencia de revisiones previas a la publicación. |
| Revisión y Actualización | Esta política será revisada anualmente o cuando se presenten cambios significativos en la legislación, estructura organizacional o riesgos tecnológicos. Toda modificación deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## 6 DOCUMENTOS Y REGISTROS

- POL-DPI-01-03 POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PLI-GDO-03-03 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- FOR-GDO-03 PLANILLA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES- TIC

|                                                                                                                                                                    |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
|  <p>Gestión Administrativa,<br/>Documental y TIC<br/>Dirección Administrativa</p> | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                                    | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                                    |                                                              |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

- Formato de Registro Incidentes EDRU (REG-GSI-01)
- Reportes trimestrales de seguimiento MIPG (Oficina de Planeación)
- Registros de respaldo y restauración
- Reportes de auditorías internas y externas
- Control de versiones del presente documento
- Actas de Comité Institucional de Gestión y Desempeño relacionadas con aprobaciones o cambios de esta política

## 7 NORMATIVIDAD, DOCUMENTOS Y/O REGISTROS RERERENCIADOS

Normatividad y documentos aplicables:

Normatividad colombiana

1. Ley 1581 de 2012 – Protección de Datos Personales
2. Decreto 1377 de 2013 – Protección y autorización de tratamiento de datos
3. Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública
4. Decreto 1083 de 2015 – Función Pública y MIPG
5. Decreto 612 de 2018 – Política de Gobierno Digital
6. Manual de Gobierno Digital – MinTIC 2023
7. Normas del Archivo General de la Nación

Estándares internacionales:

9. ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información
10. ISO/IEC 27002:2022 – Controles de Seguridad

|                                                                                                                                                              |                                                              |  |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--|-----------------------------------------------------|
| <br>Gestión Administrativa,<br>Documental y TIC<br>Dirección Administrativa | <b>SISTEMA DE GESTIÓN INTEGRADO</b>                          |  | Código:<br><b>POL-DPI-01-03</b>                     |
|                                                                                                                                                              |                                                              |  | Versión:<br><b>01</b>                               |
|                                                                                                                                                              | <b>POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |  | Fecha de entrada en vigencia:<br><b>10-dic-2025</b> |

11. ISO/IEC 27701:2022 – Gestión de Seguridad y Privacidad

12. ISO 31000:2018– Gestión del Riesgo

## 8 Control de cambios

| FICHA CONTROL DE CAMBIOS |             |                                |
|--------------------------|-------------|--------------------------------|
| Versión                  | Fecha       | Descripción de la Modificación |
| 1                        | 10-dic-2025 | Versión inicial                |
|                          |             |                                |

| Elaborado por:                                                                  | Revisado por:                                                                                                                                                                                                                                                                                                        | Comité Institucional de Gestión y Desempeño |             | Resolución de Adopción |                      |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------|------------------------|----------------------|
| Diana Marcela Orozco Jaramillo<br>Contratista – TIC<br>Dirección Administrativa | -Sandra Idalí Arévalo Peña – Director Administrativo<br>-Julián Eduardo Gómez Alarcón – Contratista – Planes Institucionales – Oficina de Planeación<br>-Adriana Millán Azcárate -Contratista - Aseguramiento de la Calidad – Oficina de Planeación.<br>-Jorge Andrés Martínez Zambrano - Jefe Oficina de Planeación | No Acta.                                    | Fecha:      | No.:                   | Fecha de expedición: |
|                                                                                 |                                                                                                                                                                                                                                                                                                                      | 10.1.2.007-2025                             | 05-dic-2025 | 10.15-115-2025         | 10-dic-2025          |