EDRU

ALCALDÍA DE
SANTIAGO DE CALI

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026
(30 de enero de 2026)
"POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION URBANA EDRU EICE"

La Gerente General de la Empresa de Desarrollo y Renovación Urbana E.I.C.E. – EDRU E.I.C.E. en uso de sus atribuciones constitucionales, legales y en especial lo descrito en la Ley 872 de 2003, modificada por el Decreto 1499 de 2017, el Decreto 1083 de 2015 y el artículo 23 de 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 Decreto 1499 de 2017, en su artículo 1°, sustituyó el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015 - Único Reglamentario del Sector de Función Pública, con el fin de reglamentar el alcance del Sistema de Gestión y su articulación con el Sistema de Control Interno de que trata el artículo 133 de la Ley 1753 de 2015, actualizando el Modelo Integrado de Planeación y Gestión.

Que, la EDRU, mediante Resolución No. 10.15-029-2018 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, de conformidad con lo establecido en el artículo 25 de la Constitución Política de Colombia, que señala que *"El trabajo es un derecho y una obligación social y goza, en todas sus modalidades, de la especial protección del Estado. Toda persona tiene derecho a un trabajo en condiciones dignas y justas."* Que, la Ley 909 de 2004 en el numeral 2, literales a) y b) del artículo 15 y en el numeral 1 del artículo 17, señala que las entidades deberán formular y adoptar anualmente los planes estratégicos de talento humano, anual de vacantes y de previsión de recursos humanos, sin consagrar fecha para el efecto.

Que, el Decreto ley 1567 de 1998 en el artículo 3 literal c) consagra que las entidades, con el propósito de organizar la capacitación interna, deberán formular con una periodicidad mínima de un año su plan institucional de capacitación; en el artículo 34 señala que el jefe de cada entidad deberá adoptar y desarrollar internamente planes anuales de incentivos institucionales, de acuerdo con la ley y los reglamentos, sin indicar plazo para su adopción.

Que, el Decreto 1072 de 2015 en el artículo 2.2.4.6.8 numeral 7 consagra, que los empleadores deben desarrollar un plan de trabajo anual para alcanzar cada uno de los objetivos propuestos en el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SGSST), sin indicar plazo para su adopción.

Que, el artículo 2.2.10.1 del Decreto 1083 de 2015, expedido por la Presidencia de la República, establece que "Las entidades deberán organizar programas de estímulos con el fin de motivar el desempeño eficaz y el compromiso de sus empleados. Los estímulos se implementarán a través de programas de bienestar social".

Que, el artículo 2.2.10.6 del Decreto 1083 de 2015, indica que*: "Los programas de Bienestar responderán a estudios técnicos que permitan, a partir de la identificación de necesidades y expectativas de los empleados, determinar actividades y grupos de beneficiarios bajo criterio de equidad, eficiencia mayor cubrimiento institucional".*

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026
(30 de enero de 2026)
"POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION URBANA EDRU EICE"

Que, el artículo 2.2.10.9 del Decreto 1083 de 2015, indica que*: "Plan de incentivos institucionales. El jefe de cada entidad adoptará anualmente el plan de incentivos institucionales y señalará en él los incentivos no pecuniarios que se ofrecerán al mejor empleado de carrera de la entidad, a los mejores empleados de carrera de cada nivel jerárquico y al mejor empleado de libre nombramiento y remoción de la entidad, así como los incentivos pecuniarios y no pecuniarios para los mejores equipos de trabajo. Dicho plan se elaborará de acuerdo con los recursos institucionales disponibles para hacerlos efectivos. En todo caso los incentivos se ajustarán a lo establecido en la Constitución Política y la ley".*

Que, el artículo 2.2.9.1 del Decreto 1083 de 2015, indica que*: "Planes de capacitación. Los planes de capacitación de las entidades públicas deben responder a estudios técnicos que identifiquen necesidades y requerimientos de las áreas de trabajo y de los empleados, para desarrollar los planes anuales institucionales y las competencias laborales.*

Que, el artículo 2.8.2.5.8 del Decreto 1080 de 2015, reglamenta las Leyes 594 de 2000 y 1437 de 2011, incluye de los instrumentos archivísticos para la gestión documental el Plan Institucional de Archivos – PINAR; el cual es un instrumento que permitirá planear, hacer seguimiento y articular con los planes estratégicos, la función archivística de acuerdo con las necesidades, debilidades, riesgos y oportunidades.

