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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

TABLA DE CONTENIDO

INTRODUCCIÓN

La Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E., en su compromiso con la transformación integral del territorio, reconoce que la información es uno de sus activos más estratégicos. Por ello, resulta indispensable establecer un marco de gestión que garantice la protección, integridad, disponibilidad y confidencialidad de los datos que se administran en el ejercicio de sus funciones misionales, administrativas y operativas.

En este contexto, el Plan de Seguridad y Privacidad de la Información se constituye como un documento clave para salvaguardar los activos de información más valiosos de la empresa. Su propósito es asegurar que las políticas, procedimientos y controles internos estén alineados con el instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como con las amenazas emergentes, los marcos regulatorios vigentes y las mejores prácticas nacionales e internacionales.

Este plan no solo está orientado a mitigar riesgos y fortalecer la capacidad institucional frente a los desafíos de la ciberseguridad, sino también a consolidar una cultura organizacional enfocada en la gestión responsable y segura de la información. Para su desarrollo durante la vigencia 2025, se ha estructurado en tres fases: Diagnóstico, que permitirá identificar el estado actual del sistema de seguridad de la información; Actualización, donde se ajustarán y optimizarán los marcos normativos y operativos existentes; e Implementación, etapa en la que se ejecutarán las acciones y controles definidos para garantizar la efectividad del sistema de gestión de seguridad (SGSI) de la información en la EDRU E.I.C.E.

1 OBJETIVO

Implementar un conjunto de controles técnicos, administrativos y físicos que permitan proteger la información institucional, mitigar los riesgos identificados, garantizar el cumplimiento de la normatividad vigente y fortalecer la madurez del sistema de gestión de seguridad de la información (SGSI) en la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E.

- Asegurar el cumplimiento de la Ley 1581 de 2012. Decreto Nacional 1377 de 2013 y Decreto 1081 de 2015.
- Proteger los datos sensibles y la información crítica institucional.
- Implementar y mejorar continuamente el SGSI conforme a ISO/IEC 27001:2022.
- Cumplir el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de la información.

2 ALCANCE

El presente Plan Estratégico de Seguridad y Privacidad de la Información aplica a todos los procesos, sistemas de información, funcionarios de planta, contratistas que gestionan o tienen acceso a datos en el marco de las operaciones de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E. de Santiago de Cali.

Este plan cubre la totalidad de los activos de información de la entidad, independientemente de su formato, ubicación o medio de procesamiento, con el fin de establecer medidas de protección que garanticen su confidencialidad, integridad, disponibilidad y trazabilidad, incluyendo:

- Datos personales de contratistas y funcionarios de planta.
- Sistemas y aplicaciones que procesan, almacenan o transmiten información sensible.
- Protocolos de seguridad para proteger la infraestructura tecnológica.

- Cumplimiento legal y normativo.
- Cuidar y proteger los recursos tecnológicos (Hardware - Software).

3 RESPONSABILIDAD

La implementación, mantenimiento y mejora del Plan de Seguridad y Privacidad de la Información es una responsabilidad compartida entre las diferentes áreas de la EDRU E.I.C.E. Cada rol tiene funciones específicas que garantizan el cumplimiento de los controles, políticas y lineamientos establecidos para proteger la información institucional.

A continuación, se describen las responsabilidades según los actores involucrados:

Comité Institucional de Gestión y Desempeño.

- Aprobar el Plan de Seguridad y Privacidad de la Información y sus actualizaciones.

Oficina de Planeación

- Liderar la consolidación de los seguimientos periódicos de políticas institucionales, incluyendo seguridad y privacidad.
- Verificar la alineación del Plan con el Modelo Integrado de Planeación y Gestión (MIPG).

Gestión Administrativa, Documental y TIC.

- Implementar, gestionar y actualizar los controles definidos en el Plan.
- Coordinar las actividades del Sistema de Gestión de Seguridad de la Información (SGSI).

