

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

TABLA DE CONTENIDO

INTRODUCCIÓN	3
OBJETIVO DEL PLAN	4
ALCANCE Y APLICABILIDAD	5
MARCO NORMATIVO Y REFERENCIAL	7
TÉRMINOS Y DEFINICIONES	10
CONTEXTO ORGANIZACIONAL Y TECNOLÓGICO	12
PRINCIPIOS DEL PLAN DE RECUPERACIÓN ANTE DESASTRES	15
GOBERNANZA, ROLES Y RESPONSABILIDADES	18
INFRAESTRUCTURA TECNOLÓGICA CRÍTICA.....	21
INVENTARIO DE ACTIVOS Y DEPENDENCIAS DE SERVICIOS.....	24
EVALUACIÓN DE RIESGOS Y ESCENARIOS DE DESASTRE	28
ESTRATEGIA GENERAL DE RECUPERACIÓN ANTE DESASTRES.....	31
NIVELES DE SEVERIDAD Y ESCALAMIENTO DE INCIDENTES MAYORES	35
PROCEDIMIENTOS DE ACTIVACIÓN DEL DRP	39
FASES DEL PROCESO DE RECUPERACIÓN	42
CENTROS DE PROCESAMIENTO DE DATOS (CPD) Y SITIOS ALTERNOS .	45
MECANISMOS DE RESPALDO Y REPLICACIÓN DE INFORMACIÓN	48
GESTIÓN DE COMUNICACIONES DURANTE UN DESASTRE	51
GESTIÓN DE PROVEEDORES Y SERVICIOS EXTERNOS CRÍTICOS	55
PLAN DE COORDINACIÓN OPERATIVA Y LOGÍSTICA.....	58
VALIDACIÓN TÉCNICA POST-RECUPERACIÓN	61
PROCEDIMIENTOS DE CIERRE Y RETORNO A LA NORMALIDAD	63
DOCUMENTACIÓN, EVIDENCIAS Y REPORTES POST-EVENTO	66
PROGRAMA DE PRUEBAS (TESTING Y SIMULACROS TÉCNICOS)	70
CAPACITACIÓN Y COMPETENCIAS DEL PERSONAL TÉCNICO	73
GESTIÓN DE CAMBIOS Y CONTROL DE VERSIONES.....	76

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

REVISIÓN, ACTUALIZACIÓN Y MEJORA CONTINUA DEL DRP 79



	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Introducción

El Plan de Recuperación ante Desastres (DRP) constituye un instrumento estratégico y técnico de EPC orientado a garantizar la recuperación ordenada, segura y oportuna de los servicios tecnológicos e informáticos que soportan la operación institucional, en caso de presentarse un desastre, incidente mayor o interrupción grave de la infraestructura tecnológica.

Su objetivo es restablecer los servicios críticos de TI dentro de los tiempos definidos en el Análisis de Impacto al Negocio (BIA), proteger la integridad de la información y reducir al mínimo las pérdidas operativas, reputacionales y financieras derivadas de eventos disruptivos, el DRP se integra como componente operativo del Sistema de Continuidad del Negocio, complementando los lineamientos del Plan de Continuidad del Negocio (PCN), con un enfoque específico en la recuperación técnica de la infraestructura de Tecnologías de la Información (TI), los sistemas de información, los servicios de red, las plataformas en la nube y los datos institucionales.

Este plan define los procedimientos detallados, responsabilidades, recursos, herramientas y mecanismos de comunicación necesarios para garantizar una respuesta estructurada y eficaz frente a contingencias de tipo tecnológico, físico o ambiental que afecten la disponibilidad de los servicios digitales de la entidad, el DRP de EPC está diseñado sobre los principios de resiliencia tecnológica, redundancia, recuperación automatizada y seguridad de la información, aplicando las mejores prácticas internacionales en gestión de desastres y ciberseguridad.

Su estructura metodológica se basa en las siguientes directrices:

- Identificación de infraestructuras tecnológicas críticas y dependencias operativas esenciales.
- Evaluación de riesgos de indisponibilidad, basados en la matriz GTI-F457 y los resultados del BIA.
- Establecimiento de niveles de servicio (RTO y RPO) para cada sistema o aplicación crítica.
- Definición de estrategias de respaldo, replicación y restauración de datos.
- Procedimientos para la activación, ejecución y cierre del proceso de recuperación.
- Mecanismos de comunicación, documentación y registro de evidencias técnicas.

El plan contempla escenarios de desastres tanto de origen físico (incendios, inundaciones, fallas eléctricas, sismos o daños en el CPD), como de origen lógico o

cibernético (ataques ransomware, pérdida de integridad de datos, intrusiones o corrupción de sistemas), asimismo, incluye procedimientos específicos para la recuperación de plataformas on-premise y en la nube, integrando servicios de respaldo DRaaS (Disaster Recovery as a Service) contratados por la entidad.

El DRP es un documento vivo y adaptable, sujeto a revisiones y pruebas periódicas, cuyo mantenimiento permanente garantiza su efectividad y alineación con la infraestructura tecnológica en evolución, su ejecución recae en el Coordinador de Tecnologías de la Información, quien lidera las acciones técnicas con apoyo de la Mesa de Ayuda (MDA) y los proveedores estratégicos de servicios tecnológicos, bajo la supervisión de la Dirección de Planeación y en articulación con las demás áreas institucionales.

La implementación de este plan refleja el compromiso institucional de EPC con la resiliencia digital, la seguridad operativa y la protección de la información pública, asegurando que los servicios esenciales permanezcan disponibles o sean recuperados con la menor afectación posible para los ciudadanos, usuarios y partes interesadas.

Objetivo del Plan

El Plan de Recuperación ante Desastres (DRP) tiene como objetivo principal garantizar la restauración oportuna, segura y ordenada de los servicios tecnológicos críticos de EPC, en caso de presentarse un evento disruptivo que afecte la infraestructura tecnológica, los sistemas de información o los datos institucionales, el propósito fundamental del plan es minimizar el impacto operativo, reputacional, financiero y legal derivado de incidentes que comprometan la disponibilidad, integridad o confidencialidad de la información, asegurando la continuidad del servicio público y el cumplimiento de la misión institucional.

Este objetivo se materializa mediante la implementación de procedimientos técnicos estandarizados que permitan:

- Restablecer los servicios tecnológicos esenciales dentro de los tiempos definidos como aceptables (RTO – *Recovery Time Objective* y RPO – *Recovery Point Objective*), de acuerdo con el Análisis de Impacto al Negocio (BIA) y la Matriz GTI-F457 de Riesgos de Seguridad de la Información.
- Asegurar la integridad y disponibilidad de los datos a través de mecanismos de respaldo, replicación y verificación de consistencia.
- Definir roles y responsabilidades técnicas, operativas y administrativas para la ejecución coordinada del proceso de recuperación.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Establecer protocolos de comunicación y coordinación entre el Coordinador de TI, la Mesa de Ayuda (MDA), los líderes de proceso y los proveedores estratégicos durante las fases del restablecimiento.
- Optimizar el uso de los recursos tecnológicos, humanos y logísticos disponibles, priorizando los sistemas misionales y de apoyo de mayor criticidad.
- Implementar medidas preventivas y correctivas orientadas a reducir el tiempo de indisponibilidad y evitar la pérdida de información o daño a la infraestructura tecnológica.
- Documentar y evaluar cada fase del proceso de recuperación, garantizando la trazabilidad y la mejora continua del plan.

El DRP busca mantener la resiliencia operativa y tecnológica de EPC ante situaciones imprevistas que afecten su infraestructura de TI, consolidando un marco de gestión basado en la anticipación, la respuesta eficiente y la recuperación controlada, en cumplimiento de las políticas nacionales de gobierno y seguridad digital.

Alcance y Aplicabilidad

El Plan de Recuperación ante Desastres (DRP) aplica a todas las infraestructuras tecnológicas, sistemas de información, servicios de red, plataformas en la nube y activos de información gestionados por EPC, cuya interrupción pudiera comprometer la continuidad de los procesos institucionales misionales, estratégicos o de apoyo.

El alcance incluye los recursos técnicos, humanos, físicos y contractuales necesarios para la restauración de los servicios críticos dentro de los tiempos de recuperación establecidos (RTO y RPO), así como los mecanismos de comunicación, documentación y coordinación requeridos durante un evento de desastre o incidente mayor.

Cobertura del Plan

El DRP cubre los siguientes componentes:

1. Centro de Procesamiento de Datos (CPD) principal, ubicado en la sede administrativa, incluyendo sus servidores físicos, virtuales, sistemas de almacenamiento, redes, energía y climatización.
2. Servicios en la nube y plataformas híbridas, tales como correo institucional, colaboración, almacenamiento, respaldos y servicios DRaaS (*Disaster Recovery as a Service*).
3. Sistemas de información institucionales críticos, entre ellos:
 - ERP contable y financiero.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Sistema SIG Planeación.
 - Sistema de Gestión de Proyectos (SIA).
 - Sistema Comercial y de Atención al Usuario.
 - Sistema de Gestión Documental Electrónica.
 - Portal Web institucional y servicios de publicación en línea.
4. Redes de comunicación LAN/WAN, VPN y enlaces de Internet, incluyendo equipos de seguridad perimetral, firewalls y routers de misión crítica.
 5. Activos de información críticos identificados en la Matriz GTI-F457, asociados a los procesos estratégicos, misionales y de apoyo.
 6. Equipos de respaldo de energía (UPS y planta eléctrica) y sistemas de climatización redundante.
 7. Proveedores tecnológicos y servicios tercerizados esenciales, vinculados mediante acuerdos de nivel de servicio (SLA) o continuidad (OLA).

Escenarios de Aplicación

El DRP se activa ante la ocurrencia de incidentes o eventos que produzcan la interrupción total o parcial de los servicios tecnológicos, incluyendo, entre otros:

- Eventos físicos: incendios, inundaciones, explosiones, daños estructurales, sismos o fallas en los sistemas eléctricos o de climatización del CPD.
- Eventos tecnológicos: fallas de hardware o software críticas, corrupción de datos, pérdida de respaldos o interrupciones prolongadas de red.
- Eventos cibernéticos: ataques de ransomware, intrusiones, sabotaje digital o explotación de vulnerabilidades que afecten la disponibilidad o integridad de la información.
- Eventos externos: cortes de energía generalizados, pérdida de conectividad de los proveedores de Internet, incidentes regionales o desastres naturales que afecten la sede principal.

Alcance Funcional

El DRP contempla las siguientes funciones operativas:

- Identificación y clasificación de desastres tecnológicos.
- Evaluación de impacto y priorización de servicios críticos.
- Activación del plan y despliegue de recursos técnicos.
- Recuperación de infraestructura física y lógica.
- Restauración de respaldos y verificación de integridad de datos.
- Validación técnica y funcional de sistemas y aplicaciones.
- Comunicación y documentación del proceso de recuperación.
- Retorno controlado a la normalidad y cierre del evento.

Exclusiones

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

El plan no cubre:

- Fallas menores o eventos que puedan ser atendidos mediante soporte operativo habitual.
- Riesgos asociados a servicios externos no administrados por EPC ni bajo su control contractual.
- Procesos no relacionados con los sistemas de información o activos tecnológicos.
- Incidentes sin afectación directa a la disponibilidad o integridad de los servicios institucionales.

En estos casos, se aplicarán los procedimientos del Plan de Continuidad del Negocio (PCN) y los protocolos regulares de la Mesa de Ayuda (MDA).

Aplicabilidad

El DRP aplica a todo el personal técnico, administrativo y contratista que tenga participación directa o indirecta en la gestión, operación o soporte de los sistemas tecnológicos institucionales, su ejecución y cumplimiento es obligatorio durante la ocurrencia de incidentes de severidad alta o crítica, bajo la coordinación del Coordinador de Tecnologías de la Información y el apoyo de la Mesa de Ayuda (MDA), quienes son responsables de la activación, seguimiento y documentación del proceso de recuperación.

Marco Normativo y Referencial

Se establecen las disposiciones legales, estándares técnicos, políticas nacionales y lineamientos institucionales que sustentan la formulación, implementación y mantenimiento del Plan de Recuperación ante Desastres (DRP) de EPC. Su aplicación asegura que las estrategias de recuperación estén alineadas con los marcos regulatorios del Gobierno colombiano, los modelos de gestión de TI y los estándares internacionales de seguridad, continuidad y resiliencia tecnológica.

Normatividad Nacional

El DRP se fundamenta en las siguientes normas, leyes y decretos vigentes en Colombia:

- Constitución Política de Colombia de 1991: artículos 15 y 20 sobre protección de datos e información pública.
- Ley 527 de 1999: define y regula el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.
- Ley 594 de 2000: Ley General de Archivos, aplicable al manejo documental y preservación de la información institucional.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Ley 1266 de 2008 y Ley 1581 de 2012: sobre protección de datos personales y tratamiento de información sensible.
- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC, establece las bases para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Decreto 338 de 2022: refuerza las políticas de seguridad digital, ciberseguridad y protección de la infraestructura crítica nacional.
- Circular 002 de 2022 del MinTIC: establece directrices sobre la gestión de incidentes y planes de continuidad en entidades públicas.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas – DAFP: orienta la identificación, valoración y tratamiento de riesgos institucionales, incluyendo los tecnológicos.
- Guía del Modelo de Seguridad y Privacidad de la Información (MSPI): documento técnico del MinTIC que establece los requisitos mínimos para la implementación de sistemas de gestión de seguridad y continuidad de la información.

Normas y Estándares Internacionales

El DRP adopta los siguientes estándares internacionales, reconocidos por su aplicabilidad en la gestión de continuidad y recuperación tecnológica:

- ISO 22301:2019 – *Security and Resilience – Business Continuity Management Systems*: establece los requisitos para planificar, implementar, mantener y mejorar un sistema de gestión de continuidad del negocio (SGCN).
- ISO/IEC 27031:2011 – *Guidelines for ICT Readiness for Business Continuity*: proporciona directrices específicas para la preparación y recuperación de tecnologías de la información ante incidentes o desastres.
- ISO/IEC 27005:2022 – *Information Security Risk Management*: norma base para la gestión de riesgos de seguridad de la información.
- ISO/IEC 27001:2022 – *Information Security Management Systems (ISMS)*: marco general para establecer, implementar y mantener controles de seguridad de la información.
- ISO/IEC 27002:2022 – *Code of Practice for Information Security Controls*: guía de buenas prácticas para controles técnicos y administrativos aplicables al DRP.
- ISO/IEC 24762:2008 – *ICT Disaster Recovery Services*: directrices específicas para la planificación y provisión de servicios de recuperación ante desastres.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- NIST SP 800-34 Rev.1 – *Contingency Planning Guide for Federal Information Systems*: referencia de mejores prácticas internacionales en planes de contingencia y recuperación de TI.
- PMBOK 7ª Edición – *Project Management Institute*: guía de buenas prácticas para la gestión de proyectos aplicable al diseño, ejecución y mejora del DRP.

Políticas y Lineamientos Institucionales

A nivel interno, el DRP se articula con los siguientes instrumentos de gestión institucional de EPC:

- Política General de Seguridad de la Información (GTI-Plt002): establece los lineamientos de protección, clasificación y tratamiento de la información institucional.
- Plan Estratégico de Tecnologías de la Información (PETI): define la hoja de ruta tecnológica y la infraestructura sobre la cual se soportan las estrategias de recuperación.
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI): orienta la gestión de ciberseguridad, privacidad y protección de activos de información críticos.
- Matriz GTI-F457 de Riesgos de Seguridad de la Información: identifica amenazas, vulnerabilidades y controles asociados a los activos de información de la entidad.
- Modelo de Seguridad y Privacidad de la Información (MSPI): instrumento rector que define las capacidades institucionales en seguridad y resiliencia digital.
- Sistema Integrado de Gestión (SIG): mecanismo de control documental, trazabilidad y mejora continua aplicable al mantenimiento del DRP.
- Análisis de Impacto al Negocio (BIA): insumo que permite definir prioridades de recuperación y tiempos máximos tolerables de inactividad (MTD).

Articulación con Planes y Sistemas Complementarios

El DRP mantiene coherencia e integración con los siguientes sistemas y planes institucionales:

- Plan de Continuidad del Negocio (PCN): establece la estrategia general de continuidad y los procesos organizacionales asociados.
- Planes de Emergencia y Evacuación Institucional: aseguran la protección del personal y la infraestructura física durante eventos críticos.
- Plan de Gestión del Riesgo Institucional: define el marco de identificación, análisis y tratamiento de riesgos corporativos.
- Sistema de Control Interno: supervisa la aplicación de las políticas, procedimientos y controles derivados del DRP.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Plan de Gobierno Digital: orienta la transformación tecnológica segura y sostenible de la entidad.

Referencias Técnicas

El desarrollo del DRP se apoya adicionalmente en documentos técnicos de referencia utilizados como guías para su estructuración, entre ellos:

- Guía MinTIC – Lineamientos para la Implementación del MSPI.
- DAFP – Manual de Gestión Integral de Riesgos.
- ISO/IEC 27001 Annex A – Controles de Seguridad Aplicables.
- NQA – Guía de Implementación para el Control del Anexo A ISO 27001.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas (versión 7).
- Autodiagnóstico MSPI y Activos de Información institucionales actualizados a 2025.

Este marco normativo y referencial proporciona la base legal, técnica y procedimental para la implementación efectiva del Plan de Recuperación ante Desastres (DRP), asegurando que sus estrategias y controles cumplan con las exigencias regulatorias nacionales, las mejores prácticas internacionales y las políticas institucionales de EPC en materia de resiliencia tecnológica y seguridad digital.

Términos y Definiciones

Activo de Información: Recurso tangible o intangible que tiene valor para la entidad y requiere protección, incluyendo datos, documentos, aplicaciones, equipos, infraestructura tecnológica, software, redes y sistemas de comunicación.

Análisis de Impacto al Negocio (BIA): Proceso sistemático para identificar los procesos críticos de la organización, evaluar los impactos que resultan de su interrupción y establecer los tiempos máximos tolerables de inactividad (MTD), así como los objetivos de tiempo y punto de recuperación (RTO y RPO).

Área Alterna de Operaciones: Ubicación física o virtual habilitada temporalmente para la reanudación de servicios y actividades críticas en caso de que las instalaciones principales queden inutilizables o inoperativas.

