PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EDUR
Empresa de Desarrollo
Territorial Urbano y Rural de Risaralda

DEPARTAMENTO DE
RISARALDA

“PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-EMPRESA DE DESARROLLO TERRITORIAL URBANO Y RURAL DE RISARALDA VIGENCIA 2026”

1. RESUMEN EJECUTIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa de Desarrollo Urbano y Rural – EDUR para la vigencia 2026 es un instrumento estratégico de planeación orientado a identificar, analizar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, así como el adecuado tratamiento de los datos personales bajo custodia de la entidad.

El plan se formula en cumplimiento de la normatividad colombiana vigente, entre la que se destacan la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, la Ley 594 de 2000 de archivos, el CONPES 3854 de 2016 de Seguridad Digital y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG. De igual manera, adopta como referencia buenas prácticas internacionales contenidas en las normas ISO/IEC 27001, 27002 y 27701.

El alcance del plan comprende todos los procesos misionales, estratégicos, de apoyo y de evaluación de EDUR, así como la información en cualquier formato (físico, digital, verbal o audiovisual), los sistemas de información, la infraestructura tecnológica y los archivos institucionales. Igualmente, involucra a funcionarios, contratistas, proveedores y terceros que tengan acceso a la información.

A partir de la aplicación de una metodología de gestión del riesgo alineada con la Guía del DAFP, el MIPG y la norma ISO 27005, se identifican los principales riesgos asociados a accesos no autorizados, pérdida o fuga de información, uso indebido

de datos personales, ataques informáticos, deficiencias en las copias de seguridad, manejo inadecuado de archivos físicos, desconocimiento normativo, debilidades en la gestión de proveedores, falta de reporte oportuno de incidentes y ausencia de políticas actualizadas.

Para el tratamiento de estos riesgos, el plan define controles técnicos, administrativos y organizacionales orientados principalmente a la mitigación y prevención, tales como la implementación de controles de acceso por roles, autenticación segura, clasificación y cifrado de la información, políticas de tratamiento de datos personales, copias de seguridad periódicas, gestión de incidentes de seguridad, capacitación del talento humano y fortalecimiento de los controles contractuales con proveedores.

El plan establece roles y responsabilidades claras para la Alta Dirección, el responsable de seguridad de la información, el oficial de protección de datos, los funcionarios, contratistas y el área de Control Interno, así como indicadores de seguimiento que permiten medir el nivel de implementación y efectividad de las acciones definidas.

Finalmente, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de EDUR se concibe como una herramienta dinámica, sujeta a seguimiento permanente, revisión anual y mejora continua, que contribuye al fortalecimiento del sistema de control interno, la gestión institucional por resultados y la confianza de la ciudadanía durante la vigencia 2026.

2. INTRODUCCION

La información constituye uno de los activos estratégicos más importantes de la Empresa de Desarrollo Urbano y Rural – EDUR, en tanto soporta la planeación institucional, la ejecución de proyectos, la toma de decisiones, la prestación de

servicios a la ciudadanía y la interacción con otras entidades públicas y privadas. En este contexto, la adecuada gestión de la seguridad y la privacidad de la información resulta fundamental para garantizar la continuidad operativa, la confianza institucional y el cumplimiento de los fines misionales de la entidad.

El incremento en el uso de tecnologías de la información, la digitalización de los procesos, la interoperabilidad entre sistemas y el manejo permanente de datos personales de ciudadanos, funcionarios, contratistas y proveedores, exponen a EDUR a diversos riesgos asociados a accesos no autorizados, pérdida o fuga de información, ataques cibernéticos, uso indebido de datos personales y fallas en la gestión documental, tanto en medios físicos como digitales.

En atención a este escenario, y en cumplimiento de la normatividad colombiana vigente en materia de protección de datos personales, transparencia, gestión documental y seguridad digital, la Empresa de Desarrollo Urbano y Rural – EDUR formula el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, como un instrumento de planeación preventiva y correctiva orientado a identificar, analizar, evaluar y tratar de manera sistemática los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Este plan se encuentra alineado con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, en particular con la Dimensión de Control Interno, y adopta buenas prácticas establecidas en estándares internacionales como las normas ISO/IEC 27001, 27002 y 27701, así como las directrices de la Política Nacional de Seguridad Digital. De esta manera, se busca fortalecer la cultura organizacional en seguridad de la información, promover la responsabilidad de todos los actores institucionales y asegurar una gestión integral y articulada del riesgo.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de EDUR no solo responde a exigencias normativas y de control, sino que se consolida

como una herramienta estratégica de apoyo a la planeación institucional, la gestión por resultados y la rendición de cuentas, contribuyendo a la mejora continua de los procesos y al fortalecimiento de la confianza de la ciudadanía y de los grupos de interés durante la vigencia 2026.

