PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EDUR
Empresa de Desarrollo
Territorial Urbano y Rural de Risaralda

DEPARTAMENTO DE
RISARALDA

"PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN- EMPRESA DE DESARROLLO TERRITORIAL URBANO Y RURAL DE RISARALDA VIGENCIA 2026"

INTRODUCCIÓN

La Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR, en cumplimiento de su misión institucional y en coherencia con los principios de legalidad, transparencia, eficiencia, responsabilidad y mejora continua que orientan la gestión pública, presenta el Plan de Seguridad y Privacidad de la Información – Vigencia 2026, como un instrumento estratégico fundamental para la protección de los activos de información y el fortalecimiento de la gobernanza digital de la entidad.

En el contexto actual, caracterizado por la acelerada transformación digital del Estado, la creciente dependencia de los sistemas de información, la interoperabilidad entre entidades públicas y el aumento de amenazas cibernéticas, la información se ha consolidado como uno de los activos más críticos para el cumplimiento de los objetivos institucionales. En este escenario, la adecuada gestión de la seguridad y privacidad de la información se convierte en un elemento clave para garantizar la continuidad operativa, la toma de decisiones basada en datos confiables y la prestación de servicios públicos seguros y oportunos a la ciudadanía.

La EDUR desarrolla y ejecuta proyectos de alto impacto en el desarrollo urbano y rural del departamento de Risaralda, los cuales requieren del uso intensivo de plataformas tecnológicas, bases de datos, sistemas de información y herramientas digitales que soportan los procesos de planeación, formulación, ejecución, seguimiento y control de la gestión institucional. Este entorno digital exige la adopción de medidas integrales que permitan proteger la información frente a riesgos tecnológicos, errores humanos, accesos no autorizados, pérdida de datos y

otros eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

El Plan de Seguridad y Privacidad de la Información 2026 se formula en alineación con el Modelo de Seguridad y Privacidad de la Información – MSPI versión 4, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión – MIPG, y los lineamientos establecidos en la norma internacional ISO/IEC 27001:2022, integrándose de manera transversal al Sistema Integrado de Gestión de la EDUR y al Plan Estratégico Institucional 2023–2027.

Durante la vigencia 2026, la EDUR orienta sus esfuerzos no solo al cumplimiento normativo, sino a la consolidación de una gestión madura de la seguridad de la información, basada en la identificación y tratamiento sistemático de riesgos, la implementación de controles técnicos, administrativos y organizacionales, y el fortalecimiento de una cultura institucional de seguridad y protección de datos. Este enfoque permite avanzar de manera progresiva hacia estándares internacionales de calidad y seguridad, promoviendo la sostenibilidad tecnológica y la resiliencia institucional frente a incidentes de seguridad de la información.

Asimismo, el Plan reconoce la importancia de la protección de los datos personales de ciudadanos, funcionarios, contratistas y aliados estratégicos, garantizando su tratamiento conforme a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios, así como el respeto por los derechos fundamentales de los titulares de la información. La privacidad y la seguridad de los datos se constituyen, de esta manera, en pilares esenciales para fortalecer la confianza ciudadana y la legitimidad de la gestión pública.

El Plan de Seguridad y Privacidad de la Información 2026 adopta el enfoque de mejora continua mediante el ciclo Planear – Hacer – Verificar – Actuar (PHVA), lo que permite evaluar permanentemente la efectividad de las políticas, procesos y controles implementados, identificar oportunidades de mejora y ajustar las

estrategias institucionales de acuerdo con los cambios del entorno tecnológico, normativo y organizacional.

De igual forma, este Plan tiene un carácter transversal y corresponsable, involucrando a todas las dependencias, procesos, funcionarios, contratistas y terceros que, en el ejercicio de sus funciones, tengan acceso a información institucional. La seguridad y la privacidad de la información no se conciben únicamente como una responsabilidad técnica, sino como un compromiso institucional colectivo que contribuye a la transparencia, la eficiencia administrativa y la consolidación de una administración pública moderna, segura y orientada al servicio del territorio risaraldense.

En este sentido, el Plan de Seguridad y Privacidad de la Información – Vigencia 2026 se consolida como una herramienta estratégica de planeación que articula la gestión del riesgo, la innovación tecnológica y el control institucional, permitiendo a la EDUR avanzar hacia una entidad más confiable, resiliente y preparada para enfrentar los desafíos del entorno digital, en beneficio del desarrollo territorial integral y del bienestar de la comunidad.

OBJETIVO GENERAL

Establecer, consolidar y fortalecer durante la vigencia 2026 el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) de la Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR, como un componente estratégico de la planeación institucional, orientado a la protección integral de los activos de información que soportan los procesos misionales, estratégicos y de apoyo de la entidad.

El presente Plan tiene como propósito garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, mediante la implementación, seguimiento y mejora continua de políticas, procedimientos, controles técnicos, administrativos y organizacionales, que permitan prevenir,

mitigar y gestionar los riesgos asociados al tratamiento, almacenamiento, transmisión y uso de la información, tanto en entornos físicos como digitales.

Asimismo, el Plan busca asegurar el cumplimiento del marco normativo vigente en materia de protección de datos personales, seguridad de la información y gobierno digital, en especial lo dispuesto en la Ley 1581 de 2012, el Modelo de Seguridad y Privacidad de la Información – MSPI versión 4, el Modelo Integrado de Planeación y Gestión – MIPG y la norma ISO/IEC 27001:2022, promoviendo una gestión institucional transparente, responsable y orientada a resultados.

De igual forma, el Objetivo General se orienta a fortalecer la cultura organizacional de seguridad y privacidad de la información, fomentando la corresponsabilidad de funcionarios, contratistas y terceros, y a integrar la gestión del riesgo de seguridad de la información con los procesos de planeación, control interno y mejora continua, contribuyendo a la continuidad operativa, la sostenibilidad tecnológica y la confianza de la ciudadanía en la gestión pública de la EDUR.