- Realizar monitoreo permanente de incidentes, vulnerabilidades y riesgos tecnológicos.
- Administrar inventarios de activos de información y asegurar la correcta clasificación de los mismos.
- Mantener actualizados los protocolos de acceso, copias de seguridad, respaldo y restauración.

Personal TIC

- Implementar y monitorear los controles técnicos asociados a accesos, redes, infraestructura, respaldos, plataformas y servicios en la nube.
- Ejecutar procedimientos de respuesta ante incidentes según el PGISI.
- Gestionar mecanismos de autenticación, contraseñas, privilegios y continuidad del servicio.

Todos los funcionarios, contratistas y terceros

- Cumplir con las políticas y lineamientos de seguridad y privacidad establecidos por la entidad.
- Clasificar adecuadamente la información que generen o administren.
- Hacer uso seguro de los dispositivos institucionales, cuentas y recursos tecnológicos.
- Reportar de manera inmediata cualquier incidente o situación sospechosa relacionada con la seguridad de la información.
- Participar en las capacitaciones y actividades de sensibilización programadas.

Enlace de Protección de Datos Personales / Delegado

- Velar por el cumplimiento de la Ley 1581 de 2012 y normativa complementaria.
- Gestionar solicitudes de los titulares de datos personales.

- Coordinar la implementación de controles de privacidad exigidos por ISO/IEC 27701.
- Apoyar el análisis de riesgos de privacidad y el cumplimiento del MSPI.

Proveedores y terceros que manejan información.

- Cumplir rigurosamente las cláusulas contractuales de seguridad y privacidad.
- Permitir auditorías o verificaciones cuando aplique.
- Reportar incidentes que comprometan información institucional.

4 TÉRMINOS Y DEFINICIONES

Acceso a la Información Pública: El acceso a la información pública es un derecho fundamental que faculta a todas las personas a conocer y acceder a la información pública que se encuentre en posesión, custodia o bajo el control de los sujetos obligados, sin necesidad de justificar interés o motivación alguna. (Ley 1712 de 2014, art 4), compilada en el Decreto 1081 de 2015.
Activos de Información y recursos: Hace referencia a los elementos de hardware y software relacionados con el procesamiento, almacenamiento y comunicación de la información, incluyendo bases de datos, procesos, procedimientos y recursos humanos vinculados a la gestión de los datos e información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

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

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Backup: Proceso mediante el cual se generan duplicados de información o sistemas con el propósito de garantizar su recuperación en caso de pérdida, daño, corrupción o incidente de seguridad.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
Confidencialidad: Propiedad de que la información no es puesta a disposición ni revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Dato personal: Cualquier información vinculada a una persona natural identificada o identificable.
Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Gestión de Incidentes de Seguridad de la Información: Conjunto de procesos para detectar, registrar, analizar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Incidente de Seguridad de la Información: Evento identificado que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas que la procesan. (ISO/IEC 27000).

Phishing: Técnica de ingeniería social mediante la cual un atacante suplanta una identidad legítima para engañar a las personas y obtener información sensible como credenciales, datos financieros o acceso no autorizado.

RBAC: Modelo de control de acceso basado en roles, donde los permisos se asignan según las funciones y responsabilidades del usuario dentro de la organización.

SGSI: Conjunto de políticas, procesos, procedimientos, recursos y responsabilidades establecidos para gestionar sistemática y continuamente la seguridad de la información según los lineamientos de ISO/IEC 27001:2022 y 27000:2022.