3. OBJETIVO GENERAL

Fortalecer la gestión integral de la seguridad y la privacidad de la información de la Empresa de Desarrollo Urbano y Rural – EDUR mediante la identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando el adecuado tratamiento de los datos personales, el cumplimiento de la normatividad colombiana vigente y la alineación con el Modelo Integrado de Planeación y Gestión – MIPG durante la vigencia 2026.

Este objetivo busca asegurar que la información institucional sea gestionada de manera segura, confiable y oportuna, como soporte fundamental para la toma de decisiones, la ejecución de los procesos misionales, la continuidad operativa, la transparencia institucional y la confianza de la ciudadanía y de los grupos de interés.

4. OBJETIVO ESPECÍFICOS

- ✓ Identificar y actualizar los activos de información de EDUR, así como las amenazas y vulnerabilidades asociadas, con el fin de contar con un panorama claro de los riesgos que pueden afectar la seguridad y la privacidad de la información institucional.
- ✓ Analizar y valorar los riesgos de seguridad y privacidad de la información, estableciendo su nivel de probabilidad e impacto, para priorizar las

acciones de tratamiento de acuerdo con su criticidad y efectos sobre los procesos institucionales.

- ✓ Definir e implementar controles técnicos, administrativos y organizacionales orientados a prevenir, mitigar, evitar o transferir los riesgos identificados, en concordancia con la normatividad vigente y las buenas prácticas nacionales e internacionales.
- ✓ Garantizar el cumplimiento de la Ley 1581 de 2012 y demás disposiciones relacionadas con la protección de datos personales, asegurando el respeto de los derechos de los titulares de la información y el uso adecuado de los datos bajo custodia de la entidad.
- ✓ Fortalecer la cultura organizacional en materia de seguridad de la información y privacidad de datos personales, mediante procesos permanentes de capacitación, sensibilización, inducción y reinducción dirigidos a funcionarios, contratistas y terceros.
- ✓ Establecer mecanismos de gestión, reporte y atención de incidentes de seguridad de la información, que permitan una respuesta oportuna, coordinada y eficaz ante eventos que comprometan los activos de información.
- ✓ Implementar indicadores de seguimiento y mecanismos de control que permitan evaluar periódicamente el nivel de cumplimiento, efectividad e impacto del plan, facilitando la toma de decisiones y la mejora continua.
- ✓ Asegurar la articulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información con la planeación estratégica institucional, el Sistema de Control Interno y los procesos de auditoría y rendición de cuentas durante la vigencia 2026.

5. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa de Desarrollo Urbano y Rural – EDUR tiene un alcance institucional e

integral, y aplica a todos los niveles, procesos, recursos y actores que intervienen en la gestión, uso, custodia y tratamiento de la información durante la vigencia 2026.

En este sentido, el plan comprende:

- ✓ ***Procesos institucionales:*** Aplica a todos los procesos misionales, estratégicos, de apoyo y de evaluación de EDUR, incluyendo aquellos relacionados con planeación, ejecución de proyectos, gestión administrativa, financiera, contractual, jurídica, documental, tecnológica y de atención a la ciudadanía.
- ✓ ***Activos de información:*** Incluye toda la información generada, recibida, administrada o custodiada por EDUR, independientemente de su formato o medio, tales como documentos físicos, archivos digitales, bases de datos, correos electrónicos, registros audiovisuales, información verbal, aplicaciones y sistemas de información.
- ✓ ***Datos personales y sensibles:*** Cubre el tratamiento de datos personales de ciudadanos, usuarios, funcionarios, contratistas, proveedores y terceros, incluyendo datos públicos, privados, semiprivados y sensibles, conforme a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- ✓ ***Infraestructura tecnológica y documental:*** Abarca la infraestructura tecnológica (hardware, software, redes, servidores, equipos de cómputo, dispositivos de almacenamiento) y la infraestructura documental (archivos físicos, expedientes, depósitos documentales), así como los controles asociados a su administración y seguridad.
- ✓ ***Talento humano y terceros:*** Aplica a todos los funcionarios, contratistas, proveedores, consultores y terceros que, en el ejercicio de sus funciones o actividades contractuales, tengan acceso, directo o indirecto.

6. MARCO NORMATIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa de Desarrollo Urbano y Rural – EDUR se formula y ejecuta en concordancia con el marco constitucional, legal, reglamentario y técnico vigente en Colombia, así como con lineamientos y buenas prácticas nacionales e internacionales en materia de seguridad de la información, protección de datos personales, gestión documental y control interno.