OBJETIVOS ESPECIFICOS

1. ***Fortalecer la cultura institucional de seguridad y privacidad de la información***: mediante la implementación de programas permanentes de sensibilización, capacitación y apropiación de buenas prácticas dirigidos a funcionarios, contratistas y terceros, promoviendo el uso responsable de los activos de información y la corresponsabilidad institucional durante la vigencia 2026.
2. ***Garantizar la protección y tratamiento adecuado de los datos personales:*** en cumplimiento del marco normativo vigente (Ley 1581 de 2012, Decreto 1377 de 2013, y demás disposiciones aplicables), asegurando que todos los procesos institucionales se desarrollen bajo los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida.

3. ***Implementar, mantener y fortalecer controles técnicos, administrativos y organizacionales*** que aseguren la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI v4 y la norma ISO/IEC 27001:2022.
4. ***Identificar, analizar, evaluar y tratar de manera sistemática los riesgos de seguridad de la información,*** integrando la gestión del riesgo tecnológico a los procesos de planeación institucional, control interno y toma de decisiones estratégicas, bajo el enfoque de mejora continua.
5. ***Consolidar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)*** como un componente transversal del Sistema Integrado de Gestión y del Modelo Integrado de Planeación y Gestión – MIPG, asegurando su articulación con el Plan Estratégico Institucional 2023–2027 y con los planes operativos de la vigencia 2026.
6. ***Fortalecer los mecanismos de monitoreo, seguimiento, auditoria y evaluación del SGSI,*** mediante la definición e implementación de indicadores de desempeño, auditorías internas y revisiones periódicas, que permitan medir la efectividad de los controles y promover acciones de mejora continua.
7. ***Asegurar la continuidad operativa y la resiliencia institucional,*** mediante la incorporación de criterios de seguridad de la información y ciberseguridad en la planeación de proyectos, la gestión de cambios y los planes de continuidad del negocio, minimizando el impacto de incidentes tecnológicos en la operación de la EDUR.

OBJETIVOS ESTRATÉGICOS

1. ***Consolidar un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) robusto, sostenible y auditable.*** Fortalecer y madurar el SGSI de la EDUR como un sistema integral, transversal y documentado, alineado con el Modelo de Seguridad y Privacidad de la Información – MSPI

v4 y la norma ISO/IEC 27001:2022, que garantice la protección efectiva de los activos de información institucionales y su adecuada gestión a lo largo del ciclo de vida de la información.

Este objetivo estratégico permite asegurar la sostenibilidad del sistema, facilita los procesos de auditoría y control, y constituye la base para avanzar hacia mayores niveles de madurez y certificación institucional.

2. ***Fortalecer la gobernanza institucional y la toma de decisiones en materia de seguridad digital.***

   Promover una gestión estratégica de la seguridad y privacidad de la información basada en la gestión del riesgo, la definición clara de roles y responsabilidades, y la participación activa de la Alta Dirección y los líderes de proceso, garantizando que las decisiones institucionales incorporen criterios de seguridad desde la planeación hasta la ejecución.

   Este objetivo fortalece la articulación entre Planeación, TIC, Control Interno y las áreas misionales, en coherencia con los principios del Gobierno Digital y el Modelo Integrado de Planeación y Gestión – MIPG.

3. ***Integrar la seguridad y privacidad de la información de manera transversal en los procesos misionales, estratégicos y de apoyo.***

   Incorporar los lineamientos, políticas y controles de seguridad y privacidad de la información en la planeación, ejecución, seguimiento y evaluación de los procesos institucionales, asegurando la continuidad operativa, la protección de la información y el adecuado desarrollo de los proyectos de la EDUR.

   Este objetivo garantiza que la seguridad de la información no sea un componente aislado, sino un eje transversal de la gestión institucional y del desarrollo territorial.

4. ***Proteger de manera integral los datos personales y la información sensible administrada por la EDUR***

Asegurar la implementación efectiva de políticas, procedimientos y controles orientados a la protección de los datos personales y la información sensible de ciudadanos, funcionarios, contratistas y terceros, garantizando el cumplimiento del marco normativo vigente y fortaleciendo la confianza ciudadana y la transparencia institucional.

Este objetivo estratégico consolida a la EDUR como una entidad responsable, ética y confiable en el tratamiento de la información y en la protección de los derechos fundamentales de los titulares de los datos.

ESTRUCTURA DE GOBERNANZA DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el fin de garantizar la dirección, sostenibilidad y toma de decisiones estratégicas en materia de seguridad y privacidad de la información, la EDUR establece la siguiente estructura de gobernanza del SGSI:

Responsable el SGSI

La entidad designará formalmente un responsable del Sistema de Gestión de Seguridad y Privacidad de la Información, quien actuará como líder técnico y articulador institucional del sistema. Sus funciones principales serán:

- Coordinar la implementación, mantenimiento y mejora continua del SGSI.
- Consolidar la gestión del riesgo de seguridad de la información.
- Hacer seguimiento a incidentes de seguridad.
- Liderar auditorías internas y revisiones técnicas.
- Presentar informes periódicos a la Alta Dirección.

ALCANCE DEL PLAN

El Plan de Seguridad y Privacidad de la Información – Vigencia 2026 establece el marco institucional mediante el cual la Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR implementa, consolida y fortalece su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), garantizando la protección integral de los activos de información que soportan el cumplimiento de sus funciones misionales, estratégicas y de apoyo.

El alcance del Plan es integral, transversal y obligatorio, y comprende todos los procesos, dependencias, proyectos, sistemas, personas y recursos que intervienen directa o indirectamente en el tratamiento de la información institucional, independientemente de su formato, origen, ubicación o medio de almacenamiento.

1. Alcance organizacional

El Plan aplica a todas las áreas, dependencias y procesos de la EDUR, incluyendo los procesos misionales, estratégicos, de apoyo y de evaluación y control, de conformidad con el mapa de procesos institucional.

Así mismo, involucra de manera obligatoria a:

- ✓ Funcionarios de planta.
- ✓ Contratistas y consultores.
- ✓ Proveedores y terceros.
- ✓ Aliados estratégicos que, en el ejercicio de sus funciones, tengan acceso a información institucional.

Cada uno de estos actores es corresponsable del cumplimiento de las políticas, procedimientos y controles definidos en el SGSI.