Backup (Copia de Seguridad): Duplicado de información y configuraciones críticas almacenado en medios físicos o digitales, que permite su restauración en caso de pérdida, corrupción o indisponibilidad.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Centro de Procesamiento de Datos (CPD): Infraestructura física donde se concentran los equipos de cómputo, servidores, sistemas de almacenamiento, energía y comunicaciones que soportan los servicios tecnológicos institucionales.

Coordinador de Tecnologías de la Información (TI): Responsable de la gestión, activación y ejecución del DRP. Dirige las acciones técnicas, supervisa los equipos de recuperación, mantiene la comunicación institucional y garantiza la trazabilidad del proceso.

Contingencia: Evento inesperado que puede afectar la disponibilidad o el funcionamiento normal de los sistemas, servicios o infraestructuras críticas de la entidad.

Copia Fuera de Sitio (Off-site Backup): Respaldo de información almacenado en un sitio físico o digital distinto al CPD principal, utilizado como medida de seguridad para evitar pérdida total de datos ante desastres locales.

Desastre: Evento de gran magnitud que interrumpe de manera total o prolongada los servicios esenciales de la organización y que requiere la activación del DRP para restablecer la operación normal.

Disponibilidad: Propiedad de la información y los sistemas que garantiza su accesibilidad y uso por usuarios autorizados cuando se requiere.

Evento Disruptivo: Situación inesperada que altera el funcionamiento normal de los servicios tecnológicos o afecta su disponibilidad, integridad o confidencialidad.

Infraestructura Crítica de TI: Conjunto de sistemas, redes, servidores, equipos y servicios tecnológicos cuya indisponibilidad puede causar una afectación significativa a la operación institucional.

Mesa de Ayuda (MDA): Equipo técnico operativo responsable de ejecutar las acciones de recuperación, diagnóstico y soporte durante la activación del DRP, en coordinación con el Coordinador de TI.

MTD (Maximum Tolerable Downtime): Tiempo máximo durante el cual un proceso o sistema puede permanecer inactivo antes de generar consecuencias inaceptables para la organización.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

RPO (Recovery Point Objective): Punto en el tiempo hasta el cual deben recuperarse los datos luego de un incidente. Define la cantidad máxima de información que puede perderse sin afectar significativamente la operación.

RTO (Recovery Time Objective): Tiempo máximo aceptable para restablecer un sistema, servicio o proceso después de una interrupción.

Recuperación ante Desastres (DR): Conjunto de procedimientos técnicos orientados a restablecer los servicios tecnológicos, la infraestructura y los datos tras un evento disruptivo que genera una pérdida significativa de disponibilidad o funcionalidad.

Resiliencia Tecnológica: Capacidad institucional para resistir, adaptarse y recuperarse rápidamente de incidentes que afecten la infraestructura tecnológica o los sistemas de información.

Restauración de Sistemas: Proceso mediante el cual se reinstalan, configuran y validan los servicios tecnológicos, datos y aplicaciones luego de una interrupción.

Servidor de Correos Institucional: Sistema propio (on-premise) que permite el envío, recepción y almacenamiento de mensajes de correo electrónico, gestionado por el área de TI y protegido mediante políticas de respaldo y seguridad perimetral.

Sitio Alternativo de Recuperación: Ubicación física o virtual designada para alojar temporalmente los sistemas y servicios críticos mientras se restaura la infraestructura principal.

Sistema Integrado de Gestión (SIG): Plataforma institucional que agrupa los procesos de planeación, gestión de calidad, seguridad de la información y mejora continua, asegurando trazabilidad documental y cumplimiento normativo.

Vulnerabilidad: Debilidad técnica, organizacional o de proceso que puede ser explotada por una amenaza y comprometer la seguridad o disponibilidad de los servicios tecnológicos.

Contexto Organizacional y Tecnológico

EPC es una entidad descentralizada del orden departamental cuya misión principal consiste en la planeación, gestión y ejecución de proyectos de infraestructura, sostenibilidad ambiental y prestación de servicios públicos domiciliarios, principalmente acueducto y alcantarillado, en los municipios de Cundinamarca, la

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

operación de la entidad depende de manera directa de sus sistemas de información, plataformas tecnológicas, infraestructura de red y servicios de comunicación, los cuales garantizan la continuidad administrativa, técnica y operativa de los procesos misionales, de apoyo y de gestión.

La gestión de las Tecnologías de la Información se encuentra bajo la Dirección de Planeación, a través del Coordinador de Tecnologías de la Información (TI) y la Mesa de Ayuda (MDA), quienes actúan como segunda línea de defensa frente a la seguridad digital, la gestión del riesgo tecnológico y la recuperación de servicios en caso de incidentes o desastres, esta estructura permite una toma de decisiones ágil, documentada y trazable en concordancia con las políticas de seguridad, continuidad y mejora continua definidas en el Sistema Integrado de Gestión (SIG).

Dependencia Tecnológica Institucional

EPC cuenta con una infraestructura tecnológica híbrida que integra componentes físicos instalados en su Centro de Procesamiento de Datos (CPD) y servicios alojados en entornos virtualizados y externos.

El CPD principal se encuentra ubicado en la sede administrativa y concentra los siguientes recursos:

- Servidores físicos y virtualizados, dedicados a los sistemas de gestión administrativa, contable, comercial y documental.
- Sistemas de almacenamiento (NAS) configurados con redundancia y esquemas RAID.
- Equipos de seguridad perimetral, incluyendo firewalls, IDS/IPS y controladores de acceso remoto seguro (VPN).
- Red LAN/WAN institucional con segmentación por VLAN y monitoreo constante.
- Planta eléctrica y sistemas UPS que garantizan respaldo energético continuo ante cortes o fluctuaciones.
- Sistema de climatización redundante para mantener condiciones estables de operación en el CPD.
- Servidor de correos institucional, configurado en infraestructura propia (*on-premise*), protegido mediante filtrado antispam, antivirus y políticas de autenticación SMTP/IMAP seguras.

Adicionalmente, la entidad cuenta con servicios de respaldo y alojamiento en nube privada contratada con proveedores certificados, donde se replican los respaldos críticos de los sistemas de información, conforme a la política de copias de seguridad 3-2-1-1-0.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Sistemas de Información Institucionales

Los sistemas de información que soportan los procesos estratégicos, misionales y de apoyo de EPC incluyen:

- SIG Planeación: sistema de seguimiento a la planeación institucional, indicadores y proyectos.
- SIA (Sistema de Gestión de Proyectos): herramienta para la planeación, control y seguimiento de proyectos de inversión y obras.
- Sistema Comercial y de Atención al Usuario: gestiona la información de usuarios, facturación y atención de PQR.
- Sistema de Gestión Documental Electrónica: soporte para la gestión de archivo, correspondencia y trámites documentales.
- Portal Web Institucional: plataforma pública de comunicación, transparencia y atención al ciudadano.
- Aplicaciones internas de soporte y control operativo: sistemas diseñados por la MDA para procesos de mantenimiento, inventarios, gestión de riesgos y seguimiento técnico.

Cada sistema está integrado con la Matriz GTI-F457 de Riesgos de Seguridad de la Información, lo que permite evaluar de forma constante las amenazas, vulnerabilidades y controles asociados a su operación.

Arquitectura de Red y Comunicaciones

La red institucional se encuentra estructurada bajo un modelo de arquitectura jerárquica y segmentada que garantiza disponibilidad, escalabilidad y seguridad.

Los principales componentes incluyen:

- Conectividad LAN/WAN entre las áreas administrativas, financieras, técnicas y operativas.
- Red inalámbrica segura con autenticación por roles.
- Conexiones redundantes de Internet con proveedores distintos para asegurar la continuidad del servicio.
- VPNs seguras para acceso remoto del personal autorizado y contratistas.
- Monitoreo de red mediante herramientas SNMP y gestión centralizada de logs.

Este esquema de comunicaciones permite que el DRP contemple múltiples rutas de recuperación, tanto para restablecer servicios locales como para redirigir tráfico hacia servidores secundarios o entornos alternos.

Dependencia de Servicios Externos

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

EPC mantiene acuerdos con proveedores tecnológicos para la operación de servicios esenciales, tales como:

- Proveedor de Hosting y Respaldo Externo (DRaaS).
- Proveedor de Conectividad y Telecomunicaciones.
- Proveedor de soporte de hardware y mantenimiento de servidores.
- Proveedor de licenciamiento y actualización de software corporativo.
- Proveedor de servicios de seguridad perimetral y monitoreo.

Cada contrato incorpora cláusulas de continuidad, seguridad y confidencialidad, así como acuerdos de nivel de servicio (SLA) y tiempos de recuperación (DRA – *Disaster Recovery Agreement*).

Capacidad Organizacional y Técnica

La capacidad institucional para ejecutar el DRP se basa en la coordinación de infraestructura, seguridad, redes y soporte, liderando la ejecución de los procedimientos de recuperación, el restablecimiento de los servicios críticos y la validación técnica posterior a un incidente, EPC mantiene esquemas de capacitación permanente en continuidad tecnológica, gestión de incidentes, seguridad digital y manejo de crisis, fortaleciendo las competencias del personal involucrado en la activación y ejecución del plan.

Contexto de Riesgo Tecnológico

El análisis de riesgo tecnológico institucional, basado en la Matriz GTI-F457 y en la Guía de Gestión Integral del Riesgo del DAFP, ha identificado amenazas de tipo:

- Cibernético: ransomware, acceso no autorizado, fugas de información.
- Técnico: fallas de hardware, corrupción de bases de datos, malfuncionamiento de software.
- Físico: incendios, inundaciones, cortes de energía, sobrecalentamiento del CPD.
- Operativo: errores humanos, configuraciones incorrectas, pérdida de respaldos.

Estos riesgos son monitoreados de forma continua y tratados mediante controles técnicos y administrativos alineados con los estándares ISO/IEC 27001 e ISO 22301, fortaleciendo la capacidad de respuesta y recuperación institucional.

Principios del Plan de Recuperación ante Desastres

El Plan de Recuperación ante Desastres (DRP) de EPC se rige por un conjunto de principios fundamentales que orientan su diseño, implementación, ejecución y mejora continua, asegurando que las acciones técnicas y administrativas estén alineadas con la estrategia institucional, el marco de gestión del riesgo y la resiliencia

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

organizacional, estos principios garantizan que la recuperación tecnológica se realice bajo criterios de eficiencia, trazabilidad, responsabilidad y sostenibilidad operativa.

Principio de Resiliencia Tecnológica

EPC adopta un enfoque de resiliencia tecnológica, entendido como la capacidad institucional de resistir, adaptarse y recuperarse de eventos disruptivos que afecten su infraestructura o servicios digitales, este principio se materializa en la implementación de arquitecturas redundantes, copias de seguridad verificadas, planes alternos de conectividad, y en la definición de procedimientos que aseguran la continuidad de los servicios esenciales bajo cualquier escenario de desastre.

Principio de Gestión Basada en el Riesgo

Todas las acciones del DRP se sustentan en la gestión basada en riesgo, conforme a los lineamientos de la Guía de Gestión Integral del Riesgo del DAFP, la Matriz GTI-F457, y las normas ISO/IEC 27005 e ISO 31000, esto implica que la planificación de la recuperación prioriza los sistemas, activos y servicios más críticos según su nivel de exposición y su impacto potencial en la operación institucional, las estrategias de restauración, pruebas y controles se diseñan en proporción directa al nivel de riesgo identificado, asegurando una asignación eficiente de recursos.

Principio de Prioridad de Servicios Críticos

El DRP prioriza la recuperación de los procesos y sistemas tecnológicos esenciales para el cumplimiento de la misión institucional, esta priorización se basa en los resultados del Análisis de Impacto al Negocio (BIA), que establece los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) para cada servicio, definiendo la secuencia de restauración y los niveles de interdependencia entre plataformas. De esta forma, se garantiza que los servicios más sensibles, como los sistemas contables, comerciales, de atención al usuario y documentales, sean restablecidos con prioridad.

Principio de Integridad y Seguridad de la Información

Durante todo el proceso de recuperación, EPC asegura la integridad, confidencialidad y disponibilidad de la información institucional, las operaciones de respaldo, restauración y migración de datos deben realizarse bajo entornos controlados, empleando autenticación segura, cifrado de información y verificación de integridad mediante *hashes* o sumas de comprobación, el principio exige que ningún proceso de recuperación comprometa la seguridad digital ni viole las políticas de protección de datos personales establecidas en la Ley 1581 de 2012.

Principio de Responsabilidad Institucional y Coordinación Operativa

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

La ejecución del DRP es una responsabilidad compartida entre el Coordinador de TI, la Mesa de Ayuda (MDA) y los líderes de proceso involucrados, cada participante debe cumplir las funciones definidas en el plan, reportar incidentes oportunamente y documentar las acciones realizadas durante la restauración, este principio garantiza una respuesta coordinada, ordenada y verificable, reduciendo tiempos de recuperación y errores operativos.

Principio de Documentación y Trazabilidad

Toda actividad derivada de la activación o prueba del DRP debe quedar documentada, asegurando su trazabilidad dentro del Sistema Integrado de Gestión (SIG), se deben registrar los procedimientos ejecutados, tiempos de respuesta, responsables, resultados de validaciones y evidencia técnica (capturas, logs, reportes), esta documentación respalda la auditoría interna, las revisiones de control y la mejora continua del plan.

Principio de Mejora Continua

El DRP se concibe como un sistema vivo y adaptable, sujeto a revisión constante en función de los resultados de pruebas, simulacros o incidentes reales. EPC aplica el ciclo PHVA para la mejora del plan, ajustando estrategias, controles y procedimientos conforme a los cambios tecnológicos, normativos u organizacionales.

Principio de Proporcionalidad y Eficiencia

Las estrategias y recursos de recuperación deben ser proporcionales al nivel de riesgo y al impacto potencial de la interrupción, este principio promueve la optimización de recursos técnicos, financieros y humanos, evitando sobredimensionar las soluciones o incurrir en costos innecesarios. EPC prioriza soluciones efectivas, escalables y sostenibles que garanticen el cumplimiento de los objetivos del plan sin comprometer la eficiencia institucional.

Principio de Confiabilidad y Verificación

Todas las acciones de recuperación deben ser verificables, auditables y reproducibles, esto implica que los procedimientos técnicos, los respaldos y las pruebas de restauración deben ejecutarse bajo control de versiones, con validaciones cruzadas y mecanismos de supervisión, el principio asegura que los datos restaurados sean íntegros, completos y operativos antes de reanudar los servicios.

En conjunto, estos principios constituyen la base metodológica del Plan de Recuperación ante Desastres (DRP), garantizando que la respuesta institucional de

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

EPC sea proactiva, controlada y alineada con los estándares internacionales de resiliencia digital y gestión del riesgo tecnológico.

Gobernanza, Roles y Responsabilidades

La gobernanza del Plan de Recuperación ante Desastres (DRP) en EPC se fundamenta en un modelo jerárquico, técnico y participativo que garantiza la claridad en las responsabilidades, la trazabilidad de las decisiones y la eficiencia en la ejecución de las acciones de recuperación, dado el carácter crítico de los servicios tecnológicos para el cumplimiento de la misión institucional, la coordinación, supervisión y activación del DRP se centralizan en el Coordinador de Tecnologías de la Información (TI), quien lidera al equipo técnico de la Mesa de Ayuda (MDA).

Este modelo de gobernanza promueve una estructura de mando clara y una comunicación directa entre los actores técnicos, administrativos y directivos involucrados en la respuesta ante un evento disruptivo.

Estructura de Gobernanza del DRP

La ejecución del DRP se organiza bajo los siguientes niveles de responsabilidad:

Nivel	Responsable Principal
Dirección de Planeación	Dirige la coordinación institucional del DRP. Aprueba la activación del plan ante incidentes mayores. Asegura la disponibilidad de recursos financieros, técnicos y humanos para la recuperación. Supervisa el cumplimiento de los objetivos del plan y aprueba los informes post-incidente.
Coordinador de Tecnologías de la Información (TI) Dirección de Planeación	Actúa como líder del DRP y jefe directo de la Mesa de Ayuda (MDA). Supervisa la ejecución técnica del plan, coordina las fases de activación, restauración y retorno a la normalidad. Garantiza la aplicación de los protocolos, la comunicación con la Dirección de Planeación y la documentación de todo el proceso.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Mesa de Ayuda (MDA)	Equipo técnico-operativo responsable de ejecutar las acciones de recuperación en campo y en entorno digital. Comprende especialistas en infraestructura, seguridad de la información, redes, servidores, bases de datos, soporte y aplicaciones. Ejecuta los procedimientos definidos, valida los resultados y reporta avances al Coordinador de TI.
Líderes de Proceso	Identifican los activos críticos de su área y validan la correcta recuperación de los sistemas y servicios asociados. Colaboran con el equipo TI en la verificación funcional posterior a la restauración. Proveen información de impacto y definen prioridades de atención junto al Coordinador de TI.
Dirección de Planeación – SIG	Asegura la documentación del proceso, el registro de evidencias y la actualización del DRP dentro del Sistema Integrado de Gestión (SIG). Supervisa la trazabilidad de las acciones y coordina la incorporación de mejoras en el plan.
Dirección Jurídica	Brinda acompañamiento legal ante situaciones que puedan implicar responsabilidades contractuales, incidentes de seguridad o afectación de datos personales. Supervisa el cumplimiento de la Ley 1581 de 2012 y la normatividad vigente.
Dirección Control Interno	Verifica que la ejecución del DRP cumpla con los procedimientos establecidos, asegurando la transparencia, el cumplimiento normativo y la disponibilidad de evidencia para auditorías internas o externas.

Responsabilidades Específicas del Equipo TI (Coordinador y MDA)

El Coordinador de TI y la Mesa de Ayuda (MDA) constituyen la unidad técnica ejecutora del DRP, encargada de aplicar las acciones preventivas, reactivas y de restauración de servicios tecnológicos.