6.1 Normatividad constitucional y legal

- ✓ Constitución Política de Colombia – Artículo 15: Reconoce el derecho fundamental al habeas data, la intimidad personal y familiar, y el buen nombre, así como la obligación de las entidades públicas de proteger la información personal y garantizar su adecuado tratamiento.
- ✓ Ley 1581 de 2012: Establece el régimen general de protección de datos personales en Colombia, definiendo principios, derechos de los titulares, deberes de los responsables y encargados del tratamiento, y medidas de seguridad aplicables.
- ✓ Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012, estableciendo disposiciones sobre autorizaciones, políticas de tratamiento de la información y ejercicio de los derechos de los titulares.
- ✓ Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que compila normas relacionadas con la protección de datos personales y su aplicación por parte de entidades públicas y privadas.
- ✓ Ley 1266 de 2008: Regula el habeas data financiero, crediticio, comercial y de servicios, aplicable al tratamiento de información financiera y crediticia.

- ✓ Ley 1712 de 2014: Ley de Transparencia y Acceso a la Información Pública Nacional, que establece obligaciones relacionadas con la disponibilidad, protección y reserva de la información pública.
- ✓ Ley 594 de 2000: Ley General de Archivos, que define principios y responsabilidades para la organización, conservación, acceso y disposición final de los documentos de archivo.

6.2 Normatividad en gestión pública y control interno

- ✓ Modelo Integrado de Planeación y Gestión – MIPG: Marco de referencia para la gestión pública, que incorpora la seguridad de la información y la protección de datos personales dentro de la Dimensión de Control Interno y la Dimensión de Gestión de la Información.
- ✓ Ley 87 de 1993: Establece las normas para el ejercicio del control interno en las entidades del Estado, incluyendo la gestión de riesgos y la protección de los activos institucionales.
- ✓ Guía para la Administración del Riesgo – DAFP: Orienta la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos institucionales.

6.3 Política y lineamientos en seguridad digital

- ✓ CONPES 3854 de 2016: Define la Política Nacional de Seguridad Digital, orientada a la gestión de riesgos digitales, la protección de activos de información y la resiliencia institucional frente a amenazas cibernéticas.
- ✓ Lineamientos de Gobierno Digital: Emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientan la

gestión segura de la información, la interoperabilidad y el uso responsable de las tecnologías.

6.4 Normas técnicas y buenas prácticas internacionales (referencia)

- ✓ ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información – requisitos para establecer, implementar y mantener controles de seguridad.

- ✓ ISO/IEC 27002: Código de buenas prácticas para los controles de seguridad de la información.
- ✓ ISO/IEC 27005: Gestión del riesgo de seguridad de la información.
- ✓ ISO/IEC 27701: Extensión para la gestión de la privacidad de la información y protección de datos personales.

6.5 Gobierno Digital e Interoperabilidad

- ✓ Decreto 1008 de 2018: Por el cual se establecen los lineamientos de la Política de Gobierno Digital, integrando el Modelo de Seguridad y Privacidad de la Información (MSPI) como referente obligatorio para la gestión de riesgos de seguridad de la información en las entidades públicas.
- ✓ Lineamientos de Interoperabilidad del Estado Colombiano Orientan el intercambio seguro de información entre entidades públicas, garantizando estándares de confidencialidad, integridad, disponibilidad y trazabilidad de los datos compartidos.
- ✓ ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio Establece los requisitos para proteger y recuperar los procesos críticos ante incidentes que afecten la disponibilidad de la información y los sistemas tecnológicos.

El cumplimiento de este marco normativo y técnico constituye un elemento esencial para la correcta implementación del presente plan, garantizando que las acciones

definidas se desarrollen de manera coherente con los principios de legalidad, responsabilidad, transparencia, seguridad y mejora continua durante la vigencia 2026.

7. DEFINICIONES

Para efectos del presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026, se adoptan las siguientes definiciones y conceptos operativos, en concordancia con los estándares nacionales e internacionales en materia de gestión del riesgo y seguridad de la información:

- ✓ ***Activo de Información***

Cualquier dato, documento, sistema, registro, medio físico o digital, o infraestructura tecnológica que contenga, procese o soporte información relevante para el cumplimiento de los objetivos institucionales de la EDUR.

Los activos de información incluyen, entre otros: bases de datos de beneficiarios, expedientes técnicos de proyectos, documentos financieros y contractuales, sistemas de información, aplicaciones corporativas, correos institucionales y dispositivos electrónicos.

- ✓ ***Amenaza***

Situación, evento o acción —intencional o accidental— que puede explotar una vulnerabilidad y causar daño o pérdida a los activos de información de la entidad.

Ejemplos de amenazas incluyen: ataques informáticos, robo de información, fallas eléctricas, errores humanos, pérdida de dispositivos, accesos no autorizados, incendios o desastres naturales.

- ✓ ***Autenticidad***

Propiedad que garantiza que la identidad de un usuario, sistema o fuente de información sea verificada y legítima. Asegura que los datos y transacciones provienen de fuentes válidas y no han sido falsificados o manipulados.