2. Alcance sobre la información

El Plan cubre toda la información generada, procesada, administrada, almacenada, transmitida o custodiada por la EDUR, sin distinción de:

- ✓ Tipo de información (administrativa, financiera, contractual, técnica, misional, estratégica).
- ✓ Nivel de clasificación (pública, de uso interno, reservada o confidencial).
- ✓ Medio de soporte (físico, digital o mixto).
- ✓ Origen (interno o externo).

Incluye de manera prioritaria la información que contenga datos personales, datos sensibles y datos de especial protección, garantizando su tratamiento conforme al marco normativo vigente.

3. Alcance sobre los activos de información

El Plan abarca la totalidad de los activos de información de la EDUR, incluyendo, entre otros:

- ✓ Bases de datos institucionales.
- ✓ Sistemas de información y aplicativos.
- ✓ Infraestructura tecnológica (servidores, redes, dispositivos de comunicación).
- ✓ Equipos de cómputo, dispositivos móviles y medios de almacenamiento.
- ✓ Documentación institucional y archivos físicos y electrónicos.

Cada activo de información deberá estar identificado, clasificado, valorado y protegido de acuerdo con su nivel de criticidad, sensibilidad e impacto institucional.

4. Alcance tecnológico

El Plan aplica a todos los servicios, plataformas y recursos tecnológicos utilizados por la EDUR para el desarrollo de sus actividades, tanto en la sede administrativa como en los proyectos ejecutados en territorio, incluyendo:

- ✓ Infraestructura local y en la nube.
- ✓ Sistemas internos y servicios tercerizados.
- ✓ Plataformas de interoperabilidad y servicios digitales.
- ✓ Herramientas de trabajo remoto y teletrabajo.

El alcance tecnológico contempla la implementación de controles de seguridad física y lógica, la gestión de accesos, la protección contra amenazas cibernéticas, la realización de copias de respaldo y la continuidad de los servicios tecnológicos.

5. Alcance en la gestión del riesgo y continuidad del negocio

El Plan incorpora la gestión del riesgo de seguridad de la información como un componente transversal de la planeación institucional, integrando:

- ✓ Identificación y evaluación de riesgos.
- ✓ Definición de controles y planes de tratamiento.
- ✓ Seguimiento y actualización permanente de la matriz de riesgos.
- ✓ Articulación con los planes de continuidad del negocio y recuperación ante desastres.

Este enfoque permite minimizar el impacto de incidentes de seguridad sobre los procesos críticos y los servicios a la ciudadanía.

6. Alcance normativo y de control

El Plan se desarrolla en cumplimiento del marco normativo nacional e institucional aplicable y se articula con:

- ✓ El Modelo de Seguridad y Privacidad de la Información – MSPI v4.
- ✓ El Modelo Integrado de Planeación y Gestión – MIPG.
- ✓ El Sistema Integrado de Gestión de la EDUR.
- ✓ Los procesos de control interno, auditoría y rendición de cuentas.

El cumplimiento del Plan será objeto de seguimiento periódico, auditorías internas y revisiones independientes, garantizando la mejora continua del SGSI.

7. Alcance temporal

El presente Plan tiene vigencia para el año 2026, sin perjuicio de que sus políticas, controles y procedimientos puedan mantenerse, ajustarse o fortalecerse en vigencias posteriores, de acuerdo con los resultados de las evaluaciones, los cambios normativos o las necesidades institucionales.

8. Enfoque estratégico del alcance

El alcance definido permite que el SGSI de la EDUR sea:

- ✓ ***Auditable***, frente a entes de control y estándares internacionales.
- ✓ ***Escalable,*** para adaptarse al crecimiento institucional.
- ✓ ***Sostenible,*** en el tiempo y en los recursos.
- ✓ ***Articulado,*** con la planeación estratégica y operativa.

De esta manera, el Plan de Seguridad y Privacidad de la Información – Vigencia 2026 se consolida como un instrumento clave de la planeación institucional, que fortalece la gestión pública, protege la información y garantiza la confianza ciudadana en la EDUR.

MARCO NORMATIVO

El presente Plan de Seguridad y Privacidad de la Información se sustenta en un conjunto de normas, políticas, decretos y estándares técnicos que establecen los lineamientos para garantizar la protección, confidencialidad, integridad y disponibilidad de la información institucional administrada por la Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR.

El marco normativo que orienta la implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), está conformado por las siguientes disposiciones:

1. **Marco legal nacional**

- ✓ ***Constitución Política de Colombia (1991)***

Artículos 15, 20, 74 y 209, que establecen el derecho a la intimidad personal, al buen nombre, al acceso a la información y la obligación de las entidades públicas de actuar conforme a los principios de eficiencia, moralidad, transparencia y responsabilidad.

- ✓ ***Ley 1581 de 2012 – Régimen General de Protección de Datos Personales***

Regula los principios, derechos y procedimientos para garantizar la protección de los datos personales en Colombia.

- ✓ ***Decreto 1377 de 2013***

Reglamenta parcialmente la Ley 1581 de 2012 y define los procedimientos para la autorización, uso, almacenamiento y tratamiento de datos personales.

- ✓ ***Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional***

Establece disposiciones para la gestión, divulgación y acceso a la información pública, promoviendo la transparencia en las entidades del Estado.

- ✓ ***Decreto 103 de 2015***

Reglamenta parcialmente la Ley 1712 de 2014, incorporando lineamientos sobre la gestión de información pública y la protección de datos personales en las entidades públicas.

- ✓ ***Decreto 1008 de 2018***

Actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro de la Política de Gobierno Digital, estableciendo lineamientos para la gestión de riesgos, seguridad y privacidad en la información pública.

- ✓ ***Decreto 612 de 2018***

Define los lineamientos para la gestión y reporte de la Planeación Institucional, integrando la planeación estratégica, la gestión del riesgo y los sistemas de control interno, de los cuales el SGSI forma parte.

- ✓ ***Ley 527 de 1999 – Comercio Electrónico y Firma Digital***

Reconoce la validez jurídica de los mensajes de datos, el uso de medios electrónicos y la firma digital como mecanismos seguros en las transacciones electrónicas.