Sus principales responsabilidades son:

- Activación del DRP: evaluar la magnitud del incidente y declarar el nivel de severidad (Alto o Crítico) que justifique la activación formal del plan.
- Diagnóstico inicial: identificar los sistemas, servicios o infraestructuras afectadas y estimar el tiempo de recuperación preliminar.
- Restauración técnica: ejecutar las tareas de recuperación de hardware, software, bases de datos y redes, según los procedimientos definidos.
- Validación operativa: comprobar la integridad de los datos restaurados, la estabilidad de los servicios y la disponibilidad de los sistemas.
- Comunicación técnica: mantener informada a la Dirección de Planeación y a los líderes de proceso sobre el estado de recuperación.
- Documentación: registrar cada acción en las bitácoras técnicas, incluyendo fecha, hora, responsable y resultado.
- Gestión de incidentes de seguridad: coordinar las acciones de contención, erradicación y remediación ante ciberataques, en conjunto con los proveedores de seguridad perimetral.
- Coordinación con terceros: gestionar el soporte y las garantías con los proveedores estratégicos (hosting, respaldo, conectividad, hardware, software).
- Levantamiento del servicio: supervisar la validación final y autorizar el retorno controlado a la operación normal.
- Post-incidente: elaborar el informe técnico de cierre, con los hallazgos, tiempos reales de recuperación, lecciones aprendidas y recomendaciones de mejora.

Coordinación Interinstitucional

El DRP requiere la interacción constante entre el equipo TI, las dependencias administrativas y operativas, y los proveedores de servicios tecnológicos. Para asegurar la efectividad del plan, se establecen los siguientes mecanismos de coordinación:

- Canal directo de comunicación entre el Coordinador de TI y la Dirección de Planeación.
- Notificación inmediata a los líderes de proceso sobre incidentes que afecten sistemas o servicios bajo su responsabilidad.
- Convocatoria de soporte especializado con proveedores externos cuando la recuperación exceda las capacidades internas.
- Reporte institucional formal posterior a la ejecución del plan, registrado en el SIG.

Continuidad del Liderazgo Técnico

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

En caso de indisponibilidad del Coordinador de TI, la Mesa de Ayuda (MDA) asume de manera inmediata la dirección operativa del plan, garantizando la continuidad de las acciones técnicas, el integrante con mayor nivel jerárquico o experiencia dentro de la MDA asumirá el rol temporal de liderazgo hasta que se restablezca la coordinación formal.

Responsabilidad Compartida y Mejora Continua

La recuperación ante desastres no es una actividad exclusiva del área de TI, sino un proceso transversal que requiere la participación activa de toda la organización, cada área debe conocer los activos de información bajo su gestión, aplicar las políticas de respaldo y participar en las pruebas y simulacros de recuperación.

De esta forma, EPC fortalece una cultura institucional de responsabilidad compartida, prevención y resiliencia tecnológica.

Infraestructura Tecnológica Crítica

La infraestructura tecnológica crítica de EPC comprende todos los componentes físicos, lógicos y energéticos que permiten la operación continua de los sistemas de información, la comunicación interna y externa, y la gestión administrativa y operativa de la entidad, estos elementos constituyen el núcleo del entorno informático institucional y su protección, redundancia y mantenimiento son prioritarios dentro del marco del Plan de Recuperación ante Desastres (DRP).

El DRP reconoce como infraestructura tecnológica crítica aquella que, en caso de falla o pérdida de disponibilidad, puede comprometer la prestación de los servicios institucionales, la integridad de la información, o la seguridad digital de la organización.

Centro de Procesamiento de Datos (CPD) Principal

El CPD principal se encuentra ubicado en la sede administrativa de EPC y actúa como el punto central de procesamiento, almacenamiento y gestión de información institucional, está diseñado bajo principios de seguridad física, redundancia eléctrica y control ambiental, y alberga los siguientes componentes:

- Servidores físicos y virtualizados:
 - Equipos configurados con redundancia RAID, balanceo de carga y virtualización mediante *hypervisores* para optimizar recursos.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Alojamiento de sistemas críticos como el ERP contable-financiero, el SIG Planeación, el SIA, el sistema de gestión documental y el sistema comercial.
- Sistemas de almacenamiento (NAS y SAN):
 - Cabinas con capacidad de alta disponibilidad (HA), replicación síncrona y asíncrona.
 - Configuración de snapshots automáticos para restauración rápida.
- Sistemas de energía y respaldo eléctrico:
 - UPS trifásicas con autonomía mínima de 30 minutos.
 - Planta eléctrica de respaldo con capacidad para sostener la operación del CPD en contingencia prolongada.
 - Sistema de transferencia automática (ATS) y supresores de picos eléctricos.
- Control ambiental y climatización:
 - Aire acondicionado redundante (N+1), sensores de temperatura y humedad.
 - Monitoreo automatizado y alarmas ante variaciones fuera de umbral.
- Seguridad física:
 - Control de acceso biométrico al CPD y registro de ingreso mediante bitácora.
 - Cámaras de videovigilancia (CCTV) con grabación continua.
 - Sistema contra incendios con detectores de humo y gas FM200.
- Red LAN y segmentación de tráfico:
 - Estructura jerárquica con *switches* de núcleo y acceso.
 - VLAN por áreas funcionales (administrativa, financiera, técnica, MDA, etc.).
 - Control de tráfico, priorización de servicios críticos y redundancia de enlaces.

Servidor de Correos Institucional

EPC administra un servidor de correos propio (on-premise) que opera sobre infraestructura dedicada y bajo protocolos de seguridad perimetral.

El servicio está protegido mediante:

- Autenticación segura (TLS, SMTP AUTH).
- Filtrado antispam y antivirus.
- Políticas de retención y respaldo diario de buzones.
- Monitoreo de puertos, tráfico y actividad anómala.
- Integración con el sistema de autenticación institucional.

Este servicio es considerado crítico para la comunicación interna y externa de la entidad, por lo que cuenta con respaldos automáticos diarios y copia fuera de sitio semanal.

Sistemas de Seguridad y Protección Perimetral

La infraestructura de seguridad perimetral protege la red institucional y los sistemas contra accesos no autorizados, intrusiones o ciberataques.

Incluye:

- Firewalls de última generación (NGFW) con inspección profunda de paquetes.
- IDS/IPS (Intrusion Detection/Prevention System) configurados para detección temprana de amenazas.
- VPNs seguras para acceso remoto del personal autorizado.
- Segmentación de red y control de tráfico entre zonas internas.
- Sistemas de monitoreo de logs y alertas (SIEM básico) administrado por la MDA.

Infraestructura de Red y Comunicaciones

El sistema de comunicaciones está estructurado bajo una arquitectura de alta disponibilidad que permite mantener la continuidad operativa en caso de interrupciones parciales.

Los principales elementos son:

- Red LAN/WAN con cableado estructurado categoría 6A.
- Enlaces de Internet redundantes mediante diferentes proveedores.
- Switches gestionables y routers de nivel empresarial configurados en failover.
- VPNs corporativas seguras para trabajo remoto o contingencia.
- Servidores de nombres (DNS) redundantes para resolución interna y externa.
- Telefonía IP institucional integrada a la red de datos.

La infraestructura cuenta con monitoreo activo de conectividad y desempeño, realizado por la Mesa de Ayuda (MDA) a través de sistemas de supervisión de red.

Sistema de Respaldo y Almacenamiento Externo

EPC implementa una política de copias de seguridad 3-2-1-1-0, que garantiza tres copias de los datos en dos medios diferentes, una copia fuera del sitio, una copia inmutable y cero errores en la verificación.

Características del sistema de respaldo:

- Respaldos automáticos diarios de servidores, bases de datos y configuraciones críticas.
- Copia de seguridad incremental y completa según cronograma.
- Almacenamiento en NAS local y repositorio externo cifrado (off-site).

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Verificación automatizada de integridad mediante comparación de *hashes*.
- Pruebas periódicas de restauración para validar la disponibilidad de los datos.

Infraestructura Alternativa y Recuperación

En caso de pérdida total del CPD principal, EPC dispone de un sitio alternativo de recuperación, configurado para recibir respaldos y desplegar servicios críticos temporalmente.

Este entorno cuenta con:

- Hardware disponible para restauración prioritaria de sistemas esenciales.
- Acceso remoto seguro mediante VPN para el personal técnico.
- Copias actualizadas de configuraciones y licencias de software.
- Capacidad de conexión a los repositorios de respaldo remoto.

El sitio alternativo puede activarse en un tiempo máximo de 8 horas tras la declaración del evento de desastre.

Monitoreo, Alertas y Supervisión Técnica

La infraestructura cuenta con herramientas de monitoreo activo para detección temprana de fallas, consumo de recursos y estado de servicios críticos.

Los mecanismos implementados incluyen:

- Monitoreo SNMP de equipos de red y servidores.
- Alertas automáticas por correo institucional ante fallos o sobrecargas.
- Supervisión de uso de CPU, RAM, almacenamiento y tráfico de red.
- Revisión diaria de respaldos y logs por la MDA.
- Reportes semanales de disponibilidad de servicios.

Esta infraestructura tecnológica constituye el pilar operativo del Plan de Recuperación ante Desastres (DRP), su mantenimiento, protección y documentación constante son esenciales para asegurar que las estrategias de recuperación se ejecuten con eficacia, permitiendo a EPC restaurar la operación institucional con los menores tiempos de interrupción posibles y con total integridad de la información.

Inventario de Activos y Dependencias de Servicios

El Inventario de Activos y Dependencias de Servicios constituye el insumo operativo fundamental para la ejecución del Plan de Recuperación ante Desastres (DRP), al permitir identificar los componentes tecnológicos, aplicaciones, servicios y recursos sobre los cuales se deben ejecutar las acciones de recuperación, este inventario integra los activos físicos, lógicos, de información, humanos y de soporte que intervienen en la operación tecnológica de EPC, vinculándolos con los procesos institucionales estratégicos, misionales y de apoyo.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

El objetivo principal es garantizar que todos los activos críticos estén debidamente registrados, clasificados, protegidos y asociados a su proceso funcional correspondiente, permitiendo priorizar su restauración conforme a los niveles de criticidad y tiempos de recuperación definidos en el BIA (Análisis de Impacto al Negocio).

Clasificación General de Activos

Los activos tecnológicos e informáticos se agrupan en las siguientes categorías, en concordancia con el MSPI y la norma ISO/IEC 27001:

1. Activos de información: bases de datos, documentos electrónicos, registros operativos, respaldos y reportes institucionales.
2. Sistemas de información y software: SIG Planeación, SIA, sistema comercial, sistema documental y demás aplicaciones institucionales.
3. Infraestructura tecnológica: servidores físicos y virtuales, NAS, firewalls, routers, switches, UPS, y climatización del CPD.
4. Servicios tecnológicos: red LAN/WAN, VPN, servidor de correos institucional, Internet, DNS, y servicios de hosting y respaldo externo.
5. Recursos humanos: personal técnico (Coordinador de TI y MDA) y usuarios con privilegios administrativos.
6. Proveedores y servicios tercerizados: contratos de soporte, mantenimiento, telecomunicaciones, respaldo externo y seguridad perimetral.

Cada activo es evaluado en términos de confidencialidad, integridad y disponibilidad (CID), asignándole un nivel de criticidad (Alta, Media o Baja) según su impacto potencial sobre la operación.

Activos Críticos Asociados a los Procesos Institucionales

Los activos críticos vinculados a los procesos institucionales, de acuerdo con el Mapa de Procesos de EPC, son los siguientes:

Proceso Institucional	Activo de Información o Servicio Tecnológico	Tipo de Activo	Nivel de Criticidad	Dependencias Asociadas
Dirección de Planeación	Sistema SIG Planeación	Software de Información	Alta	Servidor SIG, NAS principal, respaldo off-site
Gestión de Proyectos (SIA)	Sistema de Gestión de Proyectos	Software de Base de datos	Alta	Servidor SIA, VPN,

				almacenamiento redundante
Gestión Comercial	Sistema de Atención al Usuario	Software / Base de datos	Alta	Servidor Comercial, VPN, base de datos SQL
Gestión Documental	Sistema de Gestión Documental Electrónica	Software / Información	Alta	Servidor documental, NAS, respaldo incremental
Gestión Jurídica	Repositorio de Contratos y Normograma Digital	Información / Documentos	Media	NAS, respaldo documental, servidor de archivos
Gestión Administrativa	Sistema de Inventarios y Activos Fijos	Software / Base de datos	Media	Servidor compartido, almacenamiento interno
Gestión del Talento Humano	Sistema de Nómina y Control de Asistencia	Software / Información	Alta	Servidor de nómina, respaldos cifrados
Gestión de Comunicaciones	Servidor de Correos Institucional	Servicio / Software	Alta	Firewall, DNS, NAS, respaldos diarios
Atención al Ciudadano	Portal Web Institucional	Servicio / Web Hosting	Media	Servidor web, dominio institucional, proveedor externo
Mesa de Ayuda (MDA)	Sistema de Gestión de Incidentes y Soporte	Software / Base de datos	Alta	Servidor MDA, red LAN interna, respaldo local
Coordinación de TI	Infraestructura del CPD y sistemas de red	Hardware / Infraestructura	Crítica	Planta eléctrica, UPS, firewalls, switches

 EMPRESAS PÚBLICAS DE CUNDINAMARCA S.A. E.S.P.	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Seguridad de la Información	Monitoreo de eventos y logs (SIEM básico)	Software Servicio	/ Alta	Firewall, servidores críticos, red perimetral
Proveedores Estratégicos	Servicios de Hosting y Respaldo Externo (DRaaS)	Servicio Contrato	/ Alta	Enlaces VPN, contratos SLA/DRA vigentes
Control Interno	Sistema de Reportes y Auditoría	Software Información	/ Media	Servidor compartido, base de datos institucional

Dependencias entre Servicios Tecnológicos

El correcto funcionamiento de los sistemas de información depende de una serie de relaciones de dependencia técnica y lógica, que deben considerarse en los procedimientos de recuperación.

Entre las principales dependencias se encuentran:

- SIG Planeación ↔ Servidor SIG ↔ NAS / VPN / DNS interno
- SIA ↔ Servidor SIA ↔ Almacenamiento / VPN / Firewall
- Sistema Documental ↔ Servidor documental ↔ NAS / Climatización del CPD
- Servidor de correos ↔ Firewall / DNS ↔ Internet / respaldo fuera de sitio
- Portal web ↔ Hosting externo ↔ Servidor DNS / proveedor de conectividad
- MDA ↔ Servidor interno ↔ VPN / red LAN / respaldo local

Estas dependencias se documentan en la Matriz de Dependencias de Servicios Tecnológicos, la identificación de interconexiones permite definir los puntos de restauración prioritarios y el orden lógico de recuperación durante un evento de desastre.

Identificación de Puntos Únicos de Falla (SPOF)

Durante el análisis de infraestructura se identificaron los siguientes puntos únicos de falla (Single Point of Failure – SPOF) que pueden afectar la operación si no se controlan adecuadamente:

- Servidor NAS principal sin réplica geográfica inmediata.
- Dependencia de un solo proveedor de conectividad en algunas sedes.
- Ausencia de enlaces redundantes para DNS secundario.
- Dependencia crítica del CPD principal sin sitio alterno automático.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Cada uno de estos puntos cuenta con acciones de mitigación definidas en la estrategia de recuperación (sección 12 del DRP).

Actualización y Control del Inventario

El inventario de activos y dependencias debe mantenerse actualizado trimestralmente por el Coordinador de TI con el apoyo de la MDA, utilizando la base de datos de configuración (CMDB) institucional.

Cada actualización incluirá:

- Incorporación de nuevos activos o servicios.
- Registro de cambios de infraestructura o proveedor.
- Revisión de niveles de criticidad y clasificación CID.
- Validación de respaldos y tiempos de recuperación.

Las versiones del inventario se conservarán en el repositorio del SIG Planeación, con trazabilidad y control de cambios conforme a la política de documentación institucional.

Evaluación de Riesgos y Escenarios de Desastre

La evaluación permite identificar, analizar y valorar los eventos que pueden comprometer la disponibilidad, integridad o confidencialidad de los servicios tecnológicos de EPC, estableciendo el nivel de exposición de la entidad y las medidas necesarias para su mitigación o tratamiento, este análisis se realiza sobre los activos tecnológicos críticos definidos en el Inventario de Activos y Dependencias de Servicios, considerando factores técnicos, físicos, humanos y ambientales, los resultados sirven como insumo para determinar las prioridades de recuperación, los controles preventivos y correctivos, y los planes específicos de respuesta durante la activación del DRP.

Metodología de Evaluación del Riesgo

La evaluación de riesgos tecnológicos en EPC se desarrolla bajo el siguiente enfoque metodológico:

1. Identificación de activos de información y servicios críticos, con base en la matriz GTI-F457 y el inventario actualizado.
2. Determinación de amenazas potenciales, tanto internas como externas, que puedan afectar dichos activos.
3. Identificación de vulnerabilidades que podrían ser explotadas por dichas amenazas.
4. Análisis del riesgo inherente, combinando la probabilidad de ocurrencia con el impacto potencial.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

5. Evaluación del riesgo residual, considerando los controles existentes y la eficacia de los mecanismos de protección.
 6. Definición de acciones de tratamiento, priorizando medidas de prevención, mitigación, transferencia o aceptación según el apetito de riesgo institucional.
- El resultado se representa en una matriz de severidad que clasifica cada riesgo en los niveles Bajo, Medio, Alto o Crítico, según su impacto en la operación tecnológica.

Clasificación de Amenazas

Las principales amenazas identificadas en el entorno tecnológico de EPC se agrupan en cinco categorías:

a. Amenazas Físicas

- Incendios en el CPD o en áreas adyacentes.
- Inundaciones o filtraciones de agua.
- Cortes prolongados de energía eléctrica.
- Daños estructurales por sismo o vibraciones.
- Fallas en el sistema de climatización del CPD.

b. Amenazas Tecnológicas

- Fallas de hardware en servidores, NAS o equipos de red.
- Corrupción de bases de datos o archivos críticos.
- Pérdida de respaldos por errores en la política de copias.
- Saturación de red o caída de servicios por sobrecarga.
- Malfuncionamiento del servidor de correos institucional.

c. Amenazas Cibernéticas

- Ataques de ransomware, malware o phishing.
- Intrusiones o accesos no autorizados a sistemas.
- Explotación de vulnerabilidades no parchadas.
- Denegación de servicio distribuida (DDoS).
- Robo o filtración de información institucional.

d. Amenazas Humanas u Operativas

- Errores de configuración o manipulación de sistemas.
- Eliminación accidental de archivos o respaldos.
- Fallas en la aplicación de procedimientos de seguridad.
- Ausencia de personal técnico clave durante una emergencia.
- Incumplimiento de protocolos por desconocimiento o negligencia.

e. Amenazas Ambientales o Externas

- Fenómenos naturales: tormentas, granizadas, deslizamientos o descargas eléctricas.
- Daños por fluctuaciones de voltaje o descargas atmosféricas.
- Sabotaje o vandalismo externo a la infraestructura.
- Pérdida de conectividad por fallas de proveedores de Internet.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Vulnerabilidades Identificadas

El análisis de vulnerabilidades en la infraestructura de EPC permitió identificar los siguientes aspectos críticos:

- Mantenimiento insuficiente o no planificado de equipos.
- Falta de pruebas periódicas de restauración de respaldos.
- Dependencia de un único proveedor de telecomunicaciones.
- Inexistencia de replicación geográfica activa de NAS.
- Ausencia temporal de personal técnico clave en eventos no programados.
- Insuficiente control de acceso físico al CPD.
- Dependencia de sistemas con licenciamiento desactualizado.