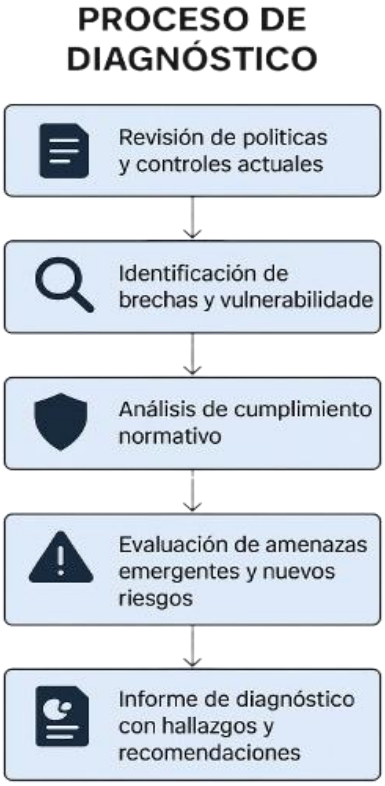
Stakeholders: Personas, grupos u organizaciones —internas o externas— que tienen interés, responsabilidad, influencia o pueden verse afectadas por la gestión de la seguridad y privacidad de la información de la EDRU E.I.C.E. Incluyen a quienes participan en el tratamiento de datos, en la operación de los sistemas de información, en la toma de decisiones, en el cumplimiento normativo y en la prestación de servicios institucionales. Estos stakeholders aportan requerimientos, expectativas y obligaciones que deben ser considerados para asegurar la confidencialidad, integridad, disponibilidad y cumplimiento legal en el manejo de la información.

5 CONTENIDO

5.1 Fase 1: Diagnóstico

5.1.1 Evaluación del estado actual del plan.

Esta fase inicial tiene como finalidad realizar un diagnóstico integral del Plan de Seguridad y Privacidad de la Información actualmente vigente. Para ello, se efectuará un análisis exhaustivo de las políticas, procedimientos y controles implementados, con el objetivo de evaluar su eficacia, nivel de madurez y grado de alineación con las mejores prácticas del sector (ISO/IEC 27001:2022) y el marco normativo aplicable. Este diagnóstico permitirá identificar fortalezas, debilidades y brechas existentes, proporcionando insumos clave para la toma de decisiones orientadas al ajuste, actualización y fortalecimiento del plan, en el marco del proceso de mejora continua y robustecimiento institucional.



5.1.2 Identificación de brechas y vulnerabilidades.

Con el fin de fortalecer la gestión integral de la seguridad y privacidad de la información, se llevará a cabo un análisis exhaustivo orientado a identificar brechas de cumplimiento frente a las

normativas aplicables, así como vulnerabilidades derivadas de deficiencias en los controles actuales. Este análisis incluirá la revisión detallada de las políticas institucionales vigentes, los procedimientos asociados y los controles implementados, con el fin de verificar su vigencia, coherencia y nivel de madurez.

Como parte del diagnóstico, se evaluarán los controles definidos en el Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo los controles alineados con el Anexo A de la ISO/IEC 27001:2022, la Política General de Seguridad y Privacidad, la Política de Gestión de Riesgos, la Política de Tratamiento de Datos Personales, la Política de Uso Aceptable, entre otras. Los hallazgos resultantes se documentarán y se integrarán en la matriz de riesgos, estableciendo la relación entre cada brecha detectada y el control asociado.

Este proceso también considerará la revisión de incidentes de seguridad documentados previamente, Así como la evaluación de la eficacia de las medidas de mitigación implementadas. De este modo, se busca detectar oportunidades de mejora, reforzar los controles existentes y adoptar acciones proactivas para minimizar las amenazas que puedan comprometer la confidencialidad, integridad, disponibilidad y resiliencia de la información institucional

5.1.3 Análisis de cambios Regulatorios y Nuevos Riesgos.

Se realizará una revisión integral del marco normativo vigente y aplicable, incluyendo normativas internacionales como el Reglamento General de Protección de Datos (GDPR), disposiciones nacionales como la Ley 1581 de 2012 en Colombia y otras regulaciones aplicables a la protección de datos personales. También se considerarán los lineamientos de la norma ISO/IEC 27001:2022 de forma paralela y aplicable para el análisis de amenazas emergentes en el entorno tecnológico, tales como nuevas vulnerabilidades, vectores de ataque y variaciones en el panorama de riesgos cibernéticos, con el objetivo de evaluar su impacto sobre la vigencia, cobertura y efectividad del plan de seguridad y privacidad de la información.

