EDRU

ALCALDÍA DE
SANTIAGO DE CALI

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

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

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

CONSIDERANDO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Estratégico:

- Proceso Direccionamiento y Planeación Institucional – Subproceso Planeación Institucional.

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

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

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

Que, conforme a lo anteriormente expuesto,

RESUELVE:

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

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

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

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

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

VIF

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

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

COMUNÍQUESE Y CÚMPLASE

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

MARIA ALEXANDRA PACHECO MUÑOZ
Gerente General EDRU E.I.C.E.
Empresa de Desarrollo y Renovación Urbana - EDRU E.I.C.E.

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

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

2025

TABLA DE CONTENIDO

INTRODUCCIÓN

La Empresa de Desarrollo y Renovación Urbana (EDRU) reconoce que la información constituye un activo estratégico esencial para el cumplimiento de su misión institucional. En este sentido, el presente plan tiene como propósito establecer las acciones necesarias para mitigar los riesgos identificados en materia de seguridad y privacidad de la información, en cumplimiento de la Ley Estatutaria 1581 DE 2012 (octubre 17) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022, la Ley 1266 de 2008, el Marco de Ciberseguridad y Privacidad del MinTIC, y de la norma ISO/IEC 27001:2022.

Este plan se fundamenta en el documento FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD de la Información, versión vigente aprobada por el comité institucional de gestión y desempeño. Asimismo, se encuentra alineado con la POL-DPI-01-03 - POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de la entidad, garantizando coherencia, trazabilidad documental y respaldo para procesos de auditoría interna y externa.

1 OBJETIVO

La Empresa de Desarrollo y Renovación Urbana (EDRU) reconoce que la información constituye un activo estratégico esencial para el cumplimiento de su misión institucional. En este sentido, el presente plan tiene como propósito establecer las acciones necesarias para mitigar los riesgos identificados en materia de seguridad y privacidad de la información, en cumplimiento de la Ley Estatutaria 1581 DE 2012 (octubre 17) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011.

Ver Decreto 255 de 2022, la Ley 1266 de 2008, el Marco de Ciberseguridad y Privacidad del MinTIC, y de la norma ISO/IEC 27001:2022.

Este plan se fundamenta en el documento FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD de la Información, versión vigente aprobada por el comité institucional de gestión y desempeño. Asimismo, se encuentra alineado con la POL-DPI-01-03 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD, garantizando coherencia, trazabilidad documental y respaldo para procesos de auditoría interna y externa.

2 ALCANCE

El presente Plan aplica a todos los riesgos de seguridad y privacidad documentados en la EDRU E.I.C.E., establece las acciones requeridas para su tratamiento y define los controles, responsables y plazos para su implementación, seguimiento y mejora continua, en cumplimiento con ISO 27001:2022, ISO 27005:2022 y la normativa de protección de datos personales vigente.

Este Plan busca garantizar que los servicios tecnológicos y de comunicaciones de la Entidad se presten con calidad, confiabilidad, confidencialidad, integridad, disponibilidad y eficiencia, promoviendo un uso adecuado y prioritario de los recursos institucionales para asegurar su correcta funcionalidad y un nivel óptimo de seguridad.

3 RESPONSABILIDAD

Son responsables de la ejecución, actualización y supervisión de este Plan:

Gestión Administrativa, Documental y TIC.

- Mantener el presente Plan actualizado.
- Administrar la Matriz de Riesgos y el registro de acciones de tratamiento.
- Consolidar evidencias de implementación.
- Coordinar actividades con todas las áreas involucradas.
- Preparar reportes para auditoría interna y externa.

Área TIC.

- Implementar los controles tecnológicos definidos en el Plan.
- Validar su efectividad operativa.
- Aportar registros técnicos y evidencia de implementación.

Propietarios del riesgo.

- Asegurar el cumplimiento de las acciones asignadas.
- Notificar cambios, incidencias y desviaciones.
- Proponer nuevos controles cuando corresponda.

Comité de seguridad de la información.

- Aprobar el Plan y sus modificaciones.
- Autorizar la aceptación del riesgo residual.
- Realizar revisiones periódicas de avance.

Gerencia General.

- Proveer recursos requeridos para su implementación.

4 TÉRMINOS Y DEFINICIONES

A efectos de este documento se adoptan las siguientes definiciones:

Acceso a la Información Pública: Derecho fundamental que tienen todas las personas de conocer sobre la existencia, solicitar y acceder a la información pública que se encuentre en posesión o bajo control de los sujetos obligados. (Ley 1712 de 2014, art. 4).

Activo de Información: Cualquier información, dato, documento, sistema, infraestructura, software, hardware, servicio, recurso tecnológico, conocimiento o medio que soporte operaciones institucionales y que posea valor para la organización. (ISO/IEC 27000:2018).

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños a un sistema, activo, proceso o a la organización. (ISO/IEC 27000:2018).