Que, el Decreto 1122 del agosto 30 de 2024, "*Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública*" en su *artículo 2.1.4.4.1.1. Ámbito de aplicación. "Las entidades obligadas del orden nacional, departamental y municipal, cualquiera que sea su régimen de contratación, deberán implementar Programas de Transparencia y Ética Pública con las características, estándares, elementos, requisitos, procedimientos y controles mínimos que para tales efectos establezca la Secretaría de Transparencia de la Presidencia de la República".*

Que, el Programa de Transparencia y Ética Pública (PTEP) es un instrumento obligatorio de gestión diseñado para prevenir riesgos de corrupción, lavado de activos y soborno en entidades públicas, fundamentado principalmente en la Ley 2195 de 2022 y el Decreto 1122 de 2024. Este programa establece la debida diligencia, gestión de riesgos y la cultura de integridad (antisoborno) como pilares fundamentales para la administración pública, integrándose con el modelo Integrado de Planeación y Gestión (MIPG).

Que, el Decreto 1008 de 2018, Establecen los Lineamientos Generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Que, dentro de la Política de Gobierno Digital, se encuentra contemplado el Plan Estratégico de Tecnología de la Información - PETI, el cual debe ser adoptado por la entidad, con el fin de garantizar la armonía en la articulación y en el desarrollo de la Política de Gobierno Digital.

Que, de acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026
(30 de enero de 2026)
"POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION URBANA EDRU EICE"

Información y las Comunicaciones, la política de gobierno digital' será definida por, MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que, según el numeral 2, del artículo anteriormente citado, los habilitadores transversales de la política de gobierno digital, son los elementos fundamentales de seguridad y privacidad de la información, arquitectura y servicios ciudadanos digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha política.

Que, la Resolución 00500 del 10 de marzo del 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*

Que, la Resolución 0448 de 2022, por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías, de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.

Que, el Decreto 612 de 2018, adicionó al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:

"2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año":

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Anual de Adquisiciones
3. Plan Anual de Vacantes
4. Plan de Previsión de Recursos Humanos
5. Plan Estratégico de Talento Humano
6. Plan Institucional de Capacitación
7. Plan de Incentivos Institucionales
8. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
9. Plan Anticorrupción y de Atención al Ciudadano
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI

Que, en sesión llevada a cabo el 29 de enero de 2026, por el Comité Institucional de Gestión y Desempeño se revisaron y se aprobaron los siguientes planes institucionales que le aplican a la EDRU E.I.C.E.:

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Estratégico de Talento Humano
3. Plan Institucional de Capacitación

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026
(30 de enero de 2026)
"POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION URBANA EDRU EICE"

4. Plan de Incentivos Institucionales
5. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
6. Programa de Transparencia y Ética Publica
7. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI
8. Plan de tratamiento de riesgos de seguridad y privacidad de la información
9. Plan de seguridad y privacidad de la información
10. Plan de acción institucional

Que, con fundamento en lo antes expuesto, la Empresa de Desarrollo y Renovación Urbana –EDRU E.I.C.E.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar los planes institucionales para la vigencia 2026 que se relacionan a continuación:

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Estratégico de Talento Humano
3. Plan Institucional de Capacitación
4. Plan de Incentivos Institucionales
5. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
6. Programa de Transparencia y Ética Publica
7. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI
8. Plan de tratamiento de riesgos de seguridad y privacidad de la información
9. Plan de seguridad y privacidad de la información
10. Plan de acción institucional

ARTÍCULO SEGUNDO: Estos planes son aplicables a los funcionarios y contratistas de la Empresa de Desarrollo y Renovación Urbana EDRU EICE y tendrán que ser socializados a través de la página web, capacitaciones, inducciones y reinducciones que se programen, de acuerdo a las temáticas definidas en su contenido.

ARTÍCULO TERCERO: La presente Resolución rige a partir de la fecha de su expedición.