Normatividad nacional:

Ley	Descripción	Información complementaria
Ley 1581 de 2012	Régimen General de Protección de Datos Personales.	Define principios y disposiciones aplicables al tratamiento de datos personales por entidades públicas y privadas.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.	Obliga a garantizar el acceso y protección adecuada de la información pública.
Ley 1273 de 2009	Delitos Informáticos.	Modifica el Código Penal colombiano y protege la información y los sistemas informáticos.
Ley 1266 de 2008	Habeas Data financiero.	Aplica a la protección de datos personales relacionados con la actividad crediticia.

Decretos:

Decreto	Descripción
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012 y define medidas para el consentimiento informado de los titulares.
Decreto 1081 de 2015	Compila normas de la Presidencia de la República. Contiene disposiciones sobre la administración de la información pública.
Decreto 1627 de 2012	Establece lineamientos sobre la administración de bases de datos personales por parte de entidades públicas.
Decreto 2106 de 2019	Simplificación de trámites, con implicaciones en la gestión segura de la información.

Directrices y circulares:

Circular	Descripción
Circular Externa 02 de 2015	Superintendencia de Industria y Comercio – Instrucciones sobre el cumplimiento del Régimen de Protección de Datos.

Normas Técnicas Internacionales:

ISO/IEC	Descripción	Información complementaria
ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información (SGSI).	Estándar para establecer, implementar, mantener y mejorar un SGSI basado en riesgos.
ISO/IEC 27002:2022	Controles de seguridad de la información.	Guía para la selección, implementación y gestión de controles de seguridad.
ISO/IEC 27701:2019	Gestión de la privacidad de la información.	Extensión del SGSI para incluir aspectos de protección de datos personales (PIMS).
ISO 22301:2019	Gestión de la continuidad del negocio.	Apoya la capacidad de recuperación ante desastres y la continuidad operativa.

Buenas Prácticas:

ISO/IEC	Descripción
Plan de Seguridad y Privacidad de la Información	Documento estructurado que integra componentes de gobernanza, clasificación de la información, gestión de incidentes, seguridad física y digital, y protección de datos personales.
Manual de Tratamiento de Datos Personales	Guía para la selección, implementación y gestión de controles de seguridad.
Guías del MinTIC y Colombia Compra Eficiente	Extensión del SGSI para incluir aspectos de protección de datos personales (PIMS).
Política de Gobierno Digital	Alineada con el marco nacional TIC y de seguridad de la información.

5.1.4 Políticas.

Las políticas de seguridad y privacidad de la información representan el marco normativo interno que regula y orienta la protección de los activos de información de la Empresa de Desarrollo y Renovación Urbana – EDRU E.I.C.E. Estas políticas establecen los principios, lineamientos, responsabilidades y normas que deben ser cumplidas por todos los funcionarios de planta, contratistas y terceros que accedan, administren o procesen información institucional. Su propósito es salvaguardar la confidencialidad.

- Política de Seguridad de la Información.
- Política de Clasificación y Manejo de la Información.
- Política de Control de Acceso.
- Política de Gestión de Incidentes de Seguridad.
- Política de Seguridad Física y Ambiental.
- Política de Uso Aceptable de Recursos.
- Política de Protección de Datos Personales.
- Política de Backup y Recuperación ante Desastres.
- Política de Seguridad en Proveedores y Terceros.
- Política General de Seguridad y Privacidad de la Información.
- Política de Derecho de Autor y Autorización de Uso de Contenidos.