Estas vulnerabilidades se encuentran priorizadas y tratadas en la Matriz GTI-F457, con controles definidos del Anexo A de la ISO/IEC 27001:2022 y planes de mejora continua del PESI.

Evaluación de Probabilidad e Impacto

El nivel de riesgo se determina combinando la probabilidad de ocurrencia del evento con su impacto esperado sobre la operación, siguiendo las escalas de la Guía del DAFP y la ISO/IEC 27005:

Nivel de Probabilidad	Descripción	Valor (%)
Muy Baja	Evento poco probable ($\leq 20\%$)	0.2
Baja	Evento posible, pero poco frecuente ($\leq 40\%$)	0.4
Media	Evento probable ($\leq 60\%$)	0.6
Alta	Evento frecuente o recurrente ($\leq 80\%$)	0.8
Muy Alta	Evento altamente probable ($> 80\%$)	1.0
Nivel de Impacto	Descripción	Valor (%)
Leve	Afectación mínima o transitoria ($\leq 20\%$)	0.2
Moderado	Interrupción parcial de servicios ($\leq 40\%$)	0.4
Mayor	Pérdida temporal de sistemas críticos ($\leq 60\%$)	0.6
Grave	Afectación severa y prolongada ($\leq 80\%$)	0.8
Catastrófico	Pérdida total de servicios o datos ($> 80\%$)	1.0

El nivel de riesgo inherente se obtiene mediante la fórmula:

Riesgo = Probabilidad $\times$ Impacto

y se clasifica como:

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Bajo: 0.00 – 0.20
- Medio: 0.21 – 0.40
- Alto: 0.41 – 0.70
- Crítico: 0.71 – 1.00

Escenarios de Desastre Identificados

El DRP contempla los siguientes escenarios representativos de desastre, priorizados por severidad y frecuencia:

1. Falla total del CPD principal por incendio, inundación o pérdida de energía prolongada.
2. Ataque de ransomware con cifrado de información en servidores críticos.
3. Corrupción masiva de bases de datos en sistemas ERP o SIG Planeación.
4. Pérdida de conectividad institucional por daño simultáneo de enlaces de Internet.
5. Caída del servidor de correos institucional por falla de hardware o intrusión.
6. Falla del sistema de respaldos o pérdida de copias fuera de sitio.
7. Inaccesibilidad de la nube privada o proveedor DRaaS.
8. Sabotaje interno o eliminación intencional de datos críticos.

Cada escenario cuenta con procedimientos específicos de respuesta y recuperación definidos en Procedimientos de Activación y Fases del Proceso de Recuperación.

Evaluación del Riesgo Residual

El riesgo residual se determina después de aplicar los controles técnicos y administrativos vigentes.

En EPC, la reducción del riesgo se logra mediante:

- Implementación de copias de seguridad automáticas e inmutables.
- Segmentación de red y control de accesos.
- Actualización periódica de parches de seguridad.
- Monitoreo continuo del tráfico de red y alertas de intrusión.
- Contratos vigentes de soporte con proveedores críticos.
- Políticas de respaldo y recuperación probadas trimestralmente.

Los riesgos residuales se documentan en la Matriz de Riesgos de Seguridad de la Información (GTI-F457) y son objeto de revisión semestral durante las auditorías de TI y las reuniones de seguimiento de la Dirección de Planeación.

Estrategia General de Recuperación ante Desastres

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

La estrategia general de recuperación constituye el marco operativo del DRP, orientado a restablecer la funcionalidad de los servicios tecnológicos y de información de EPC en el menor tiempo posible, garantizando la integridad de los datos y la continuidad de los procesos institucionales críticos, su enfoque se basa en la resiliencia tecnológica, la redundancia de infraestructura, la disponibilidad de respaldos verificados y la coordinación eficiente entre el Coordinador de TI, la Mesa de Ayuda (MDA) y las demás dependencias involucradas.

Objetivos Estratégicos de Recuperación

La estrategia busca:

- Restablecer los sistemas críticos dentro de los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) definidos en el Análisis de Impacto al Negocio (BIA).
- Reducir la pérdida de información, interrupción de servicios y afectación a la operación institucional.
- Asegurar la integridad, confidencialidad y disponibilidad (CID) de los datos durante y después del proceso de recuperación.
- Proteger la infraestructura física y lógica del Centro de Procesamiento de Datos (CPD) y sus entornos alternos.
- Implementar procedimientos documentados, verificables y repetibles.
- Coordinar las acciones técnicas, logísticas y administrativas para la restauración de servicios bajo control del Coordinador de TI.

Enfoque Estratégico

El DRP de EPC adopta un modelo de recuperación escalonado que permite responder a incidentes de diferente magnitud o severidad, garantizando la continuidad parcial o total de los servicios tecnológicos.

Los niveles de actuación se estructuran así:

Nivel	Escenario Activador	Tipo de Respuesta	Objetivo del Nivel
Nivel 1 – Incidente Crítico Local	Fallas aisladas en servidores o sistemas individuales.	Recuperación inmediata por la MDA.	Restablecer el servicio sin activar el DRP completo.
Nivel 2 – Interrupción Mayor Parcial	Fallas en componentes centrales del CPD o pérdida de un sistema clave.	Activación parcial del DRP.	Restaurar servicios críticos en menos de 8 horas.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Nivel 3 – Desastre Total	Pérdida completa del CPD, incendio, inundación o ransomware masivo.	Activación total del DRP.	Recuperar la infraestructura en sitio alternativo en ≤ 24 horas.
--------------------------	---	---------------------------	--

Cada nivel implica una secuencia de acciones de diagnóstico, priorización, restauración, validación y reporte, conforme a los procedimientos técnicos establecidos en las fases del plan (sección 15).

Principios Técnicos de la Estrategia

La estrategia técnica del DRP se fundamenta en los siguientes principios operativos:

- Redundancia: uso de infraestructura replicada, enlaces alternos y respaldos fuera de sitio para evitar puntos únicos de falla.
- Segregación: separación de ambientes de producción, respaldo y pruebas para evitar propagación de incidentes.
- Automatización: uso de herramientas de respaldo y monitoreo automatizado para acelerar la recuperación y reducir errores humanos.
- Verificación: aplicación de controles de integridad y autenticidad sobre los datos restaurados antes del retorno a la operación.
- Escalabilidad: capacidad de ampliar los recursos de recuperación según la magnitud del desastre.
- Respaldo y validación continua: política 3-2-1-1-0 para garantizar disponibilidad y confiabilidad de los respaldos institucionales.

Priorización de Servicios y Sistemas Críticos

La priorización de recuperación se define en función del nivel de criticidad asignado a cada sistema dentro del BIA y la Matriz GTI-F457, de acuerdo con su impacto en la operación institucional.

Prioridad	Sistema / Servicio Crítico	RTO Máximo	RPO Máximo	Responsable de Recuperación
1	Sistema SIG Planeación	6 horas	2 horas	MDA – Aplicaciones
2	Sistema Comercial y Atención al Usuario	6 horas	1 hora	MDA – Soporte Técnico
3	Sistema de Gestión Documental	8 horas	4 horas	MDA – Infraestructura / Líder Documental
4	Servidor de Correos Institucional	4 horas	1 hora	MDA – Comunicaciones
5	Sistema de Gestión de Proyectos (SIA)	8 horas	2 horas	MDA – Aplicaciones

Calle 24 #51-40, Bogotá
Capital Tower- Piso 7 y 11
Tel: **601 580 16 72** - Código Postal: 111321
Contactenos@epc.com.co
www.epc.com.co

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

6	Portal Web Institucional	10 horas	4 horas	MDA – Redes / Proveedor Hosting
7	Servidor de Archivos y NAS	6 horas	1 hora	MDA – Infraestructura
8	Sistema de Monitoreo y Logs (SIEM básico)	8 horas	2 horas	MDA – Seguridad de la Información

Estrategias Específicas de Recuperación

De acuerdo con los escenarios de desastre evaluados, se definen las siguientes estrategias complementarias:

- Recuperación de infraestructura física: reinstalación de servidores, equipos de red, UPS y climatización en caso de pérdida total del CPD.
- Recuperación lógica: restauración de configuraciones, sistemas operativos, bases de datos y aplicaciones institucionales.
- Recuperación de red y comunicaciones: restablecimiento de conectividad LAN/WAN, VPN y enlaces de Internet.
- Recuperación de datos: restauración desde respaldos locales y off-site, validación de integridad y sincronización de información.
- Recuperación de servicios externos: activación de respaldos contratados con proveedores DRaaS y hosting alterno.

Estas estrategias están documentadas en los procedimientos técnicos (Sección 15) y se validan mediante pruebas de restauración trimestrales.

Coordinación Operativa y Comunicación

Durante la ejecución del DRP, la coordinación operativa se mantiene centralizada en el Coordinador de TI, quien supervisa y autoriza cada fase del proceso, desde el diagnóstico inicial hasta la validación de la restauración.

La Mesa de Ayuda (MDA) se subdivide temporalmente en equipos funcionales:

- Equipo de Infraestructura: hardware, servidores y energía.
- Equipo de Redes y Comunicaciones: conectividad, VPN y servicios externos.
- Equipo de Seguridad y Monitoreo: verificación de logs, ataques o accesos indebidos.
- Equipo de Aplicaciones y Bases de Datos: recuperación de sistemas y pruebas funcionales.

La comunicación con la Dirección de Planeación y los líderes de proceso se realiza mediante canales institucionales seguros, principalmente el servidor de correos interno y, en caso de interrupción, los números de contacto.

Estrategia de Transición y Retorno

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Una vez restaurados los servicios, se aplicará una estrategia de transición controlada que garantice la estabilidad antes del retorno completo a la operación normal.

Incluye:

- Validación funcional y técnica de todos los servicios restaurados.
- Monitoreo durante 48 horas posteriores a la recuperación.
- Actualización de respaldos base post-evento.
- Revisión y ajuste de configuraciones críticas.
- Emisión del Informe Técnico de Recuperación por parte de la MDA.

Integración con el Plan de Continuidad del Negocio (PCN)

El DRP se articula directamente con el PCN, complementando su alcance en la fase tecnológica.

Mientras el PCN define los procesos institucionales que deben continuar, el DRP define cómo restaurar los sistemas y la infraestructura que los soportan. Ambos planes operan bajo un marco metodológico unificado y comparten procedimientos de comunicación, documentación y mejora continua.

Niveles de Severidad y Escalamiento de Incidentes Mayores

El manejo adecuado de un desastre o incidente tecnológico depende de la capacidad institucional para clasificar su severidad, activar los protocolos de respuesta apropiados y escalar oportunamente la atención hacia los niveles técnicos o administrativos competentes, este apartado define los criterios, niveles y procedimientos de escalamiento aplicables en la activación del Plan de Recuperación ante Desastres (DRP), garantizando una respuesta rápida, coordinada y trazable.

Objetivo del Sistema de Clasificación

El sistema de clasificación de severidad tiene por objeto:

- Determinar la magnitud del impacto del incidente sobre los servicios tecnológicos y la operación institucional.
- Establecer los tiempos máximos de respuesta y recuperación según la criticidad del evento.
- Activar el nivel de coordinación adecuado (local, institucional o con proveedores externos).
- Priorizar los recursos técnicos, humanos y logísticos de acuerdo con la gravedad del incidente.
- Facilitar la toma de decisiones informadas por parte del Coordinador de TI y la Dirección de Planeación.

Niveles de Severidad

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

EPC adopta una escala de cuatro niveles de severidad (S1 a S4) que permite clasificar los incidentes de acuerdo con su impacto, alcance y urgencia.

Nivel	Tipo de Evento / Severidad	Descripción	Ejemplos Representativos	Activación del DRP
S1 – Menor (Baja)	Evento sin afectación significativa.	No interrumpe servicios críticos. Puede ser gestionado por la MDA como soporte normal.	Fallo temporal de usuario, error de aplicación menor, saturación puntual de red.	No requiere activación. Soporte regular.
S2 – Moderado (Media)	Evento que afecta parcialmente un servicio institucional.	Impacto limitado a un sistema o dependencia. Requiere intervención técnica prioritaria.	Falla de servidor de impresión, caída temporal de base de datos secundaria.	Activación parcial del protocolo de contingencia.
S3 – Mayor (Alta)	Evento con afectación significativa a varios servicios críticos.	Impacta procesos misionales o sistemas de alto valor. Requiere acción inmediata y coordinación institucional.	Falla del servidor ERP, corrupción de base de datos SIG, caída del correo institucional.	Activación parcial del DRP. Coordinación directa del Coordinador de TI.
S4 – Crítico (Muy Alta / Desastre)	Evento que compromete la infraestructura tecnológica o los datos institucionales.	Interrumpe la operación de toda la entidad. Requiere activar el DRP completo y sitio alterno.	Incendio en el CPD, ransomware generalizado, pérdida total de conectividad.	Activación total del DRP. Coordinación con Dirección de Planeación y proveedores.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Criterios de Clasificación de Severidad

La severidad del incidente se determina evaluando las siguientes dimensiones:

1. Impacto en los servicios institucionales: cantidad y tipo de sistemas afectados.
2. Duración estimada de la interrupción: tiempo previsto de indisponibilidad.
3. Impacto sobre la información: pérdida o corrupción de datos críticos.
4. Dependencias afectadas: número de áreas o usuarios impactados.
5. Requerimiento de recursos externos: necesidad de intervención de proveedores o soporte especializado.

Cada dimensión se califica de 1 (bajo) a 5 (alto) y se obtiene un puntaje total que define el nivel de severidad, conforme a la siguiente escala:

Puntaje Total	Nivel de Severidad	Acción Requerida
5 – 8	S1 (Baja)	Atención por la MDA. Registro en ticket de soporte.
9 – 13	S2 (Media)	Activación de protocolo local. Seguimiento diario.
14 – 18	S3 (Alta)	Activación parcial del DRP. Escalamiento al Coordinador de TI.
19 – 25	S4 (Crítica)	Activación total del DRP. Comunicación inmediata a la Dirección de Planeación.

Escalamiento Técnico y Administrativo

El proceso de escalamiento define los canales y responsables para elevar la atención del incidente de acuerdo con su nivel de severidad.

a. Escalamiento Técnico

- S1–S2: la Mesa de Ayuda (MDA) gestiona el incidente directamente y documenta la acción correctiva.
- S3: el Coordinador de TI asume la dirección del proceso, define la estrategia de recuperación, asigna recursos técnicos y establece comunicación con los líderes de proceso.
- S4: el Coordinador de TI declara formalmente la activación del DRP, notifica a la Dirección de Planeación y coordina con los proveedores estratégicos (respaldo, hosting, telecomunicaciones, hardware).

b. Escalamiento Administrativo

- La Dirección de Planeación evalúa el impacto organizacional, autoriza recursos adicionales y gestiona la comunicación institucional interna y externa.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- La Oficina Asesora Jurídica interviene en caso de incidentes con implicaciones legales o de protección de datos personales.
- La Oficina de Control Interno verifica el cumplimiento de los procedimientos y documenta la trazabilidad del evento.

Tiempos Máximos de Respuesta

Cada nivel de severidad tiene un tiempo máximo de respuesta inicial (TMR) desde la detección del evento hasta el inicio de las acciones de recuperación:

Nivel de Severidad	TMR Máximo	Responsable de Activación
S1	≤ 4 horas	MDA – Técnico asignado
S2	≤ 2 horas	MDA – Supervisor técnico
S3	≤ 1 hora	Coordinador de TI
S4	Inmediato (≤ 30 minutos)	Coordinador de TI / Dirección de Planeación

El cumplimiento de estos tiempos se supervisa mediante los reportes de eventos críticos registrados en el SIG Planeación y en la bitácora técnica de la Mesa de Ayuda (MDA).

Mecanismos de Comunicación en Escenarios Críticos

Durante la ocurrencia de un evento de severidad S3 o S4, se activan los siguientes mecanismos de comunicación prioritaria:

- Canales principales: correo institucional, teléfono directo de coordinación técnica, VPN segura.
- Canales alternos: mensajería cifrada o llamadas móviles, en caso de caída del servidor de correos.
- Mensajes iniciales de alerta: deben contener el tipo de incidente, sistemas afectados, tiempo estimado de recuperación y responsable de la gestión.
- Reporte oficial del evento: emitido por el Coordinador de TI a la Dirección de Planeación con copia al SIG Planeación dentro de las primeras 4 horas.

Registro y Documentación del Incidente

Todo incidente que active el DRP debe quedar documentado mediante un registro técnico que incluya:

- Fecha, hora y descripción del evento.
- Nivel de severidad asignado.
- Sistemas y servicios afectados.
- Acciones de respuesta ejecutadas.
- Tiempos de recuperación reales (RTO alcanzado).

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Evidencias técnicas (logs, capturas, reportes de error).
- Lecciones aprendidas y recomendaciones.

Estos registros forman parte del Informe de Cierre de Evento, incorporado al Sistema Integrado de Gestión (SIG) para auditoría y mejora continua.

Procedimientos de Activación del DRP

La activación del Plan de Recuperación ante Desastres (DRP) es el punto de inicio del proceso formal de restauración de los servicios tecnológicos de EPC, y debe ejecutarse únicamente cuando se verifique una interrupción severa que afecte la disponibilidad o integridad de los sistemas críticos y que no pueda resolverse mediante los procedimientos operativos habituales de la Mesa de Ayuda (MDA), el proceso de activación garantiza que las decisiones se adopten con fundamento técnico, que se asignen responsabilidades claras y que se mantenga comunicación constante entre el Coordinador de TI, la Dirección de Planeación, los líderes de proceso y los proveedores tecnológicos implicados.