- ✓ ***Ley 1266 de 2008***

Regula el manejo de información contenida en bases de datos personales de carácter financiero, crediticio y comercial.

- ✓ ***Ley 1341 de 2009 (modificada por la Ley 1978 de 2019)***

Define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC).

- ✓ ***Ley 2052 de 2020***

Fortalece la Política de Gobierno Digital y promueve la transformación digital en el sector público colombiano, impulsando la adopción de prácticas de seguridad de la información.

- ✓ ***Ley 594 de 2000 – Ley General de Archivos***
  Establece los principios y normas para la función archivística del Estado, garantizando la preservación, integridad, disponibilidad y conservación de la información pública, elementos fundamentales para la seguridad de la información.
- ✓ ***Lineamientos de Interoperabilidad del Estado Colombiano***

Relacionados con el intercambio seguro de información entre entidades públicas, asegurando estándares de seguridad, integridad y confidencialidad.

2. Marco normativo institucional

- ✓ Política de Gobierno Digital del Estado Colombiano, establecida por el MinTIC, en el marco de la Resolución 500 de 2021, que incluye el Modelo de Seguridad y Privacidad de la Información – MSPI versión 4, como referente obligatorio para las entidades públicas.
- ✓ Política de Tratamiento de Datos Personales de la EDUR, que regula la recolección, uso, almacenamiento, circulación y supresión de los datos personales administrados por la entidad.
- ✓ Sistema Integrado de Gestión (SIG) de la EDUR, que articula los componentes de calidad, control interno, planeación, gestión documental y seguridad de la información bajo el enfoque de mejora continua.

3. Marco normativo internacional y estándares técnicos

- ✓ ***ISO/IEC 27001:2022***

Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

- ✓ ***ISO/IEC 27002:2022***

Proporciona un conjunto de controles, buenas prácticas y recomendaciones para la implementación de medidas de seguridad de la información.

- ✓ ***ISO 22301:2019 – Continuidad del Negocio***

Establece los requisitos para planificar, establecer, implementar y mantener un sistema de gestión que asegure la continuidad de las operaciones frente a incidentes disruptivos.

- ✓ ***ISO 31000:2018 – Gestión del Riesgo***

Define los principios y directrices para la gestión integral del riesgo en las organizaciones, aplicable a los riesgos asociados con la información.

- ✓ ***ISO/IEC 27005:2022 – Gestión del Riesgo en Seguridad de la Información***

Complementa la ISO 27001, proporcionando una guía detallada para identificar, analizar y tratar riesgos relacionados con la información.

4. **Otros lineamientos y referentes**

- ✓ Guía para la Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI v4 (MinTIC, 2022).
- ✓ Manual de Política de Gobierno Digital del Ministerio TIC.
- ✓ Circular Externa 02 de 2015 de la Superintendencia de Industria y Comercio, sobre buenas prácticas en el tratamiento de datos personales.
- ✓ Política Nacional de Seguridad Digital de Colombia (CONPES 3854 de 2016).
- ✓ Plan Nacional de Seguridad Digital 2023–2028 (MinTIC).

Con este marco normativo, la EDUR establece las bases legales y técnicas que sustentan la gestión integral de la seguridad y privacidad de la información, asegurando el cumplimiento de la normatividad vigente, la mejora continua del SGSI y la confianza de los ciudadanos en la gestión pública.

RESUMEN EJECUTIVO

La Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR, reconociendo la información como un activo estratégico fundamental para la toma de decisiones, la ejecución de proyectos y la prestación de servicios públicos, adopta el Plan de Seguridad y Privacidad de la Información – Vigencia 2026, como un instrumento clave de la planeación institucional y de la gobernanza digital.

En un contexto de creciente transformación digital, interoperabilidad entre entidades públicas y aumento de los riesgos cibernéticos, la EDUR enfrenta el desafío de garantizar que la información que administra sea protegida de manera integral, oportuna y conforme al marco normativo vigente. Este Plan responde a dicha necesidad, fortaleciendo el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) y consolidando una gestión institucional basada en la prevención, el control del riesgo y la mejora continua.

El Plan se formula en coherencia con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo de Seguridad y Privacidad de la Información – MSPI versión 4, y los requisitos establecidos en la norma internacional ISO/IEC 27001:2022, integrándose de manera transversal al Sistema Integrado de Gestión de la EDUR y al Plan Estratégico Institucional 2023–2027. Esta alineación garantiza que las acciones definidas no se limiten al cumplimiento normativo, sino que contribuyan efectivamente al fortalecimiento institucional y a la generación de valor público.

Durante la vigencia 2026, el Plan orienta sus acciones estratégicas a la consolidación y maduración del SGSI, fortaleciendo la identificación y clasificación de los activos de información, la gestión del riesgo de seguridad de la información, la implementación y optimización de controles técnicos, administrativos y organizacionales, y el desarrollo de una cultura institucional de seguridad y privacidad de la información.

Entre los ejes prioritarios del Plan se destacan:

- ✓ La protección integral de la información institucional y de los datos personales de ciudadanos, funcionarios, contratistas y aliados estratégicos.
- ✓ La integración de la seguridad y privacidad de la información en todos los procesos misionales, estratégicos y de apoyo de la entidad.

- ✓ El fortalecimiento de la gobernanza institucional y la toma de decisiones basadas en la gestión del riesgo.
- ✓ La mejora de la resiliencia digital y la continuidad operativa frente a incidentes de seguridad.

El Plan contempla, además, mecanismos de seguimiento, evaluación y control, mediante la definición de indicadores de desempeño, auditorías internas, revisiones independientes y procesos de mejora continua, que permiten evaluar la efectividad de los controles implementados y ajustar las estrategias institucionales de acuerdo con los resultados obtenidos.

Como resultado de la implementación del Plan de Seguridad y Privacidad de la Información – Vigencia 2026, la EDUR espera consolidar una entidad más segura, eficiente, transparente y confiable, con mayores capacidades para prevenir y gestionar incidentes de seguridad de la información, proteger los derechos de los titulares de los datos personales y garantizar la continuidad de los servicios institucionales.