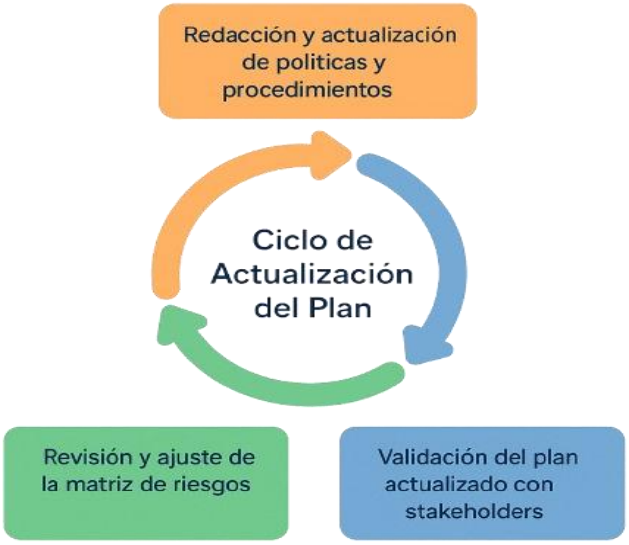
5.1.5 Matriz de responsabilidades (RACI).

Política	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Política General.	Gestión Administrativa, Documental y TIC.	Comité Institucional de Gestión y Desempeño	Oficina Jurídica y Oficina de Planeación.	Funcionarios de planta y contratistas.
Gestión de Riesgos.	Gestión Administrativa, Documental y TIC.	Comité Institucional de Gestión y Desempeño.	Oficina de Planeación.	Dirección Administrativa.
Control de Accesos.	Gestión Administrativa, Documental y TIC.	Comité Institucional de Gestión y Desempeño	Directores de Área.	Funcionarios de planta y contratistas.
Clasificación de Información.	Gestión Administrativa, Documental y TIC.	Comité Institucional de Gestión y Desempeño	Oficina de Planeación.	Dueños de información.
Backup y Recuperación.	Gestión Administrativa, Documental y TIC.	Comité Institucional de Gestión y Desempeño	Gestión Administrativa, Documental y TIC.	Directores de área.
Gestión de Incidentes.	Gestión Administrativa, Documental y TIC.	Gestión Administrativa, Documental y TIC.	Gestión Administrativa, Documental y TIC.	Todos.
Proveedores y Terceros.	Dirección Administrativa.	Comité Institucional de Gestión y Desempeño	Gestión Administrativa, Documental y TIC, Oficina Jurídica.	Proveedores.
Seguridad Física y Ambiental.	Infraestructura.	Comité Institucional de Gestión y Desempeño	Gestión Administrativa, Documental y TIC.	Todos los funcionarios.
Tratamiento de Datos Personales.	Gestión Administrativa, Documental y TIC, Oficina Jurídica.	Comité Institucional de Gestión y Desempeño	Oficina Jurídica.	Titulares de datos.
Protección de Datos Personales.	Gestión Administrativa, Documental y TIC, Oficina Jurídica.	Comité Institucional de Gestión y Desempeño	Mesa de Servicios.	Todos los funcionarios.

5.2 Fase 2: Actualización

5.2.1 Redacción y actualización de políticas y procedimientos.

Basado en los hallazgos del diagnóstico, se actualizarán las políticas y procedimientos para adaptarlos a las nuevas normativas, riesgos identificados y mejores prácticas. Esto incluye la incorporación de medidas de seguridad, privacidad y procedimientos claros de respuesta ante incidentes.



5.2.2 Revisión y ajuste de la matriz de riesgos.

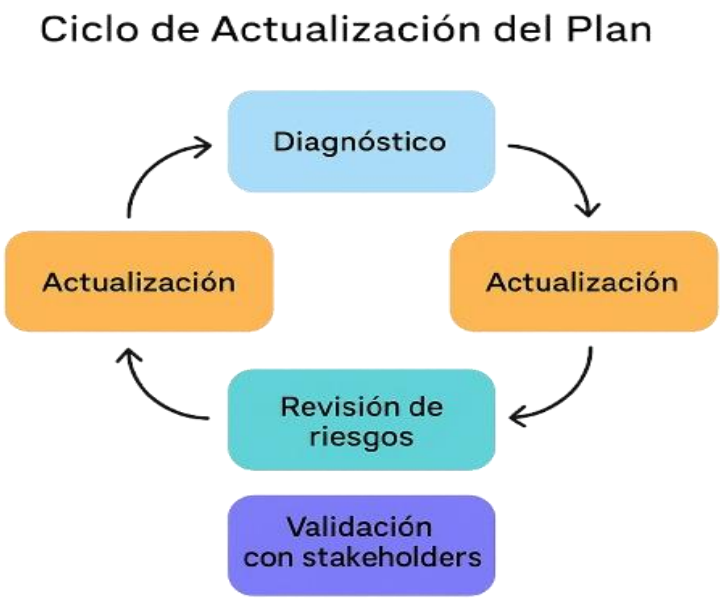
Se realizará la actualización de la matriz de riesgos, evaluando cada riesgo identificado, su nivel de impacto y la eficacia de los controles actualmente implementados. Adicionalmente, se ajustarán o incorporarán nuevos controles con el propósito de mitigar los riesgos emergentes detectados durante la fase de diagnóstico.