Condiciones de Activación

El DRP se activa cuando se presenta alguno de los siguientes escenarios:

1. Pérdida total o parcial del CPD principal debido a incendio, inundación, explosión o daño estructural.
2. Ataque cibernético de alto impacto (por ejemplo, ransomware, denegación de servicio o intrusión masiva) que impida la operación normal de los sistemas institucionales.
3. Falla simultánea de servidores críticos o del sistema de almacenamiento (NAS/SAN) que afecte más de un servicio esencial.
4. Interrupción prolongada de energía eléctrica o conectividad, superior a los tiempos de respaldo disponibles.
5. Corrupción o pérdida masiva de datos, detectada en sistemas misionales o financieros.
6. Caída total del servidor de correos institucional, afectando la comunicación interna y externa.
7. Inaccesibilidad del proveedor de respaldo externo (DRaaS) o pérdida del enlace de replicación.
8. Desastres naturales o eventos externos que impidan el acceso al CPD o al personal técnico.

Criterios para la Declaración de Activación

El Coordinador de TI tiene la autoridad para declarar la activación del DRP cuando se cumplan simultáneamente las siguientes condiciones:

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- El evento afecta uno o más sistemas catalogados como críticos o de alta prioridad en el BIA.
- La MDA no logra restablecer el servicio mediante los procedimientos normales en un tiempo inferior al RTO definido.
- El incidente genera impacto operativo transversal o compromete la integridad de los datos institucionales.
- Se requiere la participación de proveedores externos o el uso del sitio alternativo de recuperación.

La activación debe ser registrada inmediatamente en la bitácora de incidentes críticos, indicando la hora, causa probable, sistemas afectados y personal involucrado.

Secuencia de Activación

Una vez confirmada la necesidad de activar el plan, el proceso se desarrolla en la siguiente secuencia:

Fase 1: Detección y Notificación

- La MDA detecta o recibe la alerta de un evento grave y registra el incidente.
- Se verifica la afectación real y se determina el nivel de severidad (S3 o S4).
- Se notifica de inmediato al Coordinador de TI por los canales establecidos.

Fase 2: Evaluación Inicial del Evento

- El Coordinador de TI evalúa el alcance del incidente, los sistemas afectados y el posible tiempo de recuperación.
- Si la afectación supera la capacidad de resolución local, declara la activación formal del DRP.
- Se convoca al personal técnico necesario y se informa a la Dirección de Planeación.

Fase 3: Declaración Formal de Activación

- El Coordinador de TI comunica oficialmente la activación del DRP mediante correo o mensaje validado, indicando:
 - Naturaleza del incidente.
 - Sistemas afectados.
 - Nivel de severidad.
 - Hora de inicio de la activación.
 - Personal y proveedores involucrados.
- La Dirección de Planeación avala la decisión y coordina la comunicación institucional interna.

Fase 4: Implementación de Procedimientos de Recuperación

- Se ejecutan los procedimientos técnicos establecidos según el tipo de incidente.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- La MDA documenta cada acción, mantiene la trazabilidad del proceso y reporta avances periódicos.
- En caso de pérdida total del CPD, se inicia la restauración en el sitio alternativo conforme a la sección 16.

Fase 5: Seguimiento y Comunicación

- Se realizan reportes de avance cada 2 a 4 horas (según severidad).
- Se informa a los líderes de proceso sobre el estado de los servicios afectados.
- Se documentan los tiempos reales de respuesta y recuperación (RTO alcanzado).

Niveles de Activación del DRP

Nivel de Activación	Escenario Activador	Acciones Clave	Responsable Principal
Parcial	Falla localizada en servidores o aplicaciones críticas.	Recuperación controlada en el CPD principal.	Coordinador TI / MDA
Total	Desastre o pérdida total del CPD o infraestructura principal.	Activación del sitio alternativo, restauración de respaldos y coordinación con proveedores.	Coordinador TI / MDA / Dirección de Planeación

Comunicación de Activación

Una vez declarado el inicio del plan, el Coordinador de TI debe notificar formalmente a los siguientes actores:

- Dirección de Planeación: para validación institucional y gestión de comunicación externa.
- Líderes de Proceso: para informar sobre afectaciones y tiempos estimados de recuperación.
- Proveedores Estratégicos: para activar los servicios de soporte técnico, telecomunicaciones y respaldo.
- Oficina de Control Interno: para registro de auditoría y seguimiento de cumplimiento.

La notificación incluirá los elementos mínimos del evento, priorización de sistemas y medidas adoptadas.

Verificación de Autenticidad y Seguridad en la Activación

Todo proceso de activación deberá verificarse mediante autenticación multifactor (MFA) en los accesos al entorno técnico y validación cruzada de los responsables.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Ninguna acción de restauración podrá iniciarse sin la confirmación del Coordinador de TI, a fin de evitar restauraciones erróneas o duplicadas.

Registro Documental

La Mesa de Ayuda (MDA) deberá registrar en tiempo real todas las acciones ejecutadas durante la activación del plan, incluyendo:

- Hora de inicio y finalización.
- Descripción de actividades realizadas.
- Sistemas involucrados.
- Personal participante.
- Incidencias secundarias o hallazgos técnicos.

Estos registros se consolidan en el Informe de Activación del DRP, documento oficial que alimenta el proceso de revisión posterior y mejora continua del plan.

Cierre de Activación

Una vez restablecidos los servicios y verificada la estabilidad del entorno, el Coordinador de TI emite la orden de cierre de activación, indicando:

- Fecha y hora de normalización de los servicios.
- Resultados de validación técnica.
- Impacto residual (si lo hubo).
- Acciones pendientes y recomendaciones.

El cierre debe ser comunicado a la Dirección de Planeación, a los líderes de proceso y al SIG Planeación para su archivo y seguimiento.

Fases del Proceso de Recuperación

El proceso de recuperación ante desastres en EPC se desarrolla mediante cinco fases secuenciales, diseñadas para garantizar la restauración controlada, documentada y segura de los sistemas tecnológicos críticos, asegurando la continuidad operativa y la integridad de la información institucional, cada una de ellas está asociada a roles específicos, tiempos de respuesta y entregables definidos, bajo la supervisión directa del Coordinador de TI y la ejecución técnica de la Mesa de Ayuda (MDA).

Estas fases son:

Fase 1 – Evaluación del Daño y Diagnóstico Inicial

Objetivo: Determinar la magnitud y alcance del evento que generó la activación del DRP, identificando los sistemas afectados, el tipo de daño, la severidad del impacto y la viabilidad técnica de la recuperación.

Actividades principales:

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Inspección inicial del CPD o infraestructura afectada.
- Identificación de equipos, sistemas o servicios comprometidos.
- Registro de síntomas, causas probables y duración estimada de la afectación.
- Evaluación de la accesibilidad a respaldos, hardware alternativo y personal disponible.
- Clasificación del evento según nivel de severidad (S3 o S4).
- Comunicación del diagnóstico a la Dirección de Planeación.

Responsables: Coordinador de TI / Mesa de Ayuda (Infraestructura).

Tiempo estimado: 1 a 2 horas desde la activación.

Entregable: *Informe Técnico de Evaluación Inicial del Daño.*

Fase 2 – Restauración de Infraestructura Física y Lógica

Objetivo: Reestablecer las condiciones mínimas necesarias para la operación tecnológica mediante la recuperación o sustitución de la infraestructura afectada, tanto física como lógica.

Actividades principales:

- Instalación o reemplazo de servidores físicos dañados.
- Configuración inicial de equipos de red, energía y climatización.
- Instalación del sistema operativo y software base de los servidores.
- Restauración de parámetros de red, DNS, y accesos administrativos.
- Conexión segura con el sitio alternativo o entorno DRaaS si aplica.
- Verificación de disponibilidad de respaldos y volúmenes de almacenamiento.

Responsables: MDA (Infraestructura y Redes) / Coordinador de TI.

Tiempo estimado: 2 a 6 horas dependiendo del alcance del daño.

Entregable: *Informe de Restauración de Infraestructura Física y Lógica.*

Fase 3 – Recuperación de Datos y Sistemas de Información

Objetivo: Restaurar las bases de datos, aplicaciones y configuraciones institucionales desde los respaldos más recientes, garantizando la integridad de la información y la operatividad funcional de los sistemas.

Actividades principales:

- Restauración de respaldos locales o externos (off-site).
- Validación de integridad de archivos mediante sumas hash o CRC.
- Reconstrucción de bases de datos SQL y repositorios documentales.
- Instalación de aplicaciones críticas: ERP, SIG Planeación, SIA, Sistema Documental, Servidor de Correos, MDA, entre otros.
- Configuración de roles, usuarios y privilegios según políticas de seguridad.
- Ejecución de pruebas funcionales básicas por cada sistema.

Responsables: MDA (Aplicaciones y Bases de Datos) / Coordinador de TI.

Tiempo estimado: 4 a 8 horas.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Entregable: *Informe de Recuperación de Datos y Sistemas Críticos.*

Fase 4 – Validación Técnica y Pruebas de Integridad

Objetivo: Asegurar que los servicios restaurados funcionan correctamente, que los datos recuperados son íntegros y que las configuraciones cumplen con las políticas de seguridad y disponibilidad institucionales.

Actividades principales:

- Validación funcional por los líderes de proceso.
- Pruebas de acceso, autenticación, transacciones y consultas.
- Monitoreo del desempeño de CPU, RAM, almacenamiento y red.
- Ejecución de herramientas de auditoría técnica para validar integridad.
- Validación cruzada entre respaldos y datos operativos actuales.
- Documentación de resultados y firma de conformidad técnica.

Responsables: Coordinador de TI / MDA / Líderes de Proceso.

Tiempo estimado: 2 a 4 horas.

Entregable: *Acta de Validación Técnica de Servicios Restaurados.*

Fase 5 – Retorno Controlado a la Operación

Objetivo: Reintegrar los servicios restaurados al entorno de producción, asegurando su estabilidad, monitoreo y normalización progresiva, minimizando el riesgo de reincidencia del evento.

Actividades principales:

- Migración de sistemas restaurados al entorno de producción.
- Monitoreo continuo por un periodo mínimo de 48 horas.
- Actualización de respaldos post-evento (punto de restauración limpio).
- Desactivación del sitio alterno (si aplica) y sincronización final.
- Comunicación de restablecimiento completo a la Dirección de Planeación y usuarios.
- Elaboración del *Informe Final de Recuperación* con métricas alcanzadas (RTO/RPO).

Responsables: Coordinador de TI / MDA.

Tiempo estimado: 6 a 12 horas dependiendo del escenario.

Entregable: *Informe Final de Retorno y Cierre de Recuperación.*

Monitoreo Posterior y Evaluación de Efectividad

Después del retorno a la operación normal, se implementa una etapa de monitoreo y evaluación post-incidente, con el fin de identificar oportunidades de mejora y asegurar la efectividad del DRP.

Actividades:

- Monitoreo de logs y rendimiento de los sistemas.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Registro de incidentes secundarios o anomalías detectadas.
- Revisión de cumplimiento de RTO/RPO frente a objetivos definidos.
- Reunión técnica de lecciones aprendidas con el equipo TI y líderes de proceso.
- Actualización del DRP con las mejoras identificadas.

Responsables: Coordinador de TI / MDA / Dirección de Planeación.

Entregable: *Informe Post-Incidente y Plan de Mejora del DRP.*

Centros de Procesamiento de Datos (CPD) y Sitios Alternos

El Centro de Procesamiento de Datos (CPD) constituye el núcleo tecnológico de EPC, albergando los servidores, sistemas de almacenamiento, comunicaciones, equipos de seguridad perimetral y servicios esenciales que soportan los procesos misionales, administrativos y de apoyo, establece los lineamientos técnicos para la protección, respaldo y recuperación de este entorno, asegurando la continuidad de los servicios críticos mediante la disponibilidad de infraestructuras redundantes, respaldos externos y un sitio alternativo de contingencia.

CPD Principal

El CPD principal de EPC está ubicado en la sede administrativa central y cumple con los estándares básicos de seguridad física, eléctrica y ambiental para el funcionamiento continuo de los sistemas institucionales, su diseño se fundamenta en una arquitectura híbrida y escalable, que combina infraestructura física local con servicios virtualizados y componentes alojados en nube segura.

Componentes principales del CPD:

- Servidores físicos y virtuales: entorno de virtualización VMware y contenedores Linux para sistemas institucionales.
- Almacenamiento (NAS/SAN): configurado en RAID 5/6 con discos SAS de alta disponibilidad.
- Switches y routers de núcleo: con soporte para VLAN, QoS y priorización de tráfico crítico.
- Firewalls de última generación (NGFW): con filtrado por aplicación, IDS/IPS y VPN segura.
- UPS y planta eléctrica: autonomía de 2 horas con transferencia automática.
- Sistema de climatización redundante: temperatura controlada entre 18 °C y 23 °C.
- Sistema de detección y extinción de incendios: sensores térmicos y sistema de gas inerte.
- Control de acceso biométrico: ingreso restringido a personal autorizado de TI y MDA.

Servicios alojados en el CPD principal:

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- ERP Contable y Financiero.
- Sistema SIG Planeación.
- Sistema de Gestión Documental.
- Sistema Comercial y de Atención al Usuario.
- Servidor de Archivos y respaldos automáticos (NAS).
- Plataforma de la Mesa de Ayuda (MDA).

El Coordinador de TI es responsable de la administración general del CPD y de la supervisión de las operaciones de mantenimiento, seguridad y disponibilidad.

Infraestructura Virtual y Servicios en Nube

EPC emplea una infraestructura híbrida que integra servicios locales con plataformas de nube segura para garantizar mayor resiliencia y disponibilidad, estos servicios se utilizan principalmente para respaldo, colaboración institucional y recuperación ante desastres.

Principales servicios en nube:

- Almacenamiento remoto cifrado (off-site): utilizado para copias de seguridad críticas.
- Plataforma de recuperación (DRaaS): provee capacidad de restauración virtual inmediata.
- Correo institucional: gestionado en servidor dedicado con cifrado TLS y autenticación multifactor.
- Aplicaciones de colaboración y productividad: alojadas en entorno seguro controlado por EPC.

El uso de la nube sigue los principios de seguridad de la información, soberanía de datos y continuidad operativa, garantizando que toda la información institucional esté alojada en proveedores con certificaciones ISO/IEC 27001 e ISO 22301.

Sitio Alterno de Recuperación

El sitio alternativo constituye el entorno de respaldo y continuidad tecnológica que permite la restauración de los servicios institucionales en caso de pérdida total o inhabilitación del CPD principal, este sitio puede ser físico o virtual (en la nube), dependiendo del tipo de incidente y la disponibilidad de infraestructura.

Características técnicas del sitio alternativo:

- Ubicación geográfica diferente al CPD principal para mitigar riesgos ambientales o de infraestructura.
- Conectividad segura VPN con el entorno institucional.
- Servidores virtuales preconfigurados con capacidad para asumir servicios críticos.
- Almacenamiento cifrado replicado desde el CPD principal (replicación asíncrona).

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Mecanismo de autenticación controlada y acceso exclusivo para personal autorizado de MDA.
- Respaldo energético autónomo y redundancia de red.
- Capacidad de operación mínima: correo institucional, ERP, sistema documental y portal web.

El sitio alternativo se activa únicamente bajo instrucción del Coordinador de TI, y su uso está sujeto a verificación previa de integridad y sincronización de respaldos.

Mecanismos de Replicación y Sincronización

EPC implementa esquemas de replicación de datos basados en el principio 3-2-1-1-0, que garantiza la disponibilidad y recuperación ante fallos:

- 3 copias de cada dato (producción + dos copias de respaldo).
- 2 medios de almacenamiento diferentes (NAS y nube).
- 1 copia fuera del sitio principal (off-site).
- 1 copia inmutable (no modificable ni cifrable).
- 0 errores detectados tras la verificación de integridad.

La replicación se realiza de forma asíncrona cada 6 horas para datos operativos y sincrónica para bases de datos críticas, asegurando una pérdida máxima tolerable (RPO) de 1 hora, los respaldos se validan diariamente mediante pruebas automáticas de restauración parcial.

Gestión de Mantenimiento y Pruebas del CPD

El mantenimiento preventivo y las pruebas periódicas son esenciales para garantizar la disponibilidad del CPD y del sitio alternativo.

EPC aplica los siguientes controles:

- Pruebas mensuales de respaldo y restauración en entornos aislados.
- Pruebas semestrales de conmutación hacia el sitio alternativo.
- Simulacros anuales de recuperación completa.
- Mantenimiento preventivo trimestral de servidores, UPS, climatización y red.
- Actualización de firmware y parches de seguridad bajo supervisión de la MDA.
- Documentación técnica completa de cada mantenimiento y resultado de prueba.

Los resultados de las pruebas son evaluados por el Coordinador de TI y documentados en el Informe de Validación de Continuidad Tecnológica, que forma parte de la evidencia de cumplimiento del Sistema Integrado de Gestión (SIG).

Seguridad Física y Lógica del CPD

La seguridad del CPD y del sitio alternativo se gestiona de acuerdo con los principios del Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27002:2022, aplicando controles en tres niveles:

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Seguridad física: control de acceso biométrico, registro de visitantes, monitoreo CCTV y alarmas de intrusión.
- Seguridad eléctrica y ambiental: monitoreo de temperatura, humedad y sistemas de energía con redundancia N+1.
- Seguridad lógica: autenticación multifactor (MFA), cifrado AES-256, control de accesos privilegiados y segmentación de red.

Todos los accesos, físicos o remotos, quedan registrados en bitácoras automáticas de auditoría.

Mecanismos de Respaldo y Replicación de Información

Albergando los servidores, sistemas de almacenamiento, comunicaciones, equipos de seguridad perimetral y servicios esenciales que soportan los procesos misionales, administrativos y de apoyo, el Plan de Recuperación ante Desastres (DRP) establece los lineamientos técnicos para la protección, respaldo y recuperación de este entorno, asegurando la continuidad de los servicios críticos mediante la disponibilidad de infraestructuras redundantes, respaldos externos y un sitio alternativo de contingencia.