Se expide en Santiago de Cali el 30 de enero de 2026.

COMUNIQUESE Y CUMPLASE

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

	nombre	Cargo / Actividad	Firma
Proyectó	Julian Gomez Alarcón	Contratista Oficina de Planeación	
Proyectó	Adriana Millan Azcarate	Contratista Oficina de Planeación	
Revisó	Jorge Andrés Martínez Zambrano	Jefe Oficina de Planeación	
Revisó	Carolina Soto Flórez	Jefe Oficina Jurídica	
Revisó	Sandra Idali Arévalo Peña	Directora Administrativa	
Aprobó	Ana Maria Gil Rodríguez	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

2026

TABLA DE CONTENIDO

INTRODUCCIÓN

La Empresa de Desarrollo y Renovación Urbana (EDRU) reconoce la información como un activo estratégico fundamental para el cumplimiento de su misión institucional, la continuidad de sus procesos y la confianza de los grupos de interés. En un entorno caracterizado por crecientes riesgos tecnológicos, normativos y operativos, resulta indispensable adoptar medidas sistemáticas que permitan proteger la confidencialidad, integridad y disponibilidad de la información, así como garantizar el adecuado tratamiento de los datos personales.

En este contexto, el Plan de Tratamiento de Seguridad y Privacidad de la Información constituye un instrumento de gestión orientado a dar respuesta a los riesgos identificados en la entidad, asegurando el cumplimiento del marco normativo vigente, entre el cual se destacan la Ley Estatutaria 1581 de 2012, la Ley 1266 de 2008, los Decretos 1377 de 2013, 1081 de 2015 y 255 de 2022, la Sentencia C-748 de 2011, el Marco de Ciberseguridad y Privacidad del MinTIC, así como la norma ISO/IEC 27001:2022.

El presente plan se fundamenta en la Matriz de Riesgos de Seguridad y Privacidad de la Información (FOR-GDO-03-01), en su versión vigente y aprobada por el Comité Institucional de Gestión y Desempeño, y se articula con la Política de Seguridad y Privacidad de la Información (POL-DPI-01-03), garantizando coherencia institucional, trazabilidad documental y soporte para los procesos de auditoría interna y externa.

1 OBJETIVO

Establecer y ejecutar las acciones de tratamiento necesarias para mitigar, controlar o reducir los riesgos de seguridad y privacidad de la información identificados en la EDRU, de acuerdo con la Matriz de Riesgos institucional, asegurando el cumplimiento del marco normativo vigente y el fortalecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información.

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 de tratamiento asignadas.
- Notificar oportunamente cambios, incidencias y desviaciones que puedan afectar el nivel de riesgo.
- Proponer nuevos controles o ajustes a los existentes cuando corresponda.

Oficina de Control Interno

- Realizar seguimiento a los planes de mejoramiento derivados de auditorías, evaluaciones internas o externas relacionadas con la seguridad y privacidad de la información, cuando existan planes vigentes.
- Verificar la implementación y cierre efectivo de las acciones de mejora definidas.
- Emitir recomendaciones para el fortalecimiento del Plan, en el marco de sus funciones de evaluación independiente y control.

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 y sostenibilidad.

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 asociados.
- Analizar los resultados de auditorías anteriores.

La Fase 1 inicia con la revisión de los riesgos existentes, mediante un análisis integral del estado actual de la seguridad y privacidad de la información. Este proceso comienza con la consulta del inventario de activos de información, lo que permite identificar los recursos tecnológicos, físicos y lógicos críticos para la operación de la EDRU E.I.C.E., así como su nivel de exposición frente a amenazas internas y externas.

Posteriormente, se realiza el análisis del mapa de riesgos previamente definido, evaluando la vigencia de los riesgos identificados, su impacto potencial y la pertinencia de los controles existentes, considerando el contexto organizacional, normativo y tecnológico actual.