- Ver anexo – FOR-GDO-03-01 MATRIZ_RIESGOS_SEGURIDAD_INFORMACIÓN.xlsx

5.2.3 Validación del plan actualizado con stakeholders.

Una vez actualizado el plan, se revisará con los stakeholders clave, como la Secretaría General, Dirección Administrativa, Oficina de Planeación, Oficina Jurídica, Oficina de control interno, dirección de planes parciales, la Dirección Financiera, Dirección de Desarrollo, Dirección de

Proyectos, Subgerencia, Dirección de Planes Parciales y la Oficina Asesora de Coordinación, Seguimiento y Control para asegurar que los cambios sean aplicables, viables y estén alineados con las expectativas y necesidades de la empresa. Este proceso incluirá sesiones de retroalimentación y ajustes finales definidas en el acta de reunión.



5.3 Fase 3: Implementación.

5.3.1 Comunicación y publicación del plan actualizado.

Una vez aprobada la actualización del Plan de Seguridad y Privacidad de la Información por el Comité Institucional de Gestión y Desempeño de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E., se procederá con su divulgación oficial a toda la empresa. Para ello, se emitirán comunicaciones internas que informen de manera clara las principales actualizaciones y su impacto en las funciones del personal. Asimismo, el documento será publicado en los canales institucionales, como la página web institucional, garantizando su accesibilidad y consulta permanente por parte de todos los colaboradores.

5.3.2 Capacitación y sensibilización.

Se diseñará y ejecutará un programa de capacitación para asegurar que todos los empleados comprendan las políticas y procedimientos actualizados. Esto incluirá talleres y módulos en línea sobre seguridad y privacidad de la información, con un enfoque en la importancia de proteger los datos y seguir las nuevas pautas.

5.3.3 Monitoreo y mejora continua.

Después de la implementación, se establecerán indicadores clave de desempeño (KPIs) para monitorear el cumplimiento del plan. Además, se programarán monitoreos periódicos para evaluar la efectividad del plan y realizar ajustes si es necesario. Esto incluye una revisión continua de incidentes de seguridad y la adaptación a nuevas amenazas.

Las actividades de trabajo definidas en el Plan de Seguridad y Privacidad de la Información de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E, incluyen en su propuesta de trabajo las políticas definidas, el ciclo de actualización, la matriz de riesgos, los diagramas creados y la estructura del SGSI alineado a normas como ISO/IEC 27001:2022, ISO/IEC 27701:2025 y la Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y parcialmente por el Decreto 1081 de 2015.

Información detallada de las actividades a ejecutar dentro del plan de seguridad y privacidad de la información.

Actividad	Fecha inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Realizar diagnóstico de evaluación del cumplimiento del MSPI.	Febrero	Diciembre	Dirección administrativa.	Autodiagnóstico MSPI.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Autodiagnóstico diligenciado.
Revisión y apropiación de procedimientos de seguridad y privacidad de la información.	Febrero	Diciembre	Dirección administrativa.	Dominios de la norma 27001:2013.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Documento
Actualización del plan de sensibilización.	Febrero	Diciembre	Dirección administrativa.	Plan sensibilización seguridad de la información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Matriz de sensibilización de seguridad de la información.