CPD Principal

El CPD principal de EPC está ubicado en la sede administrativa central y cumple con los estándares básicos de seguridad física, eléctrica y ambiental para el funcionamiento continuo de los sistemas institucionales, su diseño se fundamenta en una arquitectura híbrida y escalable, que combina infraestructura física local con servicios virtualizados y componentes alojados en nube segura.

Componentes principales del CPD:

- Servidores físicos y virtuales: entorno de virtualización VMware y contenedores Linux para sistemas institucionales.
- Almacenamiento (NAS/SAN): configurado en RAID 5/6 con discos SAS de alta disponibilidad.
- Switches y routers de núcleo: con soporte para VLAN, QoS y priorización de tráfico crítico.
- Firewalls de última generación (NGFW): con filtrado por aplicación, IDS/IPS y VPN segura.
- UPS y planta eléctrica: autonomía de 2 horas con transferencia automática.
- Sistema de climatización redundante: temperatura controlada entre 18 °C y 23 °C.
- Sistema de detección y extinción de incendios: sensores térmicos y sistema de gas inerte.

- Control de acceso biométrico: ingreso restringido a personal autorizado de TI y MDA.

Servicios alojados en el CPD principal:

- ERP Contable y Financiero.
- Sistema SIG Planeación.
- Sistema de Gestión Documental.
- Sistema Comercial y de Atención al Usuario.
- Servidor de Correos Institucional.
- Servidor de Archivos y respaldos automáticos (NAS).
- Plataforma de la Mesa de Ayuda (MDA).

El Coordinador de TI es responsable de la administración general del CPD y de la supervisión de las operaciones de mantenimiento, seguridad y disponibilidad.

Infraestructura Virtual y Servicios en Nube

EPC emplea una infraestructura híbrida que integra servicios locales con plataformas de nube segura para garantizar mayor resiliencia y disponibilidad, estos servicios se utilizan principalmente para respaldo, colaboración institucional y recuperación ante desastres.

Principales servicios en nube:

- Almacenamiento remoto cifrado (off-site): utilizado para copias de seguridad críticas.
- Plataforma de recuperación (DRaaS): provee capacidad de restauración virtual inmediata.
- Correo institucional: gestionado en servidor dedicado con cifrado TLS y autenticación multifactor.
- Aplicaciones de colaboración y productividad: alojadas en entorno seguro controlado por EPC.

El uso de la nube sigue los principios de seguridad de la información, soberanía de datos y continuidad operativa, garantizando que toda la información institucional esté alojada en proveedores con certificaciones ISO/IEC 27001 e ISO 22301.

Sitio Alterno de Recuperación

El sitio alternativo constituye el entorno de respaldo y continuidad tecnológica que permite la restauración de los servicios institucionales en caso de pérdida total o inhabilitación del CPD principal, este sitio puede ser físico o virtual (en la nube), dependiendo del tipo de incidente y la disponibilidad de infraestructura.

Características técnicas del sitio alternativo:

- Ubicación geográfica diferente al CPD principal para mitigar riesgos ambientales o de infraestructura.
- Conectividad segura VPN con el entorno institucional.

- Servidores virtuales preconfigurados con capacidad para asumir servicios críticos.
- Almacenamiento cifrado replicado desde el CPD principal (replicación asíncrona).
- Mecanismo de autenticación controlada y acceso exclusivo para personal autorizado de MDA.
- Respaldo energético autónomo y redundancia de red.
- Capacidad de operación mínima: correo institucional, ERP, sistema documental y portal web.

El sitio alternativo se activa únicamente bajo instrucción del Coordinador de TI, y su uso está sujeto a verificación previa de integridad y sincronización de respaldos.

Mecanismos de Replicación y Sincronización

EPC implementa esquemas de replicación de datos basados en el principio 3-2-1-1-0, que garantiza la disponibilidad y recuperación ante fallos:

- 3 copias de cada dato (producción + dos copias de respaldo).
- 2 medios de almacenamiento diferentes (NAS y nube).
- 1 copia fuera del sitio principal (off-site).
- 1 copia inmutable (no modificable ni cifrable).
- 0 errores detectados tras la verificación de integridad.

La replicación se realiza de forma asíncrona cada 6 horas para datos operativos y sincrónica para bases de datos críticas, asegurando una pérdida máxima tolerable (RPO) de 1 hora.

Los respaldos se validan mediante pruebas automáticas de restauración parcial.

Gestión de Mantenimiento y Pruebas del CPD

El mantenimiento preventivo y las pruebas periódicas son esenciales para garantizar la disponibilidad del CPD y del sitio alternativo.

EPC aplica los siguientes controles:

- Pruebas mensuales de respaldo y restauración en entornos aislados.
- Pruebas semestrales de conmutación hacia el sitio alternativo.
- Simulacros anuales de recuperación completa.
- Mantenimiento preventivo trimestral de servidores, UPS, climatización y red.
- Actualización de firmware y parches de seguridad bajo supervisión de la MDA.
- Documentación técnica completa de cada mantenimiento y resultado de prueba.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Los resultados de las pruebas son evaluados por el Coordinador de TI y documentados en el Informe de Validación de Continuidad Tecnológica, que forma parte de la evidencia de cumplimiento del Sistema Integrado de Gestión (SIG).

Seguridad Física y Lógica del CPD

La seguridad del CPD y del sitio alternativo se gestiona de acuerdo con los principios del Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27002:2022, aplicando controles en tres niveles:

- Seguridad física: control de acceso biométrico, registro de visitantes, monitoreo CCTV y alarmas de intrusión.
- Seguridad eléctrica y ambiental: monitoreo de temperatura, humedad y sistemas de energía con redundancia N+1.
- Seguridad lógica: autenticación multifactor (MFA), cifrado AES-256, control de accesos privilegiados y segmentación de red.

Todos los accesos, físicos o remotos, quedan registrados en bitácoras automáticas de auditoría.

Gestión de Comunicaciones Durante un Desastre

La comunicación efectiva es un pilar fundamental del Plan de Recuperación ante Desastres (DRP), pues permite mantener la coordinación técnica, la trazabilidad de las decisiones y la confianza institucional durante la respuesta a un incidente de alto impacto, el sistema de comunicación establecido por EPC asegura la continuidad de las operaciones informativas internas y externas, aun cuando los medios tradicionales estén comprometidos, garantizando mensajes claros, verificados y alineados con las políticas de seguridad digital.

Objetivo

Establecer los canales, responsabilidades, niveles de comunicación y protocolos de validación que deben activarse durante un desastre, con el fin de asegurar la gestión oportuna y coherente de la información entre la Dirección de Planeación, el Coordinador de TI, la Mesa de Ayuda (MDA), los líderes de proceso y los proveedores estratégicos.

Principios de Comunicación en Situación de Desastre

Toda comunicación institucional durante un evento de desastre debe cumplir los siguientes principios:

- Oportunidad: los mensajes deben emitirse en el menor tiempo posible, priorizando la continuidad operativa.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Veracidad: la información debe provenir únicamente de fuentes verificadas (Coordinador de TI o Dirección de Planeación).
- Confidencialidad: los mensajes deben transmitirse por canales seguros y cifrados.
- Trazabilidad: cada comunicación debe registrarse en la bitácora del DRP.
- Unificación: toda la información técnica y administrativa se canaliza a través de una fuente institucional única para evitar versiones contradictorias.

Estructura de Comunicación Institucional

El flujo de comunicación durante la activación del DRP sigue un modelo jerárquico coordinado que asegura el control de los mensajes y la coherencia en las decisiones adoptadas.

Estructura general:

Nivel de Comunicación	Responsable Emisor	Destinatario / Receptor	Propósito Principal
Nivel 1 – Técnico Operativo	Mesa de Ayuda (MDA)	Coordinador de TI	Reporte de incidentes, avances de recuperación y alertas.
Nivel 2 – Coordinación Institucional	Coordinador de TI	Dirección de Planeación	Comunicación del estado general, decisiones estratégicas y solicitud de apoyo.
Nivel 3 – Comunicación Transversal	Dirección de Planeación	Líderes de Proceso / Áreas de Apoyo	Información validada sobre afectaciones, tiempos estimados y medidas preventivas.
Nivel 4 – Comunicación Externa	Dirección de Planeación (con apoyo del área de Comunicaciones)	Entes de control, ciudadanía y proveedores	Mensajes oficiales sobre estado del servicio y acciones institucionales.

Canales de Comunicación Durante un Desastre

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

EPC cuenta con canales primarios y alternos que garantizan la continuidad de la comunicación institucional incluso ante la pérdida de infraestructura tecnológica o conectividad principal.

Tipo de Canal	Medio Herramienta /	Condición de Uso	Seguridad Asociada
Principal	Servidor de correos institucional	Mientras la infraestructura del CPD esté operativa.	Cifrado TLS, autenticación MFA.
Alternativo 1	VPN segura + acceso remoto MDA	En caso de interrupción parcial del CPD.	Cifrado IPsec / túnel SSL.
Alternativo 2	Dispositivo móvil institucional (voz / datos)	Cuando no exista conectividad LAN/WAN.	Validación biométrica / doble autenticación.
Alternativo 3	Plataforma de mensajería segura temporal (Signal o Threema)	Emergencias críticas o pérdida total de conectividad.	Mensajes cifrados E2E.
Emergencia física	Comunicaciones directas (radio o teléfono fijo externo)	Desastre total o evacuación.	Validación verbal de identidad.

Tipología de Mensajes Institucionales

Durante la ejecución del DRP, los mensajes institucionales se clasifican en tres tipos:

1. Mensajes técnicos de recuperación: dirigidos entre la MDA y el Coordinador de TI; contienen información sobre restauraciones, fallos, pruebas y resultados.
2. Mensajes administrativos: emitidos por el Coordinador de TI a la Dirección de Planeación para informar avances, requerir recursos o solicitar aprobaciones.
3. Mensajes externos oficiales: gestionados por la Dirección de Planeación y el área de Comunicaciones, orientados a entes de control, medios o ciudadanía.

Todos los mensajes deben registrarse con su hora, emisor, receptor, asunto y medio utilizado en la bitácora de eventos del DRP.

Mensaje Inicial de Alerta

El mensaje inicial de alerta es el primer comunicado que se genera una vez verificada la activación del DRP, debe ser corto, técnico y validado por el Coordinador de TI antes de su envío.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Estructura del mensaje inicial:

- Asunto: "Alerta crítica – Activación del DRP – [Nombre del sistema o incidente]"
- Contenido mínimo:
 - Fecha y hora del evento.
 - Descripción breve de la afectación.
 - Sistemas o servicios comprometidos.
 - Nivel de severidad (S3 o S4).
 - Medidas iniciales adoptadas.
 - Tiempo estimado de recuperación (RTO preliminar).
 - Responsable técnico a cargo.

Ejemplo:

"Se informa la activación del DRP a las 08:45 AM debido a falla eléctrica que afecta el CPD principal.

Se encuentran comprometidos los servicios de correo institucional y ERP contable.

Nivel de severidad: S4.

Se inició proceso de conmutación hacia el sitio alternativo.

Tiempo estimado de recuperación: 4 horas.

Responsable técnico: Coordinador de TI."

Comunicación con Proveedores y Entes Externos

Durante un desastre, el Coordinador de TI será el único autorizado para comunicarse directamente con los proveedores tecnológicos, garantizando coherencia, trazabilidad y cumplimiento de cláusulas de confidencialidad.

Las comunicaciones con entes de control o medios externos serán gestionadas exclusivamente por la Dirección de Planeación, siguiendo los lineamientos institucionales de transparencia y manejo de crisis.

Cada interacción externa debe:

- Contar con registro de fecha, hora y contenido del mensaje.
- Ser documentada en el *Informe de Comunicaciones Críticas del DRP*.
- Utilizar únicamente canales verificados o cifrados.

Comunicación de Cierre y Normalización

Una vez restablecidos los servicios, el Coordinador de TI debe emitir el mensaje de cierre del incidente, informando a todos los actores involucrados el retorno a la normalidad operativa.

Estructura del mensaje de cierre:

- Fecha y hora de restablecimiento.
- Sistemas restaurados y pruebas validadas.
- RTO y RPO alcanzados.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Acciones pendientes o programadas.
- Firma digital del Coordinador de TI.

Este mensaje se archiva como evidencia dentro del Informe Final de Recuperación y se notifica al Sistema Integrado de Gestión (SIG).

Bitácora de Comunicaciones del DRP

Toda comunicación institucional realizada durante la activación del DRP deberá ser registrada en la bitácora de comunicaciones, la cual contendrá:

Fecha / Hora Emisor, Receptor, Medio de Comunicación, Descripción del Mensaje / Acción Validación / Firma.

Esta bitácora será consolidada por la Mesa de Ayuda (MDA) y validada por el Coordinador de TI, sirviendo como evidencia de auditoría y seguimiento.

Gestión de Proveedores y Servicios Externos Críticos

Permite asegurar la continuidad operativa de los servicios tercerizados que soportan la infraestructura tecnológica, los sistemas de información y las comunicaciones institucionales de EPC, este apartado establece los mecanismos de coordinación, control y validación que garantizan el cumplimiento de los acuerdos de nivel de servicio (SLA), los acuerdos de continuidad (OLA) y las cláusulas contractuales de recuperación ante desastres (DRA).

Principios de Coordinación con Proveedores

Toda relación con proveedores durante un incidente crítico o desastre se regirá por los siguientes principios:

- Continuidad contractual: los contratos de servicios tecnológicos deben incluir cláusulas de respaldo, recuperación y atención prioritaria ante desastres.
- Disponibilidad garantizada: los proveedores deben mantener capacidades técnicas y humanas suficientes para soportar los tiempos definidos por los RTO/RPO.
- Comunicación segura: toda interacción debe realizarse mediante canales institucionales cifrados y auditables.
- Responsabilidad compartida: la restauración de los servicios tercerizados es una tarea conjunta entre EPC y el proveedor responsable.
- Verificación y trazabilidad: toda acción ejecutada por un proveedor durante la recuperación debe ser documentada y validada por el Coordinador de TI.

Proveedores Tecnológicos Críticos

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Los siguientes proveedores y servicios se consideran críticos para la continuidad tecnológica de EPC, dada su participación directa en la operación de los sistemas institucionales:

Proveedor / Servicio	Tipo de Servicio	Dependencia Interna Responsable	Nivel de Impacto	Cláusula de Continuidad / DRP
Proveedor de Hosting Web y DNS	Alojamiento del portal institucional, DNS y servicios públicos web.	MDA – Infraestructura	Alto	Respallos diarios, recuperación ≤ 6 h.
Proveedor de Telecomunicaciones	Conectividad LAN/WAN, VPN y acceso a Internet institucional.	MDA – Redes y Comunicaciones	Crítico	Redundancia de enlaces y prioridad de reconexión.
Proveedor de Energía Eléctrica	Suministro principal de energía del CPD.	MDA – Infraestructura	Crítico	Prioridad de atención y contingencia con UPS y planta.
Proveedor de DRaaS / Nube Segura	Almacenamiento y recuperación de respaldos off-site.	Coordinador de TI	Crítico	Replicación cada 6 h y restauración ≤ 4 h.
Proveedor de Soporte ERP	Mantenimiento, actualización y recuperación del sistema contable-financiero.	MDA – Aplicaciones	Alto	Restauración funcional ≤ 4 h post incidente.
Proveedor de Sistema Documental	Soporte y restauración del gestor documental institucional.	MDA – Aplicaciones	Medio	Respallos en nube y recuperación ≤ 6 h.
Proveedor de Seguridad	Monitoreo, detección y	MDA – Seguridad TI	Crítico	Activación de incident

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Perimetral (Firewall / Antivirus / SIEM)	mitigación de incidentes cibernéticos.			response y validación post-evento.
---	--	--	--	------------------------------------

Roles y Responsabilidades Durante un Desastre

Actor / Rol	Responsabilidades
Coordinador de TI	Dirige la comunicación con todos los proveedores tecnológicos. Autoriza la activación de planes de contingencia externos. Supervisa la ejecución y cumplimiento de los SLA/DRA.
Mesa de Ayuda (MDA)	Coordina el soporte técnico con los proveedores, documenta los requerimientos, verifica la funcionalidad de los servicios restaurados y registra evidencias.
Dirección de Planeación	Gestiona la comunicación institucional con los proveedores y avala la priorización de recursos o contrataciones de emergencia.
Oficina Jurídica	Verifica la aplicación de las cláusulas contractuales de continuidad, confidencialidad y protección de datos.
Proveedor Tecnológico	Ejecuta las acciones técnicas de restauración, garantiza el cumplimiento de los tiempos acordados y reporta las evidencias de recuperación.

Mecanismos de Comunicación y Coordinación

Durante un evento de desastre, se activarán los siguientes mecanismos de comunicación con los proveedores:

- Canal principal: correo institucional cifrado (TLS 1.3).
- Canal alterno: VPN institucional o plataforma de videoconferencia autorizada.
- Canal de emergencia: comunicación telefónica validada por autenticación verbal.

Toda comunicación debe ser registrada en la bitácora del DRP, incluyendo fecha, hora, medio, responsable y resultado, los proveedores no podrán ejecutar ninguna acción crítica sin la validación del Coordinador de TI.

Validación de Cumplimiento de SLA y DRA

Los acuerdos de nivel de servicio (SLA) y los acuerdos de recuperación ante desastres (DRA) son auditados semestralmente.

Durante la activación del DRP, la MDA debe:

- Verificar que el proveedor cumpla los tiempos de respuesta establecidos (RTO/RPO).

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Confirmar la integridad de los datos recuperados y su sincronización.
- Documentar desviaciones, fallas o incumplimientos.
- Reportar los resultados al Coordinador de TI para seguimiento contractual.

Revisión y Evaluación de Proveedores

EPC mantiene un registro actualizado de proveedores críticos dentro de su Sistema Integrado de Gestión (SIG Planeación), el cual se revisa de forma anual o tras cada evento relevante.

Los criterios de evaluación incluyen:

- Cumplimiento de SLA y DRA.
- Capacidad técnica y tiempos de respuesta.
- Adherencia a las políticas de seguridad de la información.
- Resultados de auditorías y simulacros.
- Riesgo de dependencia tecnológica.

Contratación y Confidencialidad

Todos los contratos con proveedores críticos deben incluir:

- Cláusulas de confidencialidad y protección de datos personales.
- Compromisos explícitos de continuidad operativa y recuperación ante desastres.
- Mecanismos de notificación de incidentes de seguridad.
- Obligación de reportar brechas o fallos que afecten los servicios de EPC.
- Plan de comunicación y contingencia validado por el Coordinador de TI.