De manera complementaria, se revisan los resultados de auditorías internas y externas realizadas en vigencias anteriores, con especial énfasis en los planes de mejoramiento formulados y en los principales hallazgos relacionados con debilidades en la gestión de riesgos de seguridad y

privacidad de la información. En este sentido, la auditoría de Control Interno concluyó que la organización requiere fortalecer su enfoque de gestión de riesgos, debido a vacíos metodológicos, debilidades en la articulación con otros procesos institucionales y limitaciones en los mecanismos de priorización, seguimiento y toma de decisiones. Estos hallazgos evidencian la necesidad de consolidar el Plan de Tratamiento de Riesgos como una herramienta efectiva, estructurada y sostenible.

Una vez aprobados los ajustes derivados de los procesos de auditoría, se debe implementar el cronograma de acciones definido en los planes de mejoramiento, orientado a fortalecer la seguridad de la información, la privacidad y la gestión de riesgos en la EDRU E.I.C.E.

Adicionalmente, se realiza el análisis de los incidentes de seguridad ocurridos durante el periodo anterior, identificando patrones recurrentes, vulnerabilidades explotadas y lecciones aprendidas. Los resultados de este análisis permiten retroalimentar la matriz de riesgos y fortalecer los planes de tratamiento asociados, priorizando de manera estratégica las acciones correctivas y preventivas, en coherencia con los principios de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

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 de tratamiento definidas se registran en el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual constituye el instrumento institucional que consolida los riesgos priorizados, las medidas adoptadas, los responsables, los plazos y el estado de avance.

La ejecución de dichas acciones se desarrolla conforme a la ruta de acción definida a través del cronograma de actividades, establecido en el numeral 5.4.7 Cronograma de Trabajo 2026, el cual permite planificar, monitorear y hacer seguimiento a la implementación de los controles técnicos, organizacionales, legales y físicos.

Este Plan es revisado por la Oficina de Planeación en el marco del aseguramiento de la calidad, y aprobado por el Comité Institucional de Gestión y Desempeño, garantizando la trazabilidad, el cumplimiento normativo y la articulación con la Política Institucional y el Sistema de Gestión de Seguridad de la Información (SGSI).

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 el control de cambios: Cada modificación debe documentarse con la versión, fecha, motivo del cambio, responsable que autoriza y evidencia del nuevo análisis. Este registro es documentado por el proceso aseguramiento de la calidad, una vez da visto bueno al mismo.
- 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 la EDRU E.I.C.E.

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 2026	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:

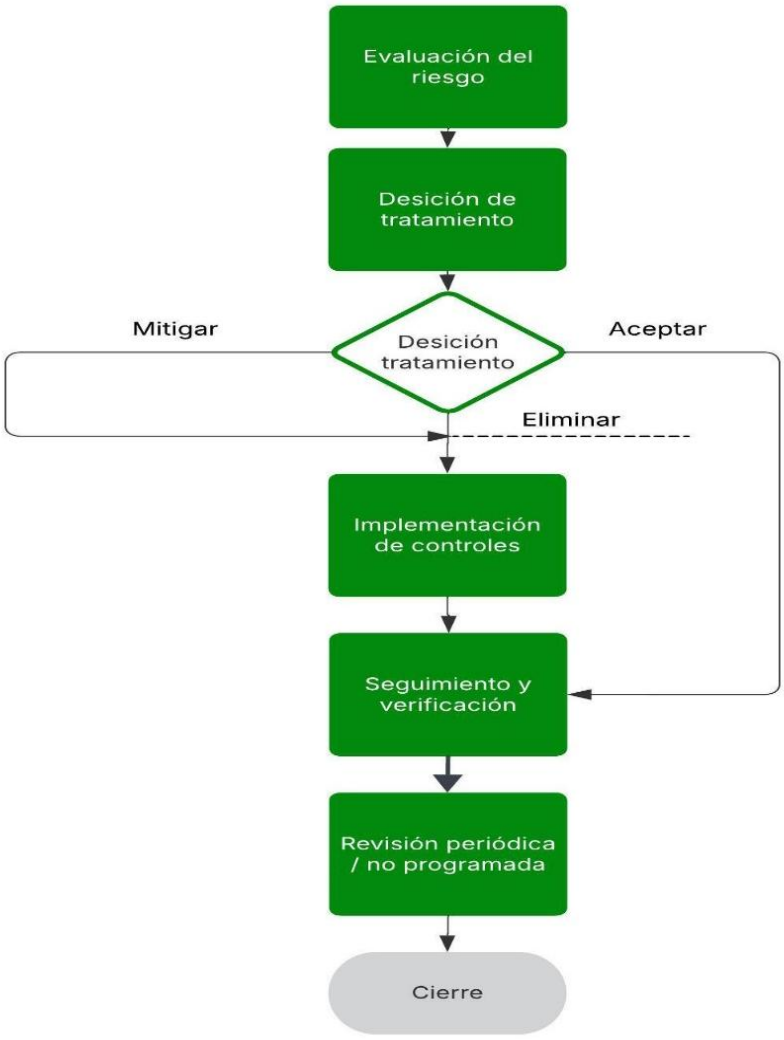
- Impacto: Consecuencias potenciales del riesgo sobre los activos de información.
- Probabilidad: Posibilidad de ocurrencia del evento.