- ✓ ***Confidencialidad***

Principio que garantiza que la información solo sea accesible a personas, sistemas o procesos debidamente autorizados. Su vulneración puede ocasionar pérdida de confianza institucional, sanciones legales y afectación a los derechos de los ciudadanos.

- ✓ ***Continuidad del Negocio***

Capacidad de la organización para mantener o restablecer sus operaciones críticas dentro de plazos aceptables tras la ocurrencia de un incidente que afecte la disponibilidad de sus recursos tecnológicos, humanos o físicos.

- ✓ ***Disponibilidad***

Condición que asegura que la información, los sistemas y los servicios tecnológicos estén accesibles y operativos cuando los usuarios autorizados los necesiten. Es fundamental para garantizar la prestación continua de los servicios institucionales de la EDUR.

- ✓ ***Gestión del Riesgo***

Proceso sistemático de identificar, analizar, valorar, tratar y monitorear los riesgos que pueden afectar el cumplimiento de los objetivos institucionales. Comprende la adopción de decisiones fundamentadas para reducir la probabilidad o el impacto de los eventos adversos.

- ✓ ***Impacto***

Consecuencia o efecto que la materialización de un riesgo puede generar sobre los objetivos, procesos, activos o la imagen institucional. En el contexto de la EDUR, el impacto puede ser operativo, financiero, reputacional, jurídico o social.

- ✓ ***Integridad***

Propiedad que garantiza que la información no ha sido alterada, modificada o destruida de manera no autorizada. Preservar la integridad asegura que los datos sean exactos, completos y confiables durante todo su ciclo de vida.

- ✓ ***Nivel de Riesgo***

Resultado de la combinación entre la probabilidad de ocurrencia y el impacto del riesgo. Se clasifica usualmente en niveles bajo, moderado, alto y extremo, para priorizar las acciones de tratamiento y control.

- ✓ ***Plan de Tratamiento del Riesgo***

Documento que define las acciones específicas, responsables, recursos y plazos establecidos para mitigar, reducir o eliminar los riesgos identificados en la organización. En la EDUR, este plan integra las acciones de todos los procesos institucionales y se actualiza anualmente.

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

Derecho y principio que protege los datos personales frente a su uso no autorizado, garantizando que sean recolectados, almacenados y tratados conforme a los fines institucionales y la normativa vigente (Ley 1581 de 2012 y Decreto 1377 de 2013).

- ✓ ***Probabilidad***

Medida que expresa la posibilidad de ocurrencia de un riesgo en un periodo determinado. Se evalúa según la exposición, el historial, las condiciones tecnológicas, humanas y ambientales de los procesos institucionales.

- ✓ ***Riesgo***

Efecto de la incertidumbre sobre los objetivos institucionales, causado por la posibilidad de que una amenaza explote una vulnerabilidad en un activo de información.

El riesgo puede tener consecuencias negativas (daño, pérdida, sanción) o positivas (identificación de oportunidades de mejora).

- ✓ ***Seguridad de la Información***

Conjunto de políticas, procedimientos, prácticas y herramientas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información institucional, así como la autenticidad, trazabilidad y responsabilidad de los actores que la gestionan.

- ✓ ***Trazabilidad***

Capacidad de rastrear y reconstruir el historial de una acción, evento o transacción de información desde su origen hasta su destino final, garantizando la transparencia, control y rendición de cuentas.

Tratamiento del Riesgo

Conjunto de medidas técnicas, administrativas o de gestión adoptadas para modificar el nivel de riesgo. Puede implicar acciones de mitigación, transferencia, aceptación o eliminación del riesgo, según su naturaleza y magnitud.

- ✓ ***Vulnerabilidad***

Debilidad o falla presente en los procesos, sistemas, personas o infraestructura que puede ser explotada por una amenaza para afectar la información o los servicios institucionales.

En la EDUR, las vulnerabilidades pueden originarse en configuraciones inseguras, falta de controles de acceso, desconocimiento de políticas, errores humanos o ausencia de procedimientos documentados.

8. METODOLOGIA DE GESTION DEL RIESGO

La Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR, en cumplimiento del Decreto 612 de 2018, adopta una metodología integral para la gestión del riesgo de seguridad y privacidad de la información, orientada a la protección de los activos institucionales, la continuidad de la operación y el cumplimiento normativo.

Esta metodología se fundamenta en el ciclo de mejora continua (PHVA – Planear, Hacer, Verificar, Actuar), integrando los principios y fases establecidas en las normas ISO 31000:2018 e ISO 27005:2022, y en la Guía para la Administración del Riesgo y Diseño de Controles del DAFP.