Evaluación Post-Evento

Tras la finalización del incidente y el retorno a la normalidad, se realiza una evaluación post-evento conjunta con los proveedores implicados, en la que se revisan:

- Resultados del proceso de recuperación.
- Cumplimiento de tiempos y niveles de servicio.
- Lecciones aprendidas.
- Ajustes contractuales o técnicos requeridos.

El Coordinador de TI consolida esta información en el Informe de Evaluación de Desempeño de Proveedores Post-Desastre, el cual se archiva en el SIG Planeación.

Plan de Coordinación Operativa y Logística

La gestión de un desastre requiere sincronización entre múltiples actores institucionales, recursos técnicos y procedimientos, el Plan de Coordinación

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Operativa y Logística establece una estructura funcional que permite ejecutar las tareas del DRP conforme a prioridades, roles y dependencias definidas, minimizando el tiempo de recuperación y evitando conflictos operativos.

Este plan articula tres niveles de coordinación:

1. Nivel Técnico-Operativo (MDA): ejecución directa de actividades de restauración, soporte y monitoreo.
2. Nivel de Gestión Institucional (Coordinador de TI): liderazgo operativo, toma de decisiones y asignación de recursos.
3. Nivel de Supervisión Estratégica (Dirección de Planeación): validación institucional, comunicación externa y registro documental en el SIG Planeación.

Activación del Plan Logístico

La activación del componente logístico se ejecuta de forma simultánea a la activación del DRP, bajo la dirección del Coordinador de TI, quien:

- Define los equipos técnicos que intervendrán según la naturaleza del evento.
- Gestiona los recursos físicos y tecnológicos requeridos (equipos, respaldos, licencias, energía, conectividad).
- Asigna los espacios alternos de operación o teletrabajo en caso de inhabilitación del CPD.
- Activa los protocolos de transporte, acceso y seguridad física del personal técnico.
- Mantiene comunicación continua con la Dirección de Planeación y la Oficina Jurídica para autorizar el uso de recursos adicionales o contratación de emergencia.

Recursos Humanos y Técnicos

Durante la ejecución del DRP, la Mesa de Ayuda (MDA) se divide funcionalmente en grupos especializados:

Equipo / Grupo		Responsabilidad Técnica Principal	Dependencia
Infraestructura y Energía	y	Restaurar servidores, UPS, NAS y climatización del CPD o sitio alternativo.	MDA
Redes y Comunicaciones	y	Restablecer enlaces WAN/LAN, VPN y servicios de acceso remoto.	MDA
Aplicaciones y Bases de Datos	y	Recuperar ERP, SIG Planeación, SIA, Sistema Documental y otros servicios críticos.	MDA
Seguridad de la Información	la	Verificar integridad de los datos, monitorear incidentes y validar controles post-recuperación.	MDA

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Soporte Funcional	Brindar apoyo técnico a los líderes de proceso durante el restablecimiento de servicios.	MDA
--------------------------	--	-----

Cada grupo designará un responsable técnico, quien reportará el estado de sus tareas al Coordinador de TI cada dos horas o según la criticidad del evento.

Recursos Logísticos y Físicos

La Dirección de Planeación, a solicitud del Coordinador de TI, podrá autorizar el uso o adquisición inmediata de:

- Equipos de cómputo o servidores de reemplazo.
- Dispositivos de almacenamiento externo certificados.
- Servicios de transporte o acceso a instalaciones remotas.
- Herramientas de diagnóstico, licencias temporales o software de respaldo.
- Recursos para hospedaje o alimentación del personal técnico si la jornada supera las 12 horas.

La gestión de estos recursos se documenta en el *Formato de Registro Logístico DRP-F01*, con trazabilidad en el SIG Planeación.

Coordinación Interinstitucional

En caso de un evento de gran magnitud, el Coordinador de TI podrá solicitar apoyo a otras entidades del orden departamental o nacional, bajo los protocolos establecidos en la Política de Gobierno Digital y el MSPI, especialmente en:

- Intercambio de información técnica de incidentes cibernéticos.
- Asistencia en recuperación de infraestructura o sistemas críticos.
- Soporte en gestión de comunicaciones oficiales y manejo de crisis.

La coordinación interinstitucional será gestionada directamente por la Dirección de Planeación, quien consolidará la información para los entes de control.

Seguimiento y Control Operativo

Durante la ejecución del DRP, se implementarán los siguientes mecanismos de control:

- Reuniones de seguimiento técnico cada 4 horas durante la fase de recuperación.
- Bitácoras automáticas de actividades en el sistema de gestión de incidentes (MDA).
- Reportes de estado (estatus, sistemas, tiempos, riesgos y acciones correctivas).
- Registro de desviaciones respecto a los RTO/RPO establecidos.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

El Coordinador de TI será responsable de consolidar la información en el *Informe de Coordinación Operativa DRP-F02*, documento que servirá de insumo para la validación final y auditoría post-evento.

Finalización del Plan de Coordinación

Una vez culminada la fase de recuperación y verificada la normalización de los servicios, el Coordinador de TI:

- Informa a la Dirección de Planeación la finalización de la coordinación operativa.
- Emite el Acta de Cierre Logístico y Operativo DRP-F03.
- Dispone la documentación técnica y evidencias en el repositorio institucional del SIG Planeación.

Validación Técnica Post-Recuperación

La fase de validación técnica post-recuperación tiene como propósito confirmar la operatividad funcional, la integridad de los datos y la estabilidad del entorno tecnológico antes del retorno completo a la operación normal, este proceso se desarrolla bajo la supervisión del Coordinador de TI, con apoyo de la Mesa de Ayuda (MDA) y la participación de los líderes de proceso que dependen de los servicios recuperados, la validación técnica se realiza mediante pruebas controladas, revisión de logs, auditoría de seguridad, monitoreo de desempeño y verificación documental, de acuerdo con las políticas definidas en el Sistema Integrado de Gestión (SIG).

Alcance

Este proceso aplica a todos los sistemas, plataformas, redes, bases de datos y servicios institucionales que hayan sido objeto de restauración parcial o total, incluyendo:

- ERP contable y financiero.
- Sistema SIG Planeación.
- Sistema de Gestión Documental.
- Sistema Comercial y Atención al Usuario.
- Servidor de correos institucional.
- Infraestructura de red, almacenamiento (NAS/SAN) y respaldos.

Fases del Proceso de Validación Técnica

La validación técnica comprende cinco fases secuenciales:

- Verificación de Integridad de Datos
 - Comprobación de hashes, checksums o firmas digitales.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Comparación entre respaldos previos y datos operativos restaurados.
- Validación de consistencia de registros en bases de datos.
- Confirmación de integridad de archivos de configuración y logs.
- b. Pruebas Funcionales
 - Validación de autenticación, roles y permisos de usuario.
 - Ejecución de operaciones estándar en aplicaciones críticas (consultas, reportes, transacciones).
 - Pruebas de comunicación entre sistemas interdependientes (API, ERP-SIA, ERP-SIG).
 - Confirmación de acceso y rendimiento en red.
- c. Pruebas de Desempeño y Disponibilidad
 - Monitoreo de CPU, memoria y latencia de red.
 - Pruebas de carga controlada para verificar la estabilidad del sistema.
 - Validación de tiempos de respuesta frente a umbrales operativos definidos.
- d. Validación de Seguridad
 - Verificación de configuraciones de firewall, antivirus y SIEM.
 - Prueba de autenticación multifactor (MFA) y políticas de contraseñas.
 - Escaneo de vulnerabilidades y revisión de parches pendientes.
 - Revisión de logs de acceso y detección de intentos no autorizados.
- e. Confirmación Funcional por Líderes de Proceso
 - Los líderes de proceso validan la funcionalidad de sus sistemas.
 - Se firma el *Acta de Conformidad de Validación Post-Recuperación (DRP-F04)*.
 - Cualquier hallazgo o desviación se documenta para tratamiento correctivo.

Roles y Responsabilidades

Rol / Cargo	Responsabilidades Específicas
Coordinador de TI	Supervisar todo el proceso de validación técnica. Autorizar el retorno a la operación normal una vez verificada la integridad total de los servicios.
Mesa de Ayuda (MDA)	Ejecutar las pruebas técnicas, registrar resultados y documentar evidencias. Coordinar con los líderes de proceso y emitir reportes de validación.
Líderes de Proceso	Verificar la funcionalidad de los sistemas de su área y reportar cualquier anomalía. Firmar el acta de conformidad o no conformidad.
Dirección de Planeación	Recibir los resultados de validación y registrar los documentos en el SIG Planeación para trazabilidad y auditoría.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Documentación y Evidencias

Todos los resultados del proceso de validación deben registrarse en el *Formato de Registro de Pruebas Post-Recuperación (DRP-F05)*, que incluirá:

- Fecha y hora de inicio y finalización de la validación.
- Servicios y sistemas evaluados.
- Descripción de las pruebas ejecutadas.
- Resultados y observaciones.
- Indicadores de cumplimiento RTO/RPO alcanzados.
- Conclusión técnica del Coordinador de TI.
- Firmas electrónicas o digitales de los participantes.

Las evidencias (capturas, reportes, logs, comparativos de hash, etc.) se almacenarán en el repositorio técnico del SIG Planeación, bajo las políticas de retención definidas en el MSPI.

Criterios de Aprobación

Se considerará validada la recuperación de un sistema cuando:

- Las pruebas funcionales y de seguridad se ejecuten sin fallas críticas.
- Los datos recuperados coincidan con la última versión íntegra del respaldo.
- Los tiempos reales de restauración estén dentro de los límites de RTO y RPO definidos.
- Los líderes de proceso confirmen la normalización operativa.

Si alguno de estos criterios no se cumple, el sistema permanecerá en estado de contingencia controlada hasta su corrección.

Informe de Validación Post-Recuperación

Una vez completado el proceso, el Coordinador de TI emitirá el Informe de Validación Técnica Post-Recuperación (DRP-F06), que incluirá:

- Descripción del evento y sistemas recuperados.
- Resultados técnicos y métricas alcanzadas.
- Riesgos o desviaciones detectadas.
- Acciones correctivas implementadas o pendientes.
- Conclusión y autorización de retorno operativo.

Este informe será presentado a la Dirección de Planeación y archivado como evidencia de cumplimiento dentro del Sistema Integrado de Gestión (SIG) y del SGSPi.

Procedimientos de Cierre y Retorno a la Normalidad

El cierre del DRP constituye la última etapa del proceso de recuperación y debe realizarse únicamente cuando:

- Todos los sistemas y servicios críticos han sido restaurados y verificados.
- Las validaciones técnicas y funcionales han sido aprobadas.
- Se ha restablecido la comunicación y conectividad con todos los usuarios.
- Se han documentado las acciones ejecutadas y resultados alcanzados.

El Coordinador de TI es la única autoridad autorizada para declarar formalmente el cierre de la fase de recuperación y el retorno a la operación normal, previa validación de la Dirección de Planeación.

Fases del Cierre y Retorno a la Normalidad

El proceso de cierre se estructura en cuatro fases secuenciales:

a. Confirmación Técnica Final

- Validar que todos los servicios tecnológicos se encuentren operativos, disponibles y accesibles.
- Verificar la sincronización entre respaldos, bases de datos y aplicaciones.
- Confirmar la estabilidad del rendimiento (memoria, CPU, red y almacenamiento).
- Validar que los controles de seguridad estén activos (firewall, antivirus, MFA, SIEM).

b. Comunicación de Restablecimiento

- El Coordinador de TI comunica oficialmente el restablecimiento completo de los servicios a la Dirección de Planeación, líderes de proceso y usuarios internos.
- El mensaje incluye la fecha y hora de normalización, los sistemas afectados, los tiempos reales de recuperación (RTO/RPO alcanzados) y las observaciones relevantes.
- La Dirección de Planeación autoriza la emisión del comunicado institucional a los entes de control o ciudadanía, si aplica.

c. Desactivación del Sitio Alterno

- Si el DRP fue ejecutado desde un entorno alternativo (físico o nube), se realiza la sincronización final de datos y la verificación de integridad.
- Se restablece la operación principal en el CPD de EPC.
- Se desactivan los recursos temporales, accesos remotos o licencias de emergencia.
- Se documenta la transición mediante el *Formato DRP-F07 – Acta de Retorno Operativo*.

d. Evaluación Inicial Post-Restauración

- Durante las primeras 48 horas posteriores al restablecimiento, la MDA realiza un monitoreo continuo de rendimiento, accesos y logs.
- Se registran incidencias menores o ajustes pendientes.
- Se confirma que las condiciones del entorno son estables y seguras.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Una vez validado, el Coordinador de TI cierra la bitácora del evento y emite el informe final.

Roles y Responsabilidades

Rol / Cargo	Responsabilidad Principal
Coordinador de TI	Declarar el cierre del DRP, consolidar la documentación técnica y emitir el informe final de restablecimiento.
Mesa de Ayuda (MDA)	Verificar la estabilidad de los servicios, monitorear los sistemas y registrar las evidencias de cierre.
Líderes de Proceso	Confirmar la disponibilidad total de los servicios asociados a su área y reportar cualquier anomalía.
Dirección de Planeación	Validar institucionalmente la finalización del DRP y autorizar el cierre en el SIG Planeación .
Oficina Jurídica / Control Interno	Revisar el cumplimiento normativo, contractual y documental asociado al proceso de cierre.

Documentación y Evidencias del Cierre

El proceso de cierre debe estar soportado con la siguiente documentación:

- *Acta de Cierre del DRP (DRP-F08)* firmada por el Coordinador de TI y la Dirección de Planeación.
- *Informe Final de Recuperación y Restablecimiento (DRP-F09)*, que incluye:
 - Descripción del evento y causas.
 - Sistemas afectados y tiempos de recuperación reales.
 - Controles técnicos implementados.
 - Resultados de validación funcional.
 - Desviaciones y acciones correctivas aplicadas.
- *Bitácora completa del DRP*, con registro cronológico de todas las acciones y comunicaciones.
- Evidencias técnicas (logs, reportes, capturas, respaldos verificados).

Toda la información debe ser archivada en el Sistema Integrado de Gestión (SIG Planeación) y vinculada a los módulos de seguridad y continuidad del SGSPI.

Informe Final del Evento

El Informe Final del Evento de Desastre Tecnológico, consolidado por el Coordinador de TI, es el documento oficial que refleja la gestión integral del DRP. Este informe deberá presentarse dentro de los cinco (5) días hábiles siguientes al cierre del plan y contendrá:

- Resumen del evento y causas raíz.
- Impacto operativo, económico y reputacional.
- Cronología de acciones y decisiones adoptadas.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Cumplimiento de RTO y RPO.
- Resultados de validación técnica y funcional.
- Participación de proveedores externos.
- Recomendaciones y oportunidades de mejora.

El informe se remite a la Dirección de Planeación, Oficina de Control Interno, y al Comité de Gestión Institucional para su análisis y seguimiento.

Actualización de Configuraciones y Copias Maestras

Una vez verificada la normalidad operativa:

- Se actualizan las configuraciones de respaldo, parámetros de red y listas de control de acceso.
- Se genera una copia maestra de respaldo post-evento, que servirá como base de restauración en el futuro.
- Se revisan y actualizan los planes de respaldo, recuperación y continuidad conforme a los hallazgos detectados.

Criterios para el Retorno Formal a la Normalidad

Se considerará completado el proceso de retorno a la normalidad cuando:

- Todos los servicios críticos estén disponibles y en producción.
- No existan alertas ni anomalías activas en el monitoreo.
- Los usuarios confirmen la funcionalidad normal de sus sistemas.
- Los líderes de proceso y el Coordinador de TI aprueben el cierre.
- La Dirección de Planeación valide el restablecimiento y autorice el cierre administrativo en el SIG Planeación.

Comunicación de Cierre Institucional

La Dirección de Planeación, con apoyo del área de Comunicaciones, emitirá el comunicado oficial de cierre, informando que los servicios tecnológicos se encuentran restablecidos y operando con normalidad, destacando:

- Fecha y hora de restablecimiento total.
- Principales acciones ejecutadas.
- Resultados de recuperación y validación.
- Compromiso de mejora continua y fortalecimiento del SGSI y DRP.

Documentación, Evidencias y Reportes Post-Evento

La documentación y conservación de las evidencias constituyen la base de la trazabilidad del DRP, cada actividad ejecutada, decisión tomada y resultado obtenido durante un evento de recuperación debe registrarse formalmente, con soporte técnico y validación institucional, estos registros permiten verificar el cumplimiento

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

de los RTO y RPO, la eficacia de los controles aplicados y la coherencia con los lineamientos del SGSPI y el Sistema Integrado de Gestión (SIG Planeación).

La información recopilada cumple una doble función:

1. Servir como evidencia para auditorías internas y externas.
2. Alimentar los procesos de análisis post-incidente, retroalimentación y mejora continua del plan.

Tipos de Documentación del DRP

Toda la información del Plan de Recuperación ante Desastres se clasifica en tres categorías:

Tipo de Documento	Descripción	Responsable de Custodia
Documentos Operativos	Registros generados durante la activación y ejecución del DRP: bitácoras, informes técnicos, comunicaciones, validaciones.	Mesa de Ayuda (MDA)
Documentos Estratégicos	Informes de impacto, reportes ejecutivos, actas de cierre y evaluación post-evento.	Coordinador de TI / Dirección de Planeación
Documentos Normativos y Contractuales	Acuerdos de nivel de servicio (SLA), contratos, políticas, procedimientos y controles asociados.	Dirección de Planeación / Oficina Jurídica

Registros y Evidencias del Proceso

Los principales registros y evidencias que deben generarse y conservarse durante el proceso de recuperación son:

1. Bitácora de Activación del DRP: hora, responsable, motivo de activación, sistemas afectados y acciones iniciales.
2. Registro de Comunicaciones Técnicas y Administrativas: mensajes internos y externos, decisiones tomadas y tiempos de respuesta.
3. Informes de Restauración Técnica: descripción de los sistemas recuperados, controles aplicados, tiempos reales de recuperación y responsables.
4. Registros de Validación Técnica y Funcional: evidencias de pruebas, resultados de verificación y aprobación de los líderes de proceso.
5. Actas de Cierre y Retorno a la Normalidad: confirmación institucional del restablecimiento total de los servicios.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

6. Informe Final del Evento: consolidado general del incidente, impacto y acciones de mejora.
7. Reportes Post-Evento: análisis de desempeño, cumplimiento de indicadores, lecciones aprendidas y actualizaciones requeridas al plan.