Apetito de riesgo: Nivel de riesgo aceptable para la organización sin necesidad de acciones adicionales.

Análisis de Riesgo: Proceso mediante el cual se comprende la naturaleza del riesgo y se determina el nivel de riesgo asociado, considerando la probabilidad de ocurrencia y el impacto. (ISO/IEC 27000:2018).

Autenticación: Proceso de verificación de la identidad de un usuario, sistema o entidad antes de autorizar el acceso a información, sistemas o servicios. (ISO/IEC 27000:2018).

Autorización: Proceso mediante el cual se otorgan permisos o niveles de acceso a usuarios, roles, sistemas o procesos, de acuerdo con sus funciones y responsabilidades.

Clasificación de la Información: Proceso mediante el cual se categoriza la información según su nivel de sensibilidad y criticidad, definiendo criterios de acceso, tratamiento y protección (p.e., pública, reservada, clasificada, confidencial). (Ley 1712 de 2014).
Confidencialidad: Propiedad mediante la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO/IEC 27000:2022).

Ciberseguridad: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, incluyendo medidas para prevenir, detectar y responder a ciberataques. (ISO/IEC 27032:2023).

Control: Políticas, procedimientos, prácticas o estructuras organizativas diseñadas para mantener los riesgos de seguridad de la información dentro del nivel aceptado por la organización. También es denominado salvaguarda o contramedida. En términos simples, es una medida que modifica o reduce el riesgo. (ISO/IEC 27000:2022).

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).

Dato Sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (salud, biometría, orientación sexual, etc.). (Ley 1581 de 2012).

Disponibilidad: Propiedad de que la información y los sistemas estén accesibles y utilizables por personas, procesos o aplicaciones autorizadas en el momento que se requieran. Garantiza continuidad operativa y acceso oportuno. (ISO/IEC 27000:2022).
Incidente de Seguridad de la Información: Evento o serie de eventos que comprometen o tienen el potencial de comprometer la confidencialidad, integridad o disponibilidad de los activos de información. (ISO/IEC 27000:2022).

Impacto: Consecuencia que tendría la materialización de un riesgo sobre la organización.
Integridad: Propiedad que salvaguarda la exactitud, completitud y consistencia de la información y de los métodos de procesamiento asociados, evitando su modificación no autorizada. (ISO/IEC 27000:2022).
Información Clasificada y Reservada: Tipos de información cuya divulgación puede poner en riesgo derechos, intereses públicos o privados, y cuya publicación se restringe conforme a la Ley 1712 de 2014.

Política: Declaración de alto nivel que establece la postura, lineamientos y directrices de la organización frente a un tema específico, orientando la toma de decisiones y el cumplimiento de objetivos institucionales.

Probabilidad: Posibilidad de ocurrencia estimada del riesgo.

Privacidad: Derecho que tienen los titulares de la información en relación con el tratamiento de sus datos personales y de la información clasificada que han entregado o que reposan en la entidad. Implica la obligación correlativa de la organización de proteger dicha información conforme al marco legal vigente, incluyendo la Ley 1581 de 2012, su decreto reglamentario y el Manual de Gobierno Digital (GEL).

Riesgo de Seguridad de la Información: Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo sobre un activo de información. (ISO/IEC 27000:2022).

Riesgo residual: Nivel de riesgo que permanece después de la implementación de controles.
Tratamiento del Riesgo: Proceso para seleccionar e implementar medidas destinadas a modificar los riesgos: evitarlos, mitigarlos, transferirlos o aceptarlos. (ISO/IEC 27005:2022).

Trazabilidad: Capacidad para rastrear actividades, accesos, cambios, movimientos o tratamientos realizados sobre la información, sistemas o procesos mediante registros, logs o auditorías.

Vulnerabilidad: Debilidad o falencia dentro de un activo, proceso, sistema o control que puede ser explotada por una amenaza. (ISO/IEC 27000:2022).

Sistema de Gestión de Seguridad de la Información – SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, procesos, procedimientos, planes, recursos y responsabilidades) que una organización implementa para establecer una política y objetivos de seguridad de la información, gestionarlos de manera sistemática y alcanzar su mejora continua. (ISO/IEC 27000:2022).

5 CONTENIDO

5.1 Metodología

La metodología aplicada para el tratamiento de riesgos se basa en los lineamientos de la norma ISO/IEC 27005:2022, ISO/IEC 27001:2022 (cláusula 6.1.3), el Modelo de Seguridad y Privacidad de la Información del MinTIC y los principios del programa de Gobierno Digital.