Finalmente, este Plan se proyecta como un insumo estratégico para la planeación de mediano y largo plazo, sentando las bases para avanzar hacia mayores niveles de madurez en seguridad de la información, la automatización de controles, el fortalecimiento de la cultura digital segura y la preparación institucional para procesos de auditoría y certificación bajo estándares internacionales, en beneficio del desarrollo territorial integral del departamento de Risaralda y de la confianza de la ciudadanía en la gestión pública de la EDUR.

DEFINICIONES DE TERMINOS

Para efectos del Plan de Seguridad y Privacidad de la Información 2026 de la Empresa de Desarrollo Territorial, Urbana y Rural de Risaralda – EDUR, se adoptan las siguientes definiciones, basadas en la normatividad nacional, la política de

Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2022:

- ✓ ***Seguridad de la Información***

Conjunto de políticas, procedimientos y medidas encaminadas a proteger los activos de información de la entidad, garantizando su confidencialidad, integridad y disponibilidad, frente a amenazas internas o externas.

- ✓ ***Privacidad de la Información***

Derecho de las personas a controlar la recolección, uso, almacenamiento y divulgación de sus datos personales. Implica el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, así como de las buenas prácticas en protección de datos.

- ✓ ***Sistema de Gestión de Seguridad de la Información (SGSI)***

Conjunto de políticas, objetivos, procesos y recursos establecidos por la EDUR para administrar y mejorar de forma continua la seguridad de la información, siguiendo el ciclo PHVA (Planear, Hacer, Verificar y Actuar).

- ✓ ***Modelo de Seguridad y Privacidad de la Información (MSPI)***

Marco de referencia definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que orienta a las entidades públicas en la implementación de controles para proteger la información institucional y los datos personales.

- ✓ ***Activo de Información***

Cualquier dato, documento, sistema, base de datos, equipo o infraestructura tecnológica que posea valor para la organización y que deba ser protegido de acuerdo con su nivel de criticidad o sensibilidad.

- ✓ ***Confidencialidad***

Propiedad de la información que garantiza que el acceso a los datos solo sea permitido a personas, sistemas o procesos debidamente autorizados.

- ✓ ***Integridad***

Propiedad que asegura que la información se mantenga completa, exacta y sin alteraciones no autorizadas durante su almacenamiento, procesamiento o transmisión.

- ✓ ***Disponibilidad***

Condición mediante la cual la información y los servicios asociados están accesibles y utilizables por los usuarios autorizados cuando lo requieran.

- ✓ ***Riesgo de Seguridad de la Información***

Posibilidad de que una amenaza explote una vulnerabilidad y cause impacto en los activos de información o en los procesos institucionales, afectando la confidencialidad, integridad o disponibilidad de los datos.

- ✓ ***Amenaza***

Evento o circunstancia con el potencial de causar daño a los activos de información, ya sea de origen humano, técnico, natural o ambiental.

- ✓ ***Vulnerabilidad***

Debilidad o falla en un sistema, proceso o control que puede ser aprovechada por una amenaza para comprometer la seguridad de la información.

- ✓ ***Control de Seguridad***

Medida preventiva, correctiva o detectiva implementada para reducir la probabilidad o el impacto de los riesgos que afectan los activos de información.

- ✓ ***Ciberseguridad***

Conjunto de prácticas, políticas y herramientas tecnológicas destinadas a proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o incidentes digitales.

- ✓ ***Tratamiento de Datos Personales***

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión, de conformidad con lo establecido en la Ley 1581 de 2012.

- ✓ ***Incidente de Seguridad de la Información***

Evento o conjunto de eventos inesperados que comprometen o tienen el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información institucional.

- ✓ ***Plan de Continuidad del Negocio (PCN)***

Conjunto de estrategias y procedimientos establecidos para garantizar la operación de los procesos críticos de la entidad en caso de interrupciones o desastres que afecten la infraestructura tecnológica o los datos.

- ✓ ***Gestión del Riesgo de Seguridad de la Información***

Proceso sistemático para identificar, evaluar, tratar y monitorear los riesgos que afectan la información institucional, con el fin de reducirlos a niveles aceptables.

- ✓ ***Clasificación de la Información***

Proceso mediante el cual se determina el nivel de sensibilidad o criticidad de la información (pública, reservada, confidencial o de uso interno), para definir los controles de protección aplicables.

- ✓ ***Usuario Autorizado***

Persona que, por función o rol institucional, cuenta con permisos válidos para acceder, procesar o gestionar información o sistemas tecnológicos de la entidad.

- ✓ ***Ciclo de Mejora Continua (PHVA)***

Modelo de gestión que promueve la mejora progresiva del sistema de seguridad de la información mediante las fases Planear, Hacer, Verificar y Actuar, asegurando la evolución constante de los controles y políticas institucionales.

ACTIVADES DEL PLAN PARA DESARROLLAR

Durante la vigencia 2026, la Empresa de Desarrollo Territorial, Urbana y Rural de Risaralda – EDUR orientará la ejecución del Plan de Seguridad y Privacidad de la Información a la consolidación, fortalecimiento y maduración del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), avanzando desde una etapa de implementación hacia un nivel superior de gestión, control y mejora continua.

Las actividades del Plan se desarrollarán bajo el enfoque del ciclo de mejora continua PHVA (Planear – Hacer – Verificar – Actuar), garantizando una gestión sistemática, evaluable y alineada con la planeación institucional, el control interno y los lineamientos del Gobierno Digital.

Cronograma general de ejecución

Actividad	**T1**	**T2**	**T3**	**T4**
Actualización inventario de activos	✓		✓	
Gestión de riesgos SGSI	✓	✓	✓	✓
Implementación de controles	✓	✓	✓	
Capacitación y cultura	✓		✓	
Auditoría interna SGSI		✓		✓
Revisión técnica independiente			✓	

Actualización documental	✓	✓		✓

A continuación, se describen las actividades estratégicas a desarrollar durante la vigencia 2026:

Actividad 1. Identificación, actualización y clasificación de los activos de información

Objetivo:

Consolidar un inventario institucional actualizado de los activos de información de la EDUR, identificando su valor, criticidad y nivel de sensibilidad, como base para la definición de controles de seguridad adecuados.