El proceso metodológico comprende cinco etapas:

1. Identificación
2. Análisis
3. Valoración
4. Tratamiento
5. Seguimiento y monitoreo

1. Identificación del Riesgo

El objetivo de esta fase es reconocer y registrar de manera sistemática los riesgos potenciales que pueden afectar la seguridad y privacidad de la información administrada por la EDUR.

Actividades principales:

- ✓ Levantamiento de información sobre procesos, activos de información, sistemas y procedimientos.
- ✓ Identificación de amenazas, vulnerabilidades y activos críticos.

- ✓ Determinación de fuentes de riesgo internas y externas (humanas, tecnológicas, físicas, legales o ambientales).
- ✓ Registro de los riesgos en la Matriz Institucional de Riesgos de Seguridad y Privacidad de la Información.

Resultados esperados:

- ✓ Listado consolidado de riesgos por proceso.
- ✓ Inventario de activos de información clasificados por nivel de criticidad.
- ✓ Mapeo de amenazas y vulnerabilidades relevantes para la EDUR.

2. Análisis del riesgo

El propósito de esta fase es evaluar las causas, consecuencias y condiciones de exposición que determinan el comportamiento de cada riesgo identificado.

Actividades principales:

- ✓ Determinar la probabilidad de ocurrencia de cada riesgo, con base en la frecuencia histórica, exposición, debilidades de control y nivel de dependencia tecnológica.
- ✓ Establecer el impacto o efecto potencial sobre los objetivos institucionales (operativo, financiero, jurídico, reputacional o social).
- ✓ Evaluar los controles existentes (tecnológicos, administrativos o físicos) y su nivel de eficacia.

Herramientas recomendadas:

- ✓ Matriz de análisis de probabilidad e impacto.
- ✓ Escalas cualitativas y cuantitativas.
- ✓ Entrevistas con líderes de proceso y personal técnico.

Resultados esperados:

- ✓ Determinación de la probabilidad e impacto de cada riesgo.

- ✓ Estimación del nivel de exposición actual (riesgo inherente).
- ✓ Identificación de brechas en los controles existentes.

3. *Valoración del riesgo*

Esta fase busca establecer la magnitud del riesgo y priorizar las acciones de tratamiento, comparando el nivel de riesgo identificado con los criterios de aceptación institucional.

Actividades principales:

- ✓ Calcular el nivel de riesgo residual considerando la eficacia de los controles implementados.
- ✓ Clasificar los riesgos en niveles (Bajo, Moderado, Alto, Extremo) según la matriz de riesgo institucional.
- ✓ Priorizar los riesgos que requieren tratamiento inmediato, seguimiento o aceptación formal.
- ✓ Validar los resultados con los líderes de proceso y el área de Planeación.

Resultados esperados:

- ✓ Matriz consolidada de valoración de riesgos.
- ✓ Priorización de riesgos significativos.
- ✓ Documentación de decisiones de aceptación o tratamiento.

4. *Tratamiento del riesgo*

En esta etapa se definen las acciones concretas para modificar el nivel de riesgo, mediante estrategias que reduzcan la probabilidad de ocurrencia o el impacto potencial.

Opciones de tratamiento:

- ✓ Mitigar: Implementar controles o medidas que reduzcan la probabilidad o el impacto.
- ✓ Evitar: Eliminar la causa del riesgo suspendiendo o modificando el proceso que lo genera.
- ✓ Transferir: Compartir o delegar la gestión del riesgo mediante contratos, seguros o acuerdos con terceros.
- ✓ Aceptar: Reconocer el riesgo y mantenerlo bajo vigilancia cuando su nivel sea bajo o el costo de mitigación sea superior al beneficio esperado.

Actividades principales:

- ✓ Definir el plan de acción y los controles asociados a cada riesgo priorizado.
- ✓ Establecer responsables, recursos, plazos y metas verificables.
- ✓ Documentar el tratamiento en el Plan de Acción Institucional y en la Matriz de Riesgos de Seguridad y Privacidad de la Información.

Resultados esperados:

- ✓ Plan de tratamiento de riesgos aprobado.
- ✓ Controles definidos y asignados por proceso.
- ✓ Evidencias de implementación y seguimiento.

5. Seguimiento y monitoreo

Esta fase busca verificar la eficacia de los controles implementados y asegurar la mejora continua del sistema de gestión de riesgos.

Actividades principales:

- ✓ Monitorear periódicamente los riesgos y la efectividad de las acciones de mitigación.
- ✓ Actualizar la matriz de riesgos y los informes de seguimiento.
- ✓ Reportar los resultados al Comité de Seguridad de la Información y a la Oficina de Planeación.
- ✓ Identificar nuevas amenazas, cambios en el entorno tecnológico o debilidades emergentes.
- ✓ Promover la retroalimentación y mejora continua.