El proceso se estructura en las siguientes fases:

- Identificación del riesgo
- ✓ Identificación del activo
- ✓ Identificación del riesgo
- ✓ Identificación de amenaza
- ✓ Identificación de vulnerabilidad
- ✓ Relación con requisito legal

- Análisis del riesgo

✓ Determinación de impacto de probabilidad

✓ Método de evaluación cualitativa y semicuantitativa

- Valoración del riesgo

✓ Clasificación del riesgo según:

-probabilidad

-impacto

-apetito de riesgo institucional

- Definición de la acción de tratamiento
  - ✓ Mitigar
  - ✓ Evitar
  - ✓ Transferir
  - ✓ Aceptar
- Implementación del tratamiento
  - ✓ Implementación de controles
  - ✓ Obtención de evidencia
  - ✓ Documentación en matriz
- Determinación del riesgo residual
  - ✓ Nueva probabilidad
  - ✓ Nuevo impacto
  - ✓ Validación formal
- Seguimiento y evaluación de eficacia
  - ✓ KPIs
  - ✓ Indicadores
  - ✓ Verificación por comité
- Registro, trazabilidad y reporte
  - ✓ Actualización de matriz
  - ✓ Reporte periódico

- ✓ Registro de mantenimiento

5.2 Fase 1: Diagnóstico

5.2.1 Revisión de riesgos existentes:

- Consultar el inventario de activos de información- FOR-GDO-03-06 PLANILLA DE INVENTARIO DE ACTIVOS DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICAICONES - TIC
- Evaluar el mapa de riesgo anterior y sus impactos.
- Analizar los resultados de auditorías anteriores.

La Fase 1 comienza con la revisión de los riesgos existentes, mediante un análisis integral del entorno actual de seguridad de la información. Este proceso inicia con la consulta del inventario de activos de información, lo que permite identificar los recursos tecnológicos, físicos y lógicos que resultan críticos para la operación de la EDRU E.I.C.E.

A continuación, se analiza el mapa de riesgos previamente definido, evaluando tanto el impacto potencial como la vigencia de cada riesgo, en función del contexto organizacional y tecnológico actual. Posteriormente, se examinan los resultados de auditorías internas y externas realizadas en años anteriores, con el objetivo de determinar la efectividad de los controles implementados y de identificar hallazgos recurrentes o pendientes que requieran atención prioritaria.

Esta revisión constituye la base para la actualización del plan de tratamiento de riesgos, asegurando que las decisiones se fundamenten en información validada y se alineen con los principios de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Adicionalmente, se realizó un análisis de los incidentes de seguridad ocurridos durante el periodo anterior, identificando patrones recurrentes, vulnerabilidades explotadas y lecciones aprendidas.

Estos resultados permitieron retroalimentar la matriz de riesgos y fortalecer los planes de tratamiento asociados, priorizando las acciones correctivas y preventivas de manera estratégica.

5.2.2 Evaluación de controles implementados:

- Verificar si los controles actuales están alineados con los objetivos de seguridad (confidencialidad, integridad, disponibilidad).
- Medir la eficacia de controles técnicos como firewalls, DLP, backups automáticos y antivirus corporativos.
- Revisar la aplicación de controles organizacionales: políticas, capacitaciones, procedimientos.

Se lleva a cabo la evaluación de los controles actualmente implementados, con el propósito de verificar su adecuación y eficacia frente a los riesgos previamente identificados. El proceso inicia con la revisión del alineamiento de dichos controles con los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (CIA). Adicional se tienen definidos los siguientes controles:

- Metodología de Mapeo de Controles a Objetivos de Seguridad (CIA) – ISO 27001:2022

Para cada control seleccionado del Anexo A de la ISO/IEC 27001:2022 se realizó un análisis técnico orientado a determinar su contribución directa y/o indirecta a los objetivos de seguridad institucional definidos como Confidencialidad, Integridad y Disponibilidad (CIA).
Este mapeo se efectuó aplicando el siguiente criterio metodológico:

- ✓ Identificación del control ISO aplicable
  Según dominio, propósito y alcance.
- ✓ Definición del riesgo asociado
  Basado en la Matriz de Riesgos de Seguridad y Privacidad.

- ✓ Evaluación del aporte del control a la CIA
  Considerando:

  -Riesgo mitigado
  -Debilidad atendida
  -Tipo de protección proporcionada

- ✓ Asignación del objetivo principal de seguridad
  (C, I, D o combinación)

- ✓ Determinación del objetivo secundario
  cuando aplique

- ✓ Registro documental en matriz
  incluyendo evidencia operativa disponible.

Este proceso queda trazado en la Matriz de Controles, la cual forma parte de los anexos del presente plan.

Control ISO 27001	Riesgo Mitigado	Objetivo Principal CIA	Objetivo Secundario CIA	Evidencia
A.8.24 Copias de seguridad	Pérdida de información	Disponibilidad	Integridad	Registro de backups
A.5.17 Clasificación de la información	Fuga de datos sensibles	Confidencialidad	Integridad	POL-GDO-01
A.8.28 Protección contra malware	Ransomware	Integridad	Disponibilidad	Consola antivirus

- El control de doble autenticación (2FA) está alineado con la confidencialidad, para fortalecer los mecanismos de acceso seguro a la información. Por su parte, los procedimientos de respaldo (backups) impactan directamente la disponibilidad, asegurando la recuperación oportuna de los datos en caso de incidentes.