Descripción:

Durante la vigencia 2026 se realizará la actualización periódica del inventario de activos de información, incorporando nuevos sistemas, bases de datos, documentos, proyectos y servicios tecnológicos. La información será clasificada de acuerdo con su nivel de confidencialidad (pública, de uso interno, reservada o confidencial), definiendo responsables, propietarios del activo y niveles de acceso autorizados.

Esta actividad permitirá fortalecer la gestión de la información a lo largo de su ciclo de vida, mejorar la trazabilidad y asegurar que los activos críticos cuenten con medidas de protección acordes a su impacto institucional.

Resultado esperado:

Inventario de activos de información actualizado, clasificado y aprobado, integrado al SGSI y articulado con la gestión documental y tecnológica de la EDUR.

Actividad 2. Gestión integral del riesgo de seguridad y privacidad de la información

Objetivo:

Fortalecer la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

Descripción:

La EDUR implementará un proceso sistemático de gestión del riesgo de seguridad de la información, alineado con los lineamientos del DAFP, el MSPI y la norma ISO/IEC 27005. Se identificarán amenazas y vulnerabilidades asociadas a los activos de información, se evaluará su impacto y probabilidad, y se definirán planes de tratamiento orientados a reducir los riesgos a niveles aceptables.

Esta actividad se integrará con la planeación institucional, el control interno y la gestión del riesgo corporativo, permitiendo que la Alta Dirección cuente con información oportuna para la toma de decisiones estratégicas.

Resultado esperado:

Matriz de riesgos de seguridad de la información actualizada, con planes de tratamiento definidos, responsables asignados y seguimiento periódico.

Actividad 3. Implementación y fortalecimiento de controles de seguridad y privacidad de la información

Objetivo:

Implementar, optimizar y mantener controles técnicos, administrativos y organizacionales que protejan los activos de información de la EDUR frente a riesgos internos y externos.

Descripción:

Durante 2026 se fortalecerán los controles de seguridad física y lógica, incluyendo la gestión de accesos, autenticación, copias de respaldo, protección contra código

malicioso, seguridad en redes, cifrado de información, control de dispositivos y protección de la información en ambientes de teletrabajo.

Así mismo, se reforzará la aplicación de las políticas de tratamiento de datos personales, la gestión documental segura y los procedimientos de respuesta ante incidentes de seguridad de la información.

Resultado esperado:

Controles de seguridad implementados y operativos, alineados con los requisitos de la ISO/IEC 27001:2022 y el MSPI, con evidencia documentada de su funcionamiento.

Actividad 4. Formación, sensibilización y fortalecimiento de la cultura institucional de seguridad

Objetivo:

Promover una cultura organizacional de seguridad y privacidad de la información, basada en la responsabilidad, la prevención y el uso adecuado de los activos de información.

Descripción:

Se desarrollarán programas de capacitación, campañas de sensibilización y estrategias de comunicación interna dirigidas a funcionarios, contratistas y terceros, abordando temas como buenas prácticas de seguridad digital, protección de datos personales, manejo seguro de la información y prevención de incidentes.

Esta actividad reconoce que el factor humano es un elemento clave en la seguridad de la información y busca reducir los riesgos asociados a errores humanos o prácticas inadecuadas.

Resultado esperado:

Personal capacitado y sensibilizado en seguridad de la información, con mayor nivel de apropiación de las políticas y reducción de incidentes asociados al factor humano.

Actividad 5. Monitoreo, auditoría, evaluación y mejora continua del SGSI

Objetivo:

Garantizar la efectividad, sostenibilidad y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información.

Descripción:

Durante la vigencia 2026 se realizarán auditorías internas, seguimientos periódicos y evaluaciones al SGSI, con el fin de verificar el cumplimiento de las políticas, procedimientos y controles implementados. Se hará seguimiento a los incidentes de seguridad, a los indicadores definidos y a los planes de mejora derivados de las evaluaciones.

Los resultados de estas actividades servirán como insumo para la toma de decisiones de la Alta Dirección y para la actualización permanente del Plan de Seguridad y Privacidad de la Información.

Resultado esperado:

SGSI evaluado y fortalecido, con acciones de mejora documentadas, indicadores actualizados y preparación institucional para procesos de auditoría y certificación.

Indicadores de Desempeño del SGSI

La EDUR implementará un sistema de indicadores que permita evaluar la efectividad del SGSI:

Dimensión	Indicador	Fórmula	Periodicidad

Gestión de incidentes	Incidentes gestionados oportunamente	Incidentes cerrados en tiempo / Total incidentes	Trimestral
Cultura de seguridad	Cobertura de capacitación	Personas capacitadas / Total personal	Semestral
Gestión del riesgo	Riesgos con tratamiento activo	Riesgos con plan implementado / Total riesgos identificados	Trimestral
Controles	Nivel de implementación de controles	Controles implementados / Controles planificados	Semestral
Respaldo de información	Cumplimiento de copias de seguridad	Copias realizadas / Copias programadas	Mensual

Enfoque estratégico de las actividades

Las actividades definidas para la vigencia 2026 permiten a la EDUR:

- ✓ Consolidar un SGSI maduro y articulado con la planeación institucional.
- ✓ Fortalecer la gestión del riesgo tecnológico y la continuidad operativa.
- ✓ Garantizar el cumplimiento normativo y la transparencia institucional.
- ✓ Avanzar hacia mayores niveles de madurez y certificación en seguridad de la información.

AJUSTES E IMPLEMENTACIÓN A LA DOCUMENTACIÓN DE LOS PROCEDIMIENTOS

Durante la vigencia 2026, la Empresa de Desarrollo Territorial, Urbana y Rural de Risaralda – EDUR adelantará un proceso integral de ajuste, actualización,

formalización e implementación de la documentación asociada a los procedimientos del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), con el propósito de garantizar su coherencia, aplicabilidad, trazabilidad y alineación con la planeación institucional y el marco normativo vigente.