Herramientas de seguimiento:

- ✓ Indicadores de gestión y desempeño.
- ✓ Auditorías internas.
- ✓ Evaluaciones técnicas de vulnerabilidades.
- ✓ Informes de incidentes y lecciones aprendidas.

Resultados esperados:

- ✓ Evaluación documentada del nivel de riesgo residual.
- ✓ Actualización continua del plan y los controles.
- ✓ Evidencia de mejora continua y madurez institucional en seguridad de la información.

6. Cronograma de implementación 2026

Actividad	T1	T2	T3	T4
Actualización matriz de riesgos	✓		✓	
Implementación controles R1–R5	✓	✓		
Capacitación institucional	✓		✓	

Evaluación de proveedores		✓		✓
Pruebas de restauración de backups	✓		✓	
Auditoría interna		✓		✓
Actualización de políticas	✓			✓

7. Integración con el MIPG y el control interno

La metodología se articula con la dimensión de Gestión del Riesgo del MIPG, y con los subsistemas de control estratégico, operativo y de evaluación independiente.

Esto garantiza que la gestión de riesgos de seguridad de la información no sea un proceso aislado, sino una práctica transversal que apoya la toma de decisiones, la rendición de cuentas y la transparencia institucional.

8. Responsabilidades metodológicas

- ✓ Oficina de Planeación: Coordina la aplicación de la metodología, consolida la información de riesgos y reporta los resultados a la Gerencia General.
- ✓ Área TIC: Ejecuta el tratamiento de los riesgos tecnológicos y mantiene los registros de incidentes y vulnerabilidades.
- ✓ Líderes de Proceso: Identifican y reportan los riesgos propios de su gestión y verifican la eficacia de los controles aplicados.
- ✓ Oficina de Control Interno: Evalúa la adherencia metodológica y la efectividad del sistema de gestión de riesgos.

9. IDENTIFICACION DE RIESGOS PRINCIPALES

Código	Riesgo
R1	Acceso no autorizado a bases de datos de ciudadanos
R2	Pérdida o fuga de información sensible
R3	Uso indebido de datos personales
R4	Ataques informáticos (malware, ransomware, phishing)
R5	Falta de copias de seguridad y recuperación de la información
R6	Manejo inadecuado de archivos físicos
R7	Desconocimiento normativo por parte del personal
R8	Proveedores sin controles adecuados de seguridad
R9	Incidentes de seguridad no reportados oportunamente
R10	Falta de actualización de políticas de seguridad y privacidad

10. MATRIZ DE VALORACIÓN DE RIESGOS

Riesgo	Probabilidad	Impacto	Nivel Inherente	Controles Clave	Nivel Residual Esperado
R1 Acceso no autorizado	Alta	Alto	Extremo	Autenticación fuerte, roles, monitoreo	Moderado
R2 Fuga de información	Media	Alto	Alto	Clasificación, cifrado, NDA	Bajo
R3 Uso indebido de datos	Media	Alto	Alto	Política datos personales, autorizaciones	Bajo

R4 Ataques informáticos	Alta	Alto	Extremo	Antivirus, firewall, parches	Moderado
R5 Falta de backups	Media	Alto	Alto	Política de copias, pruebas restauración	Bajo
R6 Manejo archivos físicos	Media	Medio	Moderado	TRD, control de acceso	Bajo
R7 Desconocimiento normativo	Alta	Medio	Alto	Capacitación	Bajo
R8 Proveedores inseguros	Media	Alto	Alto	Cláusulas seguridad	Moderado
R9 Incidentes no reportados	Media	Alto	Alto	Procedimiento incidentes	Bajo
R10 Políticas desactualizadas	Media	Medio	Moderado	Actualización anual	Bajo

11. PLAN DE TRATAMIENTO DE RIESGOS

Para cada riesgo identificado, EDUR define acciones de tratamiento orientadas a mitigar, evitar o transferir el riesgo, mediante la implementación de controles técnicos, administrativos y organizacionales, tales como:

- ✓ Control de accesos y autenticación por roles.
- ✓ Clasificación y cifrado de la información sensible.
- ✓ Políticas de tratamiento de datos personales y confidencialidad.
- ✓ Copias de seguridad periódicas y pruebas de restauración.
- ✓ Gestión de incidentes de seguridad de la información.
- ✓ Capacitación y sensibilización del talento humano.
- ✓ Evaluación y control de proveedores y terceros.

Riesgo R1: Acceso no autorizado a la información

Tratamiento: Mitigar

Controles:

- Implementar control de accesos por roles.
- Autenticación fuerte (contraseñas seguras, doble factor).
- Registro y monitoreo de accesos.
- Principio de mínimo privilegio.

Riesgo R2: Pérdida o fuga de información

Tratamiento: Mitigar

Controles:

- Clasificación de la información.
- Cifrado de información sensible.
- Políticas de uso de dispositivos externos.
- Acuerdos de confidencialidad.