  Para ello, se analiza si los mecanismos técnicos y organizacionales en funcionamiento ofrecen una protección efectiva a los activos de información críticos para la operación de la EDRU E.I.C.E, asegurando que respondan de manera coherente a las amenazas y vulnerabilidades del entorno actual.

  En lo referente a los controles técnicos, su efectividad se evalúa a través de pruebas de funcionamiento, revisión de registros (logs) y análisis de reportes generados por herramientas especializadas como firewalls, sistemas de prevención de fuga de datos (DLP), soluciones antivirus corporativas y esquemas de respaldo automatizado. Asimismo, se verifica que estos controles estén actualizados, correctamente configurados y que brinden cobertura frente a los vectores de ataque más relevantes que evidencian el funcionamiento continuo y adecuado de los controles:

  - Firewalls: Revisión de reglas activas, detección de intentos de intrusión, escaneos de puertos y pruebas de penetración.
  - DLP (Data Loss Prevention): Verificar bloqueos o alertas de filtración de datos.
  - Backups: Validación de programación, verificación de restauración exitosa, pruebas periódicas.
  - Antivirus: Revisión de actualizaciones, informes de amenazas detectadas, cobertura en endpoints.
  - % de equipos con antivirus actualizado.
  - Tiempo medio de detección y respuesta a incidentes.
  - Éxito en restauración de copias de seguridad.

Por otro lado, se realiza una evaluación de los controles organizacionales, que abarca la existencia y aplicación de políticas internas, programas de concientización y capacitación en seguridad, así como la documentación y uso efectivo de procedimientos operativos que promuevan comportamientos seguros por parte del personal.

La evaluación integral permite identificar brechas de cumplimiento, oportunidades de mejora y fortalezas del sistema de seguridad, proporcionando insumos clave para definir acciones correctivas o preventivas en las siguientes fases del plan de tratamiento.

- Revisión documental: Se validan que las políticas estén formalmente aprobadas, publicadas, comunicadas y actualizadas conforme al ciclo de mejora continua.
- Capacitaciones: Implementación de un programa de concienciación y formación periódica.

- Medir el porcentaje de personal capacitado en temas de seguridad y privacidad de la información, con relación al total del personal objetivo definido.
- Procedimientos: Verificar que existan procedimientos formalizados para actividades críticas (gestión de incidentes, control de accesos, clasificación de información).

5.2.3 Identificación de nuevos riesgos:

Cambios tecnológicos: Se identifican nuevos riesgos derivados de la adopción o migración hacia entornos en la nube, el uso de dispositivos móviles, el trabajo remoto y la tercerización de servicios tecnológicos, los cuales pueden impactar la seguridad de la información y la continuidad de las operaciones institucionales.

Cambios normativos: Se identifican riesgos relacionados con la incorporación de nuevas leyes o reglamentaciones aplicables, particularmente aquellas asociadas a protección de datos personales (Ley 1581 de 2012, Decreto 1377 de 2013 y normatividad complementaria), que puedan generar incumplimientos o requerir ajustes en procesos internos.

Cambios operativos o estructurales: Se consideran reestructuraciones internas, tercerización de servicios e incorporación de nuevas tecnologías o procesos.
Detectar riesgos asociados: falta de capacitación, errores humanos o ausencia de controles adaptados al nuevo contexto de riesgos de la información.

Para la identificación de nuevos riesgos, la EDRU E.I.C.E emplea diversas herramientas como entrevistas estructuradas, encuestas, listas de verificación y análisis de incidentes, con el fin de detectar amenazas emergentes que puedan comprometer la seguridad de la información. Este proceso se complementa con la evaluación de factores de cambio relevantes, tales como avances tecnológicos (por ejemplo, migración a la nube o adopción de dispositivos móviles), modificaciones normativas y ajustes operativos que puedan impactar la seguridad de la información.

La aplicación de estos métodos permite mantener actualizado el panorama de riesgos, fortalecer la gestión preventiva y asegurar la trazabilidad necesaria para futuras auditorías y revisiones del Sistema de Gestión de Seguridad de la Información (SGSI).

5.3 Fase 2: Actualización.

5.3.1 Reevaluación de riesgos:

- Calcular la probabilidad e impacto con matrices.
- Priorizar riesgos con base en su nivel y en el apetito de riesgo definido por la EDRU E.I.C.E.

La reevaluación de los riesgos en la EDRU se realiza de forma periódica y estructurada, en cumplimiento de los lineamientos establecidos por la norma ISO/IEC 27001:2022, la ISO/IEC 27005:2022 y la Guía para la Gestión Integral del Riesgo de la Función Pública. Este proceso tiene como finalidad garantizar que los riesgos continúen gestionándose de manera adecuada, manteniendo su alineación con el contexto institucional, los cambios tecnológicos y los objetivos estratégicos.