Este proceso reconoce que la documentación no constituye un fin en sí mismo, sino una herramienta estratégica de control, estandarización y mejora continua, que permite asegurar la correcta ejecución de los procesos, la gestión del riesgo y el cumplimiento de los objetivos institucionales.

1. Revisión y actualización de los procedimientos existentes

La EDUR realizará una revisión técnica y normativa de los procedimientos asociados a la seguridad y privacidad de la información, con el fin de:

- ✓ Verificar su alineación con el MSPI versión 4 y la ISO/IEC 27001:2022.
- ✓ Actualizar definiciones, responsabilidades y flujos de actividades.
- ✓ Incorporar cambios normativos, tecnológicos y organizacionales ocurridos en la entidad.
- ✓ Eliminar duplicidades o inconsistencias con otros procedimientos del Sistema Integrado de Gestión.

Este ejercicio permitirá asegurar que la documentación vigente refleje la realidad operativa de la entidad y facilite su correcta aplicación por parte de los responsables.

2. Estandarización y articulación con el Sistema Integrado de Gestión

Los procedimientos del SGSI serán estandarizados conforme a los lineamientos institucionales de documentación, garantizando su coherencia con:

- ✓ El mapa de procesos de la EDUR.
- ✓ Los procedimientos de gestión documental, gestión del riesgo, control interno y tecnología.

- ✓ Los formatos, registros y controles definidos por el Sistema Integrado de Gestión.

Esta articulación permitirá que la seguridad y privacidad de la información se integre de manera transversal en los procesos institucionales, evitando la fragmentación documental y fortaleciendo la eficiencia operativa.

3. Formalización de nuevos procedimientos y guías operativas

Durante la vigencia 2026 se documentarán y formalizarán procedimientos y guías operativas que permitan fortalecer la gestión de la seguridad de la información, entre ellos:

- ✓ Procedimiento de clasificación y manejo de la información.
- ✓ Procedimiento de gestión de accesos y control de usuarios.
- ✓ Procedimiento de gestión de incidentes de seguridad de la información.
- ✓ Procedimiento de respaldo, recuperación y continuidad de la información.
- ✓ Lineamientos para el tratamiento de datos personales y atención de derechos de los titulares.

La formalización de estos documentos permitirá una aplicación uniforme de los controles de seguridad y una respuesta oportuna ante eventos que afecten la información institucional.

4. Implementación progresiva y socialización de los procedimientos

Una vez ajustados y aprobados, los procedimientos serán implementados de manera progresiva en todas las áreas de la EDUR, mediante:

- ✓ Jornadas de socialización y capacitación dirigidas a funcionarios y contratistas.
- ✓ Publicación de la documentación en los repositorios institucionales.
- ✓ Acompañamiento técnico a los responsables de proceso para su correcta aplicación.

Este enfoque busca asegurar que la documentación sea comprendida y aplicada en la práctica, fortaleciendo la apropiación institucional del SGSI.

5. Control documental, trazabilidad y gestión de versiones

La EDUR garantizará la correcta administración de la documentación del SGSI mediante:

- ✓ Control de versiones y registros de cambios.
- ✓ Identificación de responsables de actualización y aprobación.
- ✓ Conservación de evidencias de implementación y cumplimiento.
- ✓ Integración con los sistemas de gestión documental institucionales.

Este control permitirá asegurar la trazabilidad de los procedimientos y facilitar los procesos de auditoría interna y externa.

6. Seguimiento, evaluación y mejora continua de los procedimientos

Durante la vigencia 2026 se realizará seguimiento periódico a la aplicación de los procedimientos documentados, evaluando:

- ✓ Su nivel de cumplimiento.
- ✓ Su efectividad en la mitigación de riesgos.
- ✓ Las oportunidades de mejora identificadas a partir de incidentes, auditorías o cambios en el contexto institucional.

Los resultados de estas evaluaciones servirán como insumo para la actualización permanente de la documentación y la mejora continua del SGSI.

Enfoque estratégico del ajuste documental

Los ajustes e implementación a la documentación de los procedimientos permitirán a la EDUR:

- ✓ Fortalecer el control interno y la gestión del riesgo.
- ✓ Garantizar la coherencia entre planeación, ejecución y control.

- ✓ Facilitar los procesos de auditoría y rendición de cuentas.

Incidentes de Seguridad de la Información

La EDUR establecerá un procedimiento formal para la gestión de incidentes que incluya:

- Detección y reporte: Todo funcionario o contratista deberá reportar eventos sospechosos.
- Clasificación del incidente: Según impacto (bajo, medio, alto, crítico).
- Respuesta y contención: Acciones inmediatas para limitar afectación.
- Investigación y análisis de causa raíz.
- Recuperación y restablecimiento del servicio.
- Lecciones aprendidas y acciones correctivas.

Nivel de impacto	Tiempo de atención inicial
Crítico	< 4 horas
Alto	< 8 horas
Medio	< 24 horas
Bajo	< 48 horas

REVISIÓN TÉCNICA INDEPENDIENTE

La Revisión Técnica Independiente constituye un componente fundamental del Plan de Seguridad y Privacidad de la Información – Vigencia 2026 de la Empresa de Desarrollo Territorial, Urbana y Rural de Risaralda – EDUR, en tanto permite evaluar de manera objetiva, imparcial y especializada el nivel de implementación,

efectividad y madurez del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI).

Esta revisión se concibe como un mecanismo de aseguramiento que fortalece la confianza institucional, facilita la toma de decisiones estratégicas y contribuye al cumplimiento de los principios de autocontrol, autorregulación y mejora continua, propios del Modelo Integrado de Planeación y Gestión – MIPG.

1. Alcance de la revisión técnica independiente

La revisión técnica independiente abarcará, como mínimo:

- ✓ La verificación del cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI versión 4.
- ✓ La evaluación de la alineación del SGSI con los requisitos aplicables de la ISO/IEC 27001:2022.
- ✓ La revisión de la documentación del SGSI (políticas, procedimientos, instructivos, registros y evidencias).
- ✓ La evaluación de la implementación y efectividad de los controles técnicos, administrativos y organizacionales.
- ✓ El análisis de la gestión del riesgo de seguridad y privacidad de la información.
- ✓ La verificación del cumplimiento normativo en materia de protección de datos personales.