Formatos Estándar de Registro

Para asegurar la uniformidad de la información, todos los registros se deben diligenciar en los formatos oficiales del DRP, codificados y controlados dentro del Sistema Integrado de Gestión (SIG Planeación):

Código	Formato / Registro	Descripción
DRP-F01	Registro Logístico y de Recursos	Documenta los recursos utilizados y su trazabilidad.
DRP-F02	Informe de Coordinación Operativa	Consolida las acciones técnicas y logísticas ejecutadas.
DRP-F03	Acta de Cierre Logístico y Operativo	Registra la finalización del proceso técnico.
DRP-F04	Acta de Validación Post-Recuperación	Evidencia la aprobación funcional y técnica.
DRP-F05	Registro de Pruebas de Restauración	Documenta las pruebas y resultados.
DRP-F06	Informe de Validación Técnica Final	Contiene la evaluación técnica de los sistemas recuperados.
DRP-F07	Acta de Retorno Operativo	Formaliza el restablecimiento del entorno de producción.
DRP-F08	Acta de Cierre del DRP	Cierre institucional con validación de la Dirección de Planeación.
DRP-F09	Informe Final del Evento	Consolidado ejecutivo del proceso completo de recuperación.

Todos los formatos deben contener campos para fecha, responsable, firma digital, observaciones y evidencias anexas.

Custodia y Almacenamiento de Evidencias

- Los documentos en formato digital serán almacenados en el repositorio institucional del SIG Planeación, bajo control de versiones y permisos restringidos.
- Las evidencias físicas (actas, reportes impresos, discos o dispositivos de respaldo) se custodiarán en el archivo técnico de la Dirección de Planeación Área de TI.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- La información clasificada como reservada o sensible deberá conservarse conforme a los lineamientos de la Ley 1712 de 2014 y la Ley 1581 de 2012 sobre acceso y protección de datos personales.
- Se mantendrá una copia de seguridad inmutable de toda la documentación crítica por un periodo mínimo de 5 años.

Indicadores de Desempeño y Seguimiento Post-Evento

Para evaluar la eficacia del DRP y las acciones de recuperación, se aplicarán los siguientes indicadores:

Indicador	Fórmula / Método de Cálculo	Meta	Frecuencia de Seguimiento
Cumplimiento del RTO (%)	$(\text{RTO Alcanzado} / \text{RTO Planificado}) \times 100$	$\geq 90\%$	Post-evento
Cumplimiento del RPO (%)	$(\text{RPO Alcanzado} / \text{RPO Planificado}) \times 100$	$\geq 95\%$	Post-evento
Disponibilidad post-recuperación (%)	$(\text{Horas de disponibilidad} / \text{Horas totales del periodo}) \times 100$	$\geq 98\%$	Mensual
Porcentaje de registros documentados	$(\text{Registros completos} / \text{Registros requeridos}) \times 100$	100%	Post-evento
Cumplimiento de acciones de mejora	$(\text{Acciones implementadas} / \text{Acciones identificadas}) \times 100$	$\geq 85\%$	Trimestral

Estos indicadores serán gestionados en el módulo de Continuidad y Seguridad de la Información del SIG Planeación, y revisados en las reuniones técnicas semestrales del área de TI.

Auditoría y Control Documental

La documentación generada por el DRP será objeto de revisión y auditoría por parte de:

- Oficina de Control Interno: verificación de cumplimiento normativo y documental.
- Dirección de Planeación: control de coherencia técnica y validación de trazabilidad.
- Coordinador de TI: revisión de evidencias técnicas y cumplimiento de los estándares ISO aplicables.

Toda observación o hallazgo deberá generar un plan de acción correctivo, que será monitoreado en el SIG Planeación.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Conservación y Eliminación de Documentos

La eliminación de documentos o evidencias del DRP solo podrá realizarse tras cumplir el periodo de retención establecido y con la aprobación de la Dirección de Planeación, documentando la acción en el *Acta de Eliminación de Evidencias DRP-F10*.

El procedimiento seguirá las normas de gestión documental institucional y los lineamientos de la ISO 15489-1:2016 sobre administración de documentos.

Integración con el Sistema Integrado de Gestión (SIG)

Todos los registros, informes y evidencias del DRP se integran dentro del SIG Planeación, en los módulos de:

- Gestión de Seguridad de la Información (SGSPI).
- Gestión de Continuidad y Riesgo Operativo.
- Gestión Documental y Transparencia Activa.

Esta integración permite la trazabilidad completa del ciclo del DRP, desde la activación hasta la mejora continua, y garantiza el cumplimiento con el Decreto 338 de 2022 sobre políticas de seguridad digital del Estado colombiano.

Programa de Pruebas (Testing y Simulacros Técnicos)

El programa de pruebas y simulacros es un componente obligatorio del DRP y forma parte del proceso de mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), su aplicación permite identificar debilidades técnicas, validar los procedimientos documentados, medir la capacidad de coordinación y asegurar que los mecanismos de respaldo y recuperación funcionen correctamente, las pruebas se realizarán bajo condiciones controladas y documentadas, evitando afectar los servicios productivos, y sus resultados serán registrados en los formatos oficiales y reportados a la Dirección de Planeación.

Tipos de Pruebas

El programa contempla cinco tipos de pruebas, que se aplicarán según el alcance, complejidad y madurez del sistema de recuperación:

Tipo de Prueba	Descripción	Objetivo Principal	Frecuencia Recomendada
Prueba de Revisión de Documentación	Evaluación de la estructura, procedimientos y roles del DRP.	Verificar que el contenido esté actualizado y sea coherente con la infraestructura actual.	Semestral

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Prueba de Comunicación	Validación de los canales internos y externos definidos en el DRP.	Confirmar la operatividad de los mecanismos de notificación, alertas y coordinación.	Trimestral
Prueba de Restauración Parcial	Restauración de servicios o sistemas no críticos desde respaldos reales.	Validar la integridad de respaldos y tiempos de restauración en entornos controlados.	Trimestral
Prueba de Conmutación (Failover DRaaS)	Simulación de pérdida del CPD y activación del sitio alterno.	Comprobar la capacidad de recuperación completa y la operatividad del sitio de contingencia.	Anual
Simulacro Integral de Desastre	Ejercicio completo que incluye activación, comunicación, restauración, validación y cierre.	Evaluar integralmente la eficacia del plan, los tiempos de respuesta y la coordinación institucional.	Cada 2 años o tras un incidente mayor

Planificación de las Pruebas

Todas las pruebas deben planificarse con anticipación, bajo la coordinación del Coordinador de TI y la Mesa de Ayuda (MDA).

El plan anual de pruebas deberá incluir:

- Objetivo de la prueba.
- Alcance y sistemas involucrados.
- Tipo de prueba a realizar.
- Fechas y duración estimada.
- Recursos técnicos y humanos requeridos.
- Riesgos y medidas de mitigación.
- Formato de registro y documentación de resultados.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

El cronograma de pruebas será aprobado por la Dirección de Planeación y registrado en el SIG Planeación, dentro del módulo de continuidad y seguridad.

Ejecución de Pruebas

Durante la ejecución de las pruebas se deben cumplir las siguientes condiciones:

- Las pruebas no deben comprometer la operación de los servicios críticos de producción.
- Cada actividad debe estar documentada paso a paso, con responsable asignado y hora de ejecución.
- Los equipos participantes deben contar con roles y permisos previamente definidos.
- Toda acción o cambio temporal debe ser reversible y supervisado por el Coordinador de TI.
- Los resultados deben registrarse en el *Formato DRP-F11 – Registro de Pruebas de Continuidad*.

Evaluación y Resultados

Una vez concluida la prueba o simulacro, el Coordinador de TI consolidará los resultados mediante el *Informe de Prueba y Simulacro (DRP-F12)*, el cual incluirá:

- Objetivos planteados y resultados obtenidos.
- Tiempos de ejecución reales frente a RTO/RPO planificados.
- Incidentes o fallas detectadas durante el ejercicio.
- Eficacia de la comunicación y coordinación operativa.
- Recomendaciones técnicas y de gestión.
- Plan de acción para la corrección de hallazgos.

El informe será presentado a la Dirección de Planeación y almacenado en el SIG Planeación, con seguimiento de las acciones correctivas hasta su cierre.

Indicadores de Efectividad de las Pruebas

Indicador	Fórmula / Método de Cálculo	Meta	Frecuencia de Medición
Cumplimiento del Cronograma de Pruebas (%)	$(\text{Pruebas realizadas} / \text{Pruebas programadas}) \times 100$	100 %	Anual
Eficacia de Recuperación (%)	$(\text{RTO alcanzado} / \text{RTO planificado}) \times 100$	≥ 90 %	Post-prueba
Disponibilidad del Sitio Alterno (%)	$(\text{Pruebas exitosas} / \text{Total de pruebas de conmutación}) \times 100$	≥ 95 %	Anual

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

Cumplimiento de Acciones Correctivas (%)	(Acciones cerradas / Acciones generadas) × 100	$\geq 85\%$	Trimestral
---	--	-------------	------------

Estos indicadores permiten medir el desempeño general del DRP y sirven como evidencia de la madurez del sistema de continuidad tecnológica.

Responsables del Programa de Pruebas

Rol / Cargo	Responsabilidades
Coordinador de TI	Planificar, dirigir y aprobar todas las pruebas del DRP. Validar los resultados y garantizar la implementación de acciones correctivas.
Mesa de Ayuda (MDA)	Ejecutar las pruebas técnicas, documentar resultados y mantener evidencias.
Dirección de Planeación	Supervisar la ejecución del programa, revisar informes y validar su inclusión en el SIG Planeación.
Líderes de Proceso	Participar en pruebas que involucren sistemas de su área, reportar fallas y validar la funcionalidad posterior.
Proveedores Críticos	Apoyar técnicamente las pruebas de respaldo, recuperación o conmutación bajo las cláusulas contractuales del DRP.

Revisión de Resultados y Mejora Continua

Posterior a cada prueba o simulacro, se llevará a cabo una reunión técnica de revisión con todos los participantes para:

- Analizar los resultados obtenidos.
- Identificar brechas, fallas o tiempos de respuesta no conformes.
- Evaluar la eficacia de los procedimientos y roles asignados.
- Actualizar la documentación del DRP y del BIA según los hallazgos.
- Programar las mejoras técnicas o de capacitación requeridas.

Toda acción derivada será registrada en el Plan de Mejoramiento del DRP, con su responsable, fecha de implementación y seguimiento en el SIG Planeación.

Capacitación y Competencias del Personal Técnico

El éxito del DRP depende en gran medida del nivel de conocimiento y preparación del equipo encargado de su ejecución, el proceso de capacitación busca mantener un personal técnico actualizado, con habilidades en gestión de incidentes, ciberseguridad, respaldo y recuperación de sistemas, redes, comunicaciones, virtualización y continuidad tecnológica.

El Coordinador de TI, en conjunto con la Mesa de Ayuda (MDA) y la Dirección de Planeación, establecerá un Programa Anual de Capacitación y Entrenamiento,

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

basado en necesidades detectadas, resultados de simulacros, auditorías y nuevas tecnologías adoptadas por EPC.

Competencias Requeridas del Personal Técnico

El personal involucrado en el DRP debe cumplir con un perfil técnico y actitudinal acorde con las funciones asignadas.

A continuación, se presentan las competencias esenciales según el rol:

Rol / Cargo	Competencias Técnicas y de Gestión
Coordinador de TI	- Conocimiento avanzado en continuidad de servicios tecnológicos y gestión de riesgos. - Certificaciones o formación en ISO 22301, ISO/IEC 27001 o ISO/IEC 27031. - Capacidad de liderazgo, coordinación y toma de decisiones en escenarios de crisis.
Mesa de Ayuda (MDA)	- Conocimientos en administración de servidores, redes, virtualización y respaldo de información. - Manejo de herramientas de monitoreo, diagnóstico y soporte técnico. - Capacidad de respuesta ante incidentes, documentación de acciones y comunicación efectiva.
Líderes de Proceso	- Comprensión de los procedimientos de continuidad aplicables a su área. - Identificación de activos críticos y dependencias tecnológicas. - Participación en simulacros y validación funcional post-recuperación.
Dirección de Planeación	- Gestión de políticas institucionales, control documental y evaluación de riesgos. - Supervisión del cumplimiento de los objetivos de recuperación y mejora continua.
Proveedores Estratégicos	- Conocimiento técnico del entorno tecnológico bajo contrato. - Cumplimiento de SLA, OLA y DRA relacionados con continuidad y recuperación.

24.3 Programa de Capacitación Anual

El programa de formación técnica se planificará anualmente y deberá incluir:

1. Inducción institucional al DRP: dirigida a todo el personal nuevo o reasignado.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

2. Capacitación técnica avanzada: enfocada en recuperación de sistemas, copias de seguridad, virtualización, y gestión de incidentes.
3. Simulacros prácticos y talleres de respuesta ante desastres: ejercicios operativos con escenarios reales o simulados.
4. Entrenamiento en ciberseguridad y buenas prácticas de seguridad digital: centrado en prevención de incidentes, manejo de accesos y protección de información.
5. Capacitaciones cruzadas (cross-training): para que los funcionarios puedan reemplazarse temporalmente entre sí durante una contingencia.
6. Actualización normativa y de políticas institucionales: sobre el MSPI, Decreto 338 de 2022 y otras disposiciones vigentes.

Mecanismos de Ejecución y Registro

- Todas las capacitaciones deberán registrarse en el SIG Planeación mediante el formato *DRP-F14 – Registro de Capacitación y Competencias*.
- Cada sesión incluirá: fecha, tema, modalidad, responsable, lista de asistencia y evaluación final.
- Las actividades podrán ser presenciales o virtuales, según la naturaleza del tema y los recursos disponibles.
- El Coordinador de TI deberá mantener actualizado el Listado de Competencias Técnicas Certificadas, con los funcionarios que hayan recibido formación específica en continuidad o recuperación.

Evaluación del Nivel de Competencia

Para garantizar la efectividad de las capacitaciones, se aplicarán evaluaciones periódicas al personal técnico, con indicadores como:

Indicador	Fórmula / Método de Evaluación	Meta Mínima
Cumplimiento del Plan de Capacitación Anual (%)	$\frac{\text{Capacitaciones ejecutadas}}{\text{Capacitaciones programadas}} \times 100$	100 %
Nivel de competencia del personal técnico (%)	$\frac{\text{Funcionarios certificados}}{\text{Total de funcionarios del área}} \times 100$	≥ 85 %
Participación en simulacros (%)	$\frac{\text{Participantes reales}}{\text{Participantes convocados}} \times 100$	≥ 90 %
Satisfacción del personal capacitado (%)	Promedio de calificaciones de encuestas post-capacitación	≥ 90 %

Mantenimiento de Competencias y Mejora Continua

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- El personal técnico deberá actualizar sus conocimientos al menos una vez al año en temas de continuidad, ciberseguridad y nuevas tecnologías.
- Cada simulacro o evento real deberá generar una sesión de retroalimentación para identificar lecciones aprendidas y necesidades de capacitación adicionales.
- Los resultados de las evaluaciones de competencia serán revisados en conjunto por el Coordinador de TI y la Dirección de Planeación, como parte del ciclo de mejora continua del DRP.
- Las brechas detectadas en conocimientos o habilidades deberán incluirse en el Plan de Mejoramiento del DRP (DRP-F13).

Certificación de Competencias

La Dirección de Planeación, en coordinación con el Coordinador de TI, emitirá certificaciones internas o de participación en las actividades de capacitación, las cuales deberán conservarse en el expediente de cada funcionario y asociarse al módulo de talento humano del SIG Planeación, para roles críticos (Coordinador de TI, Administrador de Sistemas, Analista de Seguridad), se fomentará la obtención de certificaciones externas reconocidas como:

- ISO/IEC 27001 Lead Implementer o Lead Auditor
- Certified Information Systems Security Professional (CISSP)
- ITIL Foundation / Intermediate
- CompTIA Security+ o Network+
- Continuity and Resilience Professional (CBCP, ISO 22301)

Gestión de Cambios y Control de Versiones

La Gestión de Cambios y Control de Versiones es un proceso continuo que garantiza que el DRP permanezca actualizado, refleje la infraestructura tecnológica real, los riesgos actuales y las capacidades institucionales disponibles, cada actualización del plan debe responder a una necesidad justificada, derivada de:

- Cambios en la infraestructura tecnológica o arquitecturas de red.
- Incorporación o sustitución de sistemas de información.
- Ajustes en políticas institucionales, normativas o lineamientos del MinTIC.
- Lecciones aprendidas de simulacros, auditorías o incidentes reales.
- Cambios en el personal, roles o proveedores estratégicos.

Procedimiento para la Gestión de Cambios

El proceso de actualización del DRP se desarrollará siguiendo las siguientes fases:

- a. Identificación del Cambio

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Cualquier funcionario de TI o líder de proceso podrá proponer modificaciones al DRP mediante el *Formato DRP-F15 – Solicitud de Cambio Documental*.
 - La propuesta deberá describir la necesidad, el alcance, la justificación y el impacto esperado.
- b. Evaluación del Cambio
- El Coordinador de TI y la Dirección de Planeación evaluarán la pertinencia técnica, operativa y normativa de la solicitud.
 - Si el cambio afecta componentes críticos (por ejemplo, arquitectura del CPD, proveedores DRaaS, mecanismos de respaldo o roles institucionales), se requerirá análisis de impacto en los tiempos RTO/RPO y validación de seguridad de la información.
- c. Aprobación
- Una vez evaluado, el cambio será aprobado formalmente por la Dirección de Planeación, quedando registrado en el *Acta de Aprobación de Cambios DRP-F16*.
 - La versión actualizada se incorporará al SIG Planeación con la trazabilidad correspondiente.
- d. Implementación
- La Mesa de Ayuda (MDA) será responsable de ejecutar los ajustes técnicos derivados del cambio (actualización de configuraciones, repositorios, respaldos o documentación técnica).
 - Si el cambio implica pruebas de funcionamiento, estas se realizarán en un entorno controlado antes de su despliegue final.
- e. Comunicación
- Una vez aprobado e implementado, el Coordinador de TI