Para ello, se aplican métodos de valoración cualitativa y semicuantitativa que permiten recalcular la probabilidad e impacto, considerando criterios como:

- Disponibilidad
- Integridad
- Confidencialidad
- Cumplimiento legal
- Impactos operativos, financieros, reputacionales y tecnológicos.

La reevaluación incorpora fuentes de información tales como resultados de auditorías internas y externas, cambios normativos, registro de incidentes, desempeño de controles y retroalimentación de líderes de proceso.

Este proceso incluye las siguientes actividades:

- Identificación de variaciones normativas, tecnológicas u operativas.
- Revisión del desempeño de controles establecidos.
- Cálculo actualizado de la probabilidad y el impacto.
- Determinación del nivel de riesgo resultante.
- Actualización del plan de tratamiento y sus acciones asociadas.
- Registro documental de los cambios e historial de versiones.

Este proceso incluye los siguientes pasos:

- Calcular la probabilidad e impacto de cada riesgo, utilizando la matriz de riesgos institucional.
- Priorizar los riesgos en función de su nivel, dando atención prioritaria a aquellos con mayor impacto y menor tolerancia, en línea con el umbral de riesgo aceptado por la entidad.
- Aplicar metodologías de evaluación consistentes, ya sea mediante enfoques cualitativos (clasificación en niveles como bajo, medio o alto) o semicuantitativos (asignación de valores numéricos a cada variable).

- ✓ Método cualitativo: Asignar valores descriptivos (bajo, medio, alto) a la probabilidad e impacto.
- ✓ Método semicuantitativo: Asignar valores numéricos a escalas cualitativas (Bajo = 1, Medio = 2, Alto = 3, Crítico = 4), que permitan calcular el nivel de riesgo mediante multiplicación (Impacto × Probabilidad).

Valor	Nivel de Impacto	Descripción
1	Bajo	El riesgo ocasiona consecuencias mínimas sobre los procesos de la entidad. No compromete activos críticos ni genera interrupciones significativas.
2	Medio	El riesgo ocasiona afectaciones moderadas en procesos o servicios. Puede requerir acciones de mitigación, pero no compromete de forma grave la continuidad operativa.
3	Alto	El riesgo genera un impacto considerable en los procesos institucionales, afectando activos de información relevantes, la disponibilidad de servicios y/o el cumplimiento normativo.
4	Crítico	El riesgo provoca consecuencias graves e inmediatas: interrupción de operaciones críticas, pérdida de información sensible, incumplimiento legal o sanciones significativas, afectando de forma directa la misión institucional.

Esta reevaluación periódica permite ajustar las estrategias de tratamiento de riesgos frente a los cambios del entorno, optimizar la toma de decisiones y fortalecer el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).

5.3.2 Definición de acciones de tratamiento:

- Opciones: Mitigar, Transferir, Aceptar o Eliminar.

- Asignar controles técnicos (firewalls, cifrado, controles de acceso), organizacionales (manuales, protocolos), legales (cláusulas contractuales) o físicos (cámaras, cerraduras).

La EDRU E.I.C.E establece el tratamiento de cada riesgo priorizado conforme a la norma ISO/IEC 27001:2022. Para cada riesgo, se selecciona una de las siguientes opciones: mitigarlo, transferirlo, aceptarlo o eliminarlo, según su nivel de impacto y probabilidad.

Luego, se asignan los controles adecuados:

- Técnicos: firewalls, cifrado, autenticación multifactor, etc.
- Organizacionales: políticas, capacitaciones, procedimientos.
- Legales: cláusulas en contratos.
- Físicos: controles de acceso, cámaras, etc.

Todas las acciones se registran en un plan de tratamiento estructurado que incluye responsables, fechas y estado de avance. Este plan es revisado por la Oficina de Planeación, en el marco de aseguramiento de la calidad y aprobado por el Comité Institucional de Gestión y Desempeño y se encuentra alineado con la Política Institucional, lo que asegura la trazabilidad y el cumplimiento de los requisitos normativos.

Práctico:

- Riesgo: Acceso indebido a la información correspondiente a los proyectos que se estén o se hayan ejecutado.
- Tratamiento: Implementar control de acceso basado en roles (RBAC) y registro de auditoría.
- Responsable: Área de TI.
- Plazo: 30 días.

5.3.3 Actualización del Plan de Tratamiento de Riesgos:

- Incluir: riesgo, tratamiento, responsable, cronograma, estado.

- Asegurar trazabilidad y revisión periódica.

El Plan de Tratamiento de Riesgos es un componente fundamental del Sistema de Gestión de Seguridad de la Información (SGSI), el cual debe ser actualizado de manera periódica para reflejar los riesgos actuales, su nivel de exposición y las medidas implementadas para su mitigación. Su actualización garantiza la trazabilidad, el cumplimiento normativo y promueve la mejora continua del sistema.