Riesgo R3: Uso indebido de datos personales

Tratamiento: Mitigar / Evitar

Controles:

- Política de Tratamiento de Datos Personales.
- Autorizaciones explícitas de los titulares.
- Registro de bases de datos ante la SIC.
- Capacitación en Ley 1581 de 2012.

Riesgo R4: Ataques informáticos

Tratamiento: Mitigar

Controles:

- Antivirus y firewall actualizados.
- Copias de seguridad periódicas.

- Simulacros de incidentes de ciberseguridad.
- Actualización de sistemas y parches.

Riesgo R5: Falta de copias de seguridad

Tratamiento: Mitigar

Controles:

- Política de backups.
- Pruebas periódicas de restauración.
- Almacenamiento externo y seguro.

Riesgo R6: Manejo inadecuado de archivos físicos

Tratamiento: Mitigar

Controles:

- Tablas de Retención Documental.
- Control de acceso a archivos.
- Eliminación segura de documentos.

Riesgo R7: Desconocimiento normativo

Tratamiento: Mitigar

Controles:

- Plan anual de capacitación.
- Inducción y reinducción en seguridad de la información.
- Divulgación de políticas institucionales.

Riesgo R8: Proveedores sin controles adecuados

Tratamiento: Mitigar / Transferir

Controles:

- Cláusulas contractuales de seguridad.
- Evaluación de proveedores.
- Acuerdos de confidencialidad.

Riesgo R9: Incidentes no reportados

Tratamiento: Mitigar

Controles:

- Procedimiento de gestión de incidentes.
- Canales de reporte definidos.
- Comité de Seguridad de la Información.

Riesgo R10: Falta de políticas actualizadas

Tratamiento: Evitar

Controles:

- Actualización anual de políticas.
- Aprobación por la alta dirección.
- Publicación y divulgación interna.

12. ARTICULACIÓN CON CONTINUIDAD DEL NEGOCIO

Los riesgos asociados a disponibilidad de la información y fallas tecnológicas (R4 y R5) se articularán con:

- Plan de Continuidad del Negocio (PCN)
- Plan de Recuperación ante Desastres (DRP)
- Pruebas periódicas de restauración de servicios críticos

Esto asegura que el tratamiento del riesgo no solo reduzca amenazas, sino que garantice la resiliencia institucional.

13. ROLES Y RESPONSABILIDADES

- ✓ ***Alta Dirección:*** Aprobar el plan y garantizar los recursos para su implementación.
- ✓ ***Responsable de Seguridad de la Información:*** Coordinar y supervisar la ejecución del plan.

- ✓ ***Oficial de Protección de Datos:*** Velar por el cumplimiento de la Ley 1581 de 2012.
- ✓ ***Funcionarios y Contratistas:*** Cumplir las políticas y reportar incidentes.
- ✓ ***Control Interno:*** Evaluar, auditar y hacer seguimiento al cumplimiento del plan.

14. INDICADORES DE SEGUIMIENTO Y MEDICION

El seguimiento y la medición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026 son elementos fundamentales para garantizar la eficacia, coherencia y mejora continua del proceso de gestión del riesgo dentro de la EDUR

Esta sección define los mecanismos, responsables, herramientas e indicadores que permiten monitorear de forma sistemática el cumplimiento de las acciones propuestas, verificar la reducción del nivel de exposición al riesgo y asegurar la alineación del plan con los objetivos estratégicos, normativos y operativos de la entidad.

1) Objetivos del Seguimiento y Medición

- ✓ Verificar el grado de avance de las actividades y controles definidos en el plan de tratamiento.
- ✓ Evaluar la efectividad de las medidas implementadas para reducir la probabilidad e impacto de los riesgos.
- ✓ Identificar desviaciones, retrasos o fallas en la ejecución que requieran acciones correctivas.
- ✓ Garantizar la trazabilidad de la gestión del riesgo frente a auditorías internas y externas.
- ✓ Aportar información para la toma de decisiones por parte de la Gerencia, el Área TIC, Planeación y Control Interno.

- ✓ Fomentar una cultura de autocontrol, responsabilidad y mejora continua.

2) *Mecanismos de Seguimiento*

La EDUR implementará los siguientes mecanismos institucionales para monitorear el plan:

a) *Informes de Avance Trimestral*

El Área TIC y los líderes de proceso reportarán trimestralmente a la Oficina de Planeación el avance de los controles y actividades programadas.

Los informes incluirán:

- ✓ % de ejecución del plan.
- ✓ Controles implementados y pendientes.
- ✓ Riesgos con variaciones en su nivel de exposición.
- ✓ Necesidades de ajuste o reasignación de recursos.

b) *Actualización semestral de la Matriz de Riesgos*

Cada seis meses se actualizarán los valores de probabilidad, impacto y nivel residual, para determinar si los controles aplicados están reduciendo efectivamente los riesgos.

c) *Comité de Seguridad de la Información*

Aunque no requiere actas explícitas, se recomienda mantener reuniones periódicas de análisis técnico con:

- ✓ Oficina de Planeación
- ✓ Área TIC
- ✓ Control Interno
- ✓ Líderes de proceso

Estas reuniones permiten revisar el estado del plan y tomar decisiones estratégicas.

d) Auditorías Internas

La Oficina de Control Interno evaluará:

- ✓ Cumplimiento de la metodología de gestión del riesgo.
- ✓ Eficacia de los controles implementados.
- ✓ Conformidad con la normativa nacional de seguridad digital.

e) Evaluaciones Técnicas de Seguridad

Cuando sea aplicable, la EDUR podrá realizar:

- ✓ Pruebas de vulnerabilidad internas.
- ✓ Análisis técnico de brechas.
- ✓ Verificación de configuraciones y políticas de acceso.

Estas evaluaciones aportan evidencia objetiva para la toma de decisiones.

Indicadores de Seguimiento del Plan

Indicador	Fórmula	Meta
Incidentes reportados oportunamente	Incidentes reportados / Total incidentes	≥ 90%
Riesgos con tratamiento activo	Riesgos con plan implementado / Total riesgos	100%
Cumplimiento de copias de seguridad	Copias realizadas / Copias programadas	≥ 95%
Personal capacitado	Funcionarios capacitados / Total funcionarios	≥ 90%
Evaluaciones de proveedores realizadas	Proveedores evaluados / Total proveedores críticos	100%

15. SEGUIMIENTO Y MEJORA CONTINUA

El presente plan será objeto de:

- ✓ Seguimiento periódico durante la vigencia 2026.
- ✓ Revisión y actualización anual o cuando se presenten cambios normativos, tecnológicos u organizacionales.
- ✓ Evaluación a través de auditorías internas y externas, en el marco del Sistema de Control Interno.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026 se consolida como un instrumento estratégico fundamental para la Empresa de Desarrollo Territorial, Urbano y Rural de Risaralda – EDUR, orientado a fortalecer de manera integral la gestión institucional, asegurar la protección de la información y promover un entorno digital confiable que soporte la operación, la toma de decisiones y el cumplimiento de la misión.

La seguridad de la información, entendida como un pilar transversal del funcionamiento organizacional, se convierte en un habilitador clave para el desarrollo urbano y rural del territorio. Por ello, este plan articula de manera coherente los lineamientos de la política pública, las mejores prácticas internacionales, la infraestructura tecnológica disponible y las necesidades reales de la EDUR, con el fin de anticipar, mitigar y gestionar efectivamente los riesgos que puedan afectar los procesos misionales y de apoyo.

Al integrar la gestión del riesgo con la planeación institucional, la EDUR avanza hacia un modelo de operación basado en la anticipación, la resiliencia y la mejora continua, donde cada proceso y dependencia contribuye activamente a la protección de los activos de información, la continuidad del servicio, la transparencia y la confianza ciudadana. El plan establece un conjunto claro de acciones, responsables, recursos, indicadores y mecanismos de seguimiento que permitirán hacer trazable y verificable su implementación durante la vigencia.

Asimismo, este esfuerzo institucional no solo busca evitar incidentes o reducir vulnerabilidades, sino también potenciar el uso responsable, seguro y estratégico de la información como un activo de alto valor para la planeación, ejecución y

evaluación de los proyectos que impulsa la entidad. La correcta protección de la información se refleja en mejores decisiones, mayor eficiencia operativa y un servicio público más confiable para la ciudadanía y los territorios donde la EDUR tiene presencia.

De igual forma, la implementación del plan permitirá fortalecer la cultura organizacional en torno a la seguridad digital, empoderando a funcionarios, directivos y contratistas para que adopten buenas prácticas, comprendan su rol dentro del Sistema de Seguridad de la Información y participen activamente en la prevención de riesgos, incidentes y contingencias.

Con este plan, la EDUR reafirma su compromiso con una gestión pública moderna, transparente y alineada con los principios del Gobierno Digital, entendiendo que la ciberseguridad, la protección de datos personales y el manejo adecuado de la información son elementos esenciales para consolidar un modelo institucional más sólido, confiable y resiliente.

Finalmente, el plan aquí presentado será objeto de seguimiento permanente y actualización periódica, permitiendo que la entidad se adapte a los cambios del contexto tecnológico, normativo y operativo. La visión estratégica de la EDUR se mantiene firme: avanzar hacia una gestión integral del riesgo que asegure una infraestructura digital robusta y contribuya al fortalecimiento de la gobernanza territorial y la excelencia institucional.

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