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 2026

El presente cronograma define las actividades para la implementación, seguimiento y mejora continua del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información durante la vigencia 2026, asegurando coherencia con el Sistema de Gestión de Seguridad de la Información (SGSI), los planes de mejoramiento vigentes y los lineamientos del Comité Institucional de Gestión y Desempeño.

Mes	Actividad	Responsable	Entregable / Evidencia
Enero	Socialización del Plan de Tratamiento de Riesgos aprobado	Gestión Administrativa, Documental y TIC	Acta de socialización
Enero	Actualización del inventario de activos de información	Área TIC	FOR-GDO-03-06 actualizado
Febrero	Revisión y actualización del mapa de riesgos	Gestión Administrativa, Documental y TIC	FOR-GDO-03-01 versión vigente
Febrero	Análisis de planes de mejoramiento vigentes (auditorías)	Control Interno / TIC	Informe de análisis
Marzo	Reevaluación de riesgos (probabilidad e impacto)	Gestión Administrativa, Documental y TIC	Matriz de riesgos ajustada
Marzo	Definición y priorización de acciones de tratamiento	Gestión Administrativa, Documental y TIC	Plan de tratamiento actualizado
Abril	Implementación de controles técnicos priorizados	Área TIC	Registros técnicos / logs
Abril	Implementación de controles organizacionales	Gestión Administrativa, Documental y TIC	Políticas / procedimientos
Mayo	Jornada de capacitación y concientización	Gestión Administrativa, Documental y TIC	Listas de asistencia
Junio	Seguimiento semestral al plan y a los KPIs	TIC / Control Interno	Informe de seguimiento
Julio	Revisión de incidentes de seguridad del primer semestre	Área TIC	Registro de incidentes
Agosto	Ajustes a controles según resultados de seguimiento	Área TIC	Evidencias de ajuste
Septiembre	Auditoría interna al SGSI / Plan de Riesgos	Control Interno	Informe de auditoría
Octubre	Ejecución de acciones correctivas de auditoría	TIC / Procesos	Plan de mejoramiento
Noviembre	Evaluación de efectividad del plan	Gestión Administrativa, Documental y TIC	Informe de evaluación
Diciembre	Revisión final y actualización para vigencia siguiente	Comité / Gerencia	Acta y versión ajustada

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_EDRU_Control de cambios
-

6 CONTROL DE CAMBIOS

FICHA CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción de la Modificación**
1	31-ene-2025	Versión inicial. Aprobado a través del acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.001-2025 del 31 de enero de 2025. Resolución de adopción No. 10.15-014-2025 del 31 de enero de 2025
2	10-dic-2025	Actualización del contenido del documento para dar cumplimiento al plan de mejoramiento establecido por la Oficina de Control Interno. Aprobado a través de acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.007-2025 del 5 de diciembre de 2025. Resolución de adopción No. 10.15-115-2025 del 10 de diciembre de 2025.
3	30-ene-2026	Revisión y actualización del documento, aprobado a través del acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.001-2026 del 29 de enero de 2026. Resolución de adopción No. 10.15-013-2026 del 29 de enero de 2026.

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. 10.1.2.001-2026	Fecha: 29-ene-2026	No.: 10.15-013-2026	Fecha de expedición: 30-ene-2026