Elementos mínimos:

Elemento	Descripción según ISO 27001:2022, MinTIC y Gobierno Digital
Riesgo	Debe estar identificado con un código único, alineado con la matriz de riesgos del SGSI. Descripción clara del evento de riesgo.
Tratamiento	Describir la medida adoptada (evitar, mitigar, transferir o aceptar). Incluir controles específicos que se implementarán.
Responsable	Designar claramente el rol, cargo o área responsable de ejecutar el tratamiento. (Alineado con matriz RACI del SGSI).
Cronograma	Establecer fechas realistas de inicio, ejecución y cierre de cada actividad de tratamiento. Priorizar según el nivel de riesgo.
Estado	Identificar el avance: "No iniciado", "En ejecución", "Ejecutado", "Reprogramado", "No viable"

5.3.4 Asegurar trazabilidad:

- Mantener una bitácora de cambios: Cada modificación debe documentarse con la fecha, motivo del cambio, responsable que autoriza y evidencia del nuevo análisis.
- Establecer una numeración o versión del plan para que sea fácilmente auditable.
- Relacionar cada tratamiento con el código del riesgo en la matriz y con el control del Anexo A (ISO 27001:2022).
- Vincular el plan con hallazgos de auditorías internas o externas, incidentes o reevaluaciones.

5.3.5 Anexos:

Se dispone de una plantilla editable en formato Excel que incorpora los campos previamente mencionados, así como columnas adicionales para registrar evidencias de implementación, fechas de revisión, responsables secundarios y observaciones. Su estructura permite una fácil integración con herramientas de seguimiento, como tableros de control, y fortalece la trazabilidad en los procesos de auditoría y verificación de cumplimiento.

Ver formato FOR-GDO-03-02 - SEGUIMIENTO Y EVALUACIÓN DE RIESGOS.

ANEXO A – Catálogo de controles ISO 27001:2022 aplicados en EDRU

Incluir tabla con columnas:

- Control ISO
- Descripción
- Riesgo mitigado
- Proceso responsable
- Evidencia

5.4 Fase 3: Implementación.

5.4.1 Validación y aprobación del plan:

- Presentar al Comité Institucional de Gestión y Desempeño.
- Documentar actas de aprobación.
- Incorporar el plan en la estrategia institucional.

Socializar el plan con el Comité Institucional de Gestión y Desempeño y dejar registro en el acta de reunión del mes correspondiente.

5.4.2 Comunicación y capacitación:

- Difundir el plan a las áreas involucradas.
- Realizar talleres y campañas.

Actividad: Campaña sobre uso seguro de sistemas de información y manejo de datos.

5.4.3 Seguimiento inicial:

- Verificar la ejecución de las acciones planteadas.
- Medir plazos y efectividad.
- Documentar resultados de seguimiento en reuniones de control.

Indicadores sugeridos (KPIs): % de acciones mitigadas en el plazo definido.

Los indicadores de seguimiento y efectividad del Plan de Tratamiento de Riesgos deberán estar definidos, documentados y gestionados a través de la Ficha Institucional de Indicadores, asegurando su alineación con la normativa ISO/IEC 27001:2022, Gobierno Digital y con los lineamientos internos de Gestión Organizacional.

Indicadores propuestos para la gestión y revisión del plan:

- Nº de incidentes post-tratamiento por riesgo residual.
- Nivel de cumplimiento del plan por unidad responsable.
- Tiempo promedio de implementación de controles.
- Frecuencia de revisión y actualización del plan.

Cada indicador deberá contar con su respectiva Ficha de Indicadores, formato FOR-GAC-08 FICHA TÉCNICA DE FORMULACIÓN DE INDICADORES incluyendo:

- nombre del indicador
- objetivo
- fórmula de cálculo
- unidad de medida
- línea base
- meta

- fuente de datos
- método de medición
- responsable
- periodicidad
- estado de avance.

Indicador	Fórmula	Unidad	Meta 2025	Periodicidad	Responsable
% de acciones mitigadas	(# acciones cerradas / # total acciones) x 100	%	≥ 90%	Mensual	Oficina TIC
Nº incidentes post-tratamiento	Conteo de incidentes por riesgo residual	Número	0	Mensual	Oficina TIC
Cumplimiento por unidad	(# actividades cumplidas / # planificadas) x100	%	≥ 95%	Trimestral	Procesos
Tiempo promedio de implementación	Días promedio por control implementado	Días	≤ 45 días	Mensual	Seguridad TI

5.4.4 Revisión Periódica.

Se establecerá una revisión semestral o cuando ocurra un cambio significativo en los sistemas, normatividad o procesos críticos de la EDRU E.I.C.E.