Actividad	Fecha inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Ejecución del plan de sensibilización.	Febrero	Diciembre	Dirección administrativa.	Plan sensibilización seguridad de la información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Informe de ejecución.
Actualización de activos de información.	Marzo	Diciembre	Dirección administrativa.	Activos de información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Matriz de activos.
Identificación y actualización del análisis de riesgos de seguridad de la información	Marzo	Diciembre	Dirección administrativa.	Riesgos seguridad de información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Matriz de activos
Tratamiento de riesgos de seguridad de la información	Marzo	Diciembre	Dirección administrativa.	Riesgos seguridad de información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Actas, correos electrónicos

Actividad	Fecha inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Actualización indicadores de gestión SGSI.	Marzo	Diciembre	Dirección administrativa.	Indicadores de gestión.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Hoja de vida de indicadores
Reportes indicadores de gestión SGSI.	Marzo	Diciembre	Dirección administrativa.	Indicadores de gestión.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Hoja de vida de indicadores
Comunicación de riesgos de seguridad de la información	Abril	Diciembre	Dirección administrativa.	Riesgos de seguridad de la información	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Actas, correos electrónicos.
Revisión de controles de la norma ISO 270001:2022.	Mayo	Diciembre	Dirección administrativa.	Dominios de norma 270001:2013.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Declaración de aplicabilidad.

Actividad	Fecha inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Seguimiento y revisión de riesgos de seguridad.	Julio	Diciembre	Dirección administrativa.	Riesgos de seguridad de la información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Informes.
Revisión y actualización del inventario de activos (software - hardware).	Agosto	Diciembre	Gestión Administrativa, Documental y TIC.	Mantenimiento / revisión.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Inventario actualizado.
Evaluación y análisis de riesgos del portal web.	Agosto	Diciembre	Gestión Administrativa, Documental y TIC.	Diagnóstico.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Informe de evaluación del estado de la página web.
Actualización de la matriz de riesgos.	Agosto	Diciembre	Gestión Administrativa, Documental y TIC.	Actualización técnica.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Matriz de riesgos revisada y validada.

Actividad	Fecha inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Actualización de políticas de seguridad y privacidad de la información.	Agosto	Diciembre	Oficina Jurídica / Gestión Administrativa, Documental y TIC.	Actualización / mejora.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Documento de Políticas ajustadas.
Capacitación y sensibilización en seguridad, privacidad y uso aceptable.	Agosto	Diciembre	Dirección Administrativa / Gestión Administrativa, Documental y TIC.	Formación / sensibilización.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Registro de asistentes, evaluaciones y material de formación.
Publicación activos de información.	Diciembre	Diciembre	Comunicaciones.	Activos de Información.	Cumplimiento del 100 % en el desarrollo de la actividad.	1 Matriz de activos.

6 DOCUMENTOS Y/O REGISTROS REFERENCIADOS

Fase	Entregable
Diagnóstico.	Revisión y diagnóstico del Plan de Seguridad y Privacidad de la Información vigente, análisis de brechas (Informe y diagnóstico de hardware y software EDRU E.I.C.E) y matriz de riesgos.
Actualización.	Redacción y actualización de políticas y sus procedimientos, ajuste de la matriz de riesgos.
Implementación.	Validación del plan con stakeholders, aprobación final del plan. Comunicación del plan, capacitación, y establecimiento de monitoreo.

7 ANEXOS

- POL-DPI-01-03 POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- FOR-GDO-03-01MATRIZ_RIESGOS_SEGURIDAD_INFORMACIÓN
- Informe y diagnóstico de hardware y software EDRU E.I.C.E.

8 CONTROL DE CAMBIOS

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

Elaborado por:	Revisado por:	Comité Institucional de Gestión y Desempeño		Resolución de Adopción	
		No Acta.	Fecha:	No.:	Fecha de expedición:
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	10.1.2.007-2025	05-dic-2025	10.15-115-2025	10-dic-2025