El alcance podrá ajustarse de acuerdo con el nivel de madurez del SGSI y las prioridades definidas por la Alta Dirección.

2. Naturaleza y carácter independiente de la revisión

La revisión técnica será realizada por un equipo o profesional independiente, con competencias técnicas en seguridad de la información, gestión del riesgo y estándares internacionales, que no haya participado directamente en la

implementación operativa del SGSI, garantizando así la objetividad e imparcialidad del proceso.

Esta independencia fortalece la credibilidad de los resultados y permite identificar de manera clara brechas, debilidades y oportunidades de mejora que no siempre son evidentes en las autoevaluaciones internas.

3. Metodología de la revisión

La revisión técnica independiente se desarrollará mediante una metodología estructurada que incluirá, entre otras actividades:

- ✓ Revisión documental del Plan, políticas y procedimientos del SGSI.
- ✓ Entrevistas con responsables de proceso, líderes de área y personal clave.
- ✓ Verificación de evidencias de implementación y operación de los controles.
- ✓ Análisis de indicadores, registros de incidentes y planes de tratamiento de riesgos.
- ✓ Evaluación del nivel de madurez del SGSI frente a los estándares de referencia.

Esta metodología permitirá obtener una visión integral del estado del SGSI y de su capacidad para proteger los activos de información institucionales.

4. Resultados y productos de la revisión

Como resultado de la revisión técnica independiente se generarán, entre otros, los siguientes productos:

- ✓ Informe técnico de revisión, con conclusiones claras y sustentadas.
- ✓ Identificación de brechas frente a los requisitos del MSPI y la ISO/IEC 27001:2022.
- ✓ Recomendaciones priorizadas para el fortalecimiento del SGSI.
- ✓ Identificación de riesgos residuales y oportunidades de mejora.

- ✓ Insumos para la actualización del Plan de Seguridad y Privacidad de la Información.

Estos productos servirán como base para la toma de decisiones estratégicas y la definición de planes de mejora.

5. Articulación con el control interno y la Alta Dirección

Los resultados de la revisión técnica independiente serán presentados a la Alta Dirección y articulados con:

- ✓ El Sistema de Control Interno.
- ✓ Los planes de mejoramiento institucional.
- ✓ La planeación estratégica y operativa de la EDUR.

De esta manera, la revisión técnica se convierte en un instrumento de gestión que trasciende el cumplimiento formal y aporta valor real a la gestión institucional.

6. Seguimiento y mejora continua

La EDUR realizará seguimiento al cumplimiento de las recomendaciones derivadas de la revisión técnica independiente, definiendo responsables, plazos e indicadores de avance. Este seguimiento permitirá:

- ✓ Verificar la efectividad de las acciones correctivas y preventivas.
- ✓ Fortalecer la madurez del SGSI.
- ✓ Preparar a la entidad para futuras auditorías o procesos de certificación.

Enfoque estratégico de la revisión técnica independiente

La Revisión Técnica Independiente permite a la EDUR:

- ✓ Contar con una evaluación objetiva y especializada del SGSI.
- ✓ Reducir brechas de cumplimiento normativo y técnico.
- ✓ Fortalecer la gestión del riesgo y la continuidad operativa.

- ✓ Avanzar hacia mayores niveles de madurez y buenas prácticas internacionales.

El Plan de Seguridad y Privacidad de la Información – Vigencia 2026 de la Empresa de Desarrollo Territorial, Urbana y Rural de Risaralda – EDUR se consolida como un instrumento estratégico de planeación institucional, orientado a garantizar la protección integral de los activos de información que soportan la gestión pública, la ejecución de proyectos y la prestación de servicios a la ciudadanía.

A lo largo del Plan se definen objetivos, actividades y mecanismos de control que permiten fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), avanzando hacia mayores niveles de madurez, articulación y sostenibilidad. Su implementación durante la vigencia 2026 permitirá a la EDUR consolidar una gestión de la información basada en la prevención, el control del riesgo y la mejora continua, en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo de Seguridad y Privacidad de la Información – MSPI versión 4 y los estándares internacionales de seguridad de la información.

El Plan reconoce la seguridad y la privacidad de la información como responsabilidades institucionales compartidas, que trascienden el ámbito tecnológico y se integran de manera transversal en los procesos misionales, estratégicos y de apoyo. En este sentido, promueve una cultura organizacional orientada al uso responsable de la información, la protección de los datos personales y la adopción de buenas prácticas que fortalecen la transparencia, la confianza ciudadana y la legitimidad institucional.

La ejecución de las actividades definidas permitirá mejorar la identificación y gestión de los riesgos asociados a la información, fortalecer los controles técnicos, administrativos y organizacionales, estandarizar los procedimientos y consolidar mecanismos efectivos de seguimiento, evaluación y control. Así mismo, la incorporación de procesos de revisión técnica independiente y auditoría interna

contribuirá a asegurar la efectividad del SGSI y a orientar las decisiones estratégicas de la Alta Dirección.

Finalmente, el Plan de Seguridad y Privacidad de la Información – Vigencia 2026 se proyecta como una base sólida para la planeación de mediano y largo plazo de la EDUR, facilitando la continuidad de las acciones, la optimización de recursos y la preparación institucional para futuros procesos de evaluación y certificación. Su implementación reafirma el compromiso de la entidad con una gestión pública moderna, segura y responsable, que protege la información como un activo estratégico y contribuye al desarrollo territorial integral y sostenible del departamento de Risaralda.

Elaboró	Revisión	Aprobó
Bayron Restrepo Profesional contratista oficina de Planeación	Carlos Augusto Hincapié Franco Director Administrativo y financiero Juan Adrián Torres Orozco Jeje Oficina de Planeación Daniela Forondo Tamayo Jefe Oficina Jurídica	Comité de Gestión y Desempeño Acta 1: Enero 30 de 2026