5.4.5 Criterios para revisión no programada:

- Incidentes de seguridad relevantes (ej. fuga de datos, accesos no autorizados).
- Cambios tecnológicos sustanciales (migración a la nube, nuevos sistemas críticos).
- Modificaciones normativas que impacten el SGSI (nuevas leyes o regulaciones).
- Resultados de auditorías internas o externas que recomienden ajustes inmediatos.
- Identificación de nuevos riesgos de alto impacto no contemplados previamente. establecerá una revisión semestral o cuando ocurra un cambio significativo en los sistemas, normatividad o procesos críticos de la EDRU E.I.C.E.

5.4.6 Definición de los anexos sugeridos.

- Matriz de Riesgos completa (formato Excel) – Nivel de riesgo, activos involucrados, controles existentes y residuales.
- Mapa de calor de riesgos – Visualización gráfica para priorización.

Este mapa permite visualizar la priorización de los riesgos de acuerdo con su nivel de impacto y probabilidad. Se basa en una matriz 4x3 (Crítico, Alto, Medio, Bajo), donde:

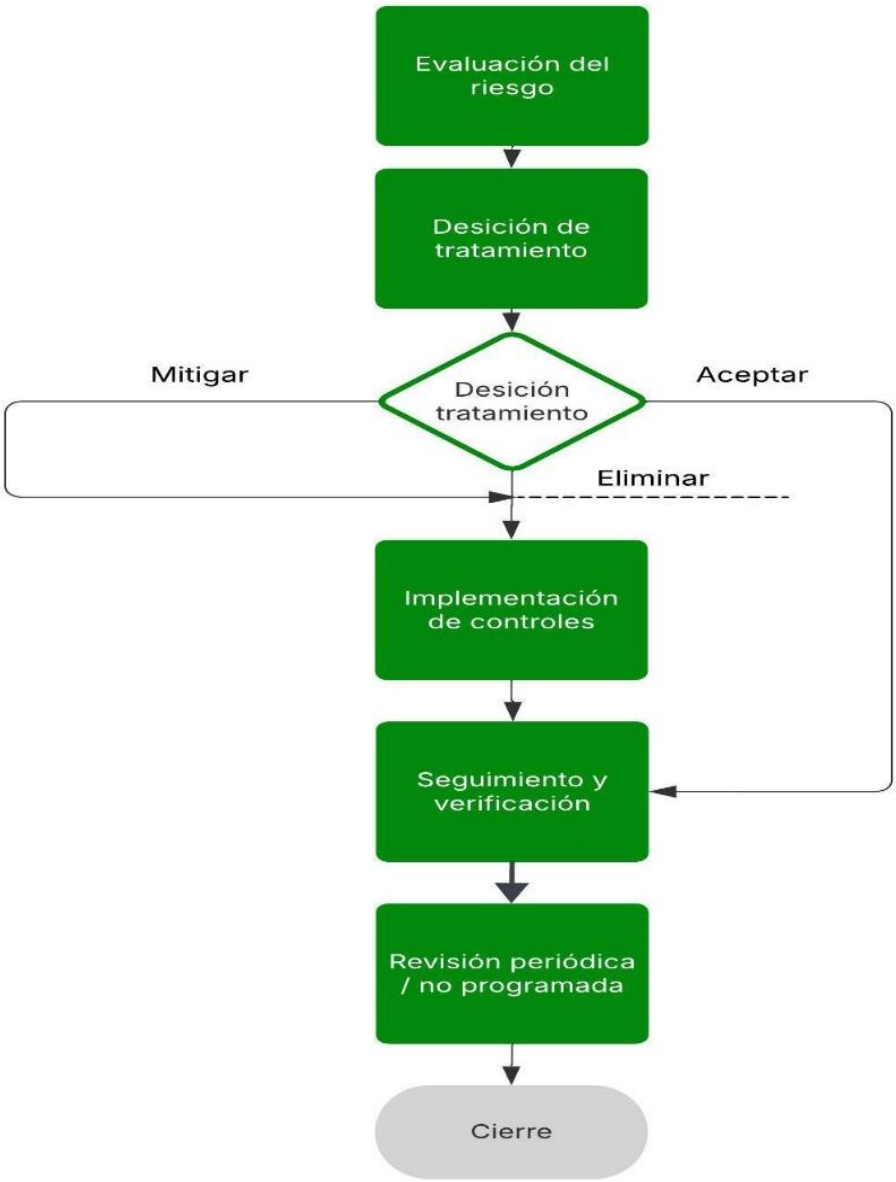
- Impacto: Consecuencias potenciales del riesgo sobre los activos de información.
- Probabilidad: Posibilidad de ocurrencia del evento.

Impacto \ Probabilidad	**Alta**	**Media**	**Baja**
Crítico (4)	Crítico	Crítico	Alto
Alto (3)	Crítico	Alto	Moderado
Medio (2)	Alto	Moderado	Bajo
Bajo (1)	Moderado	Bajo	Bajo

- Cronograma de implementación del plan – Gantt con responsables y fechas.

Ver anexo - Cronograma_Plan_Seguridad_EDRU.

- Diagrama de flujo del ciclo de tratamiento de riesgos – Desde identificación hasta cierre.



5.4.7 Cronograma de Trabajo (Diciembre).

Mes	Actividad	Responsable	Entregable / Evidencia	Fecha de entrega	Estado / Observaciones
Diciembre	Elaboración del Plan de Tratamiento de Riesgos	Gestión Administrativa, Documental y TIC.	Documento PLI-GDO-03-02	10/12/2025	Entregado a revisión.
	Diseño del Formato de Seguimiento y Evaluación de Riesgos	Gestión Administrativa, Documental y TIC.	Formato en Excel (editable) FOR-GDO-03-02	10/12/2025	Entregado a revisión.
	Elaboración de la Matriz de Riesgos de Seguridad de la Información (versión inicial)	Gestión Administrativa, Documental y TIC.	Matriz en Excel FOR-GDO-03-01	10/12/2025	Entregado a revisión.
	Cronograma_Plan_Seguridad_EDRU.xlsx	Gestión Administrativa, Documental y TIC.	Archivo Excel con cronograma	10/12/2025	Finalizado.
	Redacción inicial del Plan de Seguridad y Privacidad PLI-GDO-03-03	Gestión Administrativa, Documental y TIC.	Plan de Seguridad y privacidad de la información PLI-GDO-03-03	10/12/2025	Entregado a revisión.
	Consolidación y aprobación del Plan de Seguridad y Privacidad PLI-GDO-03-03	Gestión Administrativa, Documental y TIC.	Documento PLI-GDO-03-03 aprobado	11/12/2025	Entregado a revisión.

Mes	Actividad	Responsable	Entregable / Evidencia	Fecha de entrega	Estado / Observaciones
Diciembre	Inclusión de Política de Seguridad Física y Ambiental	Gestión Administrativa, Documental y TIC.	Documento actualizado	11/12/2025	A revisión.
	Inclusión de Política de Uso Aceptable de Recursos	Gestión Administrativa, Documental y TIC.	Documento actualizado	11/12/2025	A revisión.
	Desarrollo de la Política de Derecho de Autor y Uso de Contenidos	Gestión Administrativa, Documental y TIC.	Documento completo con principios rectores	11/12/2025	A revisión.
	Actualización de la Matriz de Riesgos FOR-GDO-03-01	Gestión Administrativa, Documental y TIC.	Matriz en Excel actualizada FOR-GDO-03-01	12/12/2025	Versión 2.
Diciembre	Documentación de Procesos y Procedimientos TI.	Gestión Administrativa, Documental y TIC.	Documento detallado.	12/12/2025	A revisión
	Elaboración de informes de soporte a auditorías (evidencias, PETI, riesgos)	Gestión Administrativa, Documental y TIC.	Informe técnico y evidencias.	12/12/2025	Pendiente auditoría
	Ajustes a políticas entregadas (retroalimentación interna)	Gestión Administrativa, Documental y TIC.	Versiones actualizadas	12/12/2025	Pendiente.

Mes	Actividad	Responsable	Entregable / Evidencia	Fecha de entrega	Estado / Observaciones
	Creación de formatos y plantillas complementarias (controles, checklist)	Gestión Administrativa, Documental y TIC.	Paquete de formatos en Word/Excel	12/12/2025	Aprobación interna.
Diciembre	Consolidación de todas las políticas en un documento marco único	Gestión Administrativa, Documental y TIC.	Documento marco consolidado	12/12/2025	Versión final preliminar.
	Preparación de evidencias y anexos para auditorías externas	Gestión Administrativa, Documental y TIC.	Carpeta digital con anexos	12/12/2025	Pendiente auditoría
	Desarrollo del Glosario de Seguridad de la Información y TI	Gestión Administrativa, Documental y TIC.	Documento de glosario	15/12/2025	Pendiente.
Diciembre	Validación final de actividades y formatos con gerencia/comité	Gestión Administrativa, Documental y TIC.	Acta de aprobación	15/12/2025	Validación final.
	Ajustes finales al Plan de Seguridad y anexos	Gestión Administrativa, Documental y TIC.	Versión definitiva del plan y anexos	15/12/2025	Versión final.

	Entrega de documentación completa consolidada	Gestión Administrativa, Documental y TIC.	Carpeta digital con todos los documentos	15/12/2025	Entrega oficial.
	Presentación de informe final de cierre de actividades	Gestión Administrativa, Documental y TIC.	Informe ejecutivo de cierre	15/12/2025	Pendiente.

5.4.8 Anexos.

- FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
- FOR-GDO-03-02 SEGUIMIENTO Y EVALUACIÓN DE RIESGOS
- Cronograma_Plan_Seguridad_EDRUControl de cambios

FICHA CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción de la Modificación**
1	31-ene-2025	Plan de tratamiento de riesgos de seguridad y privacidad de la información.
2	10-dic-2025	Actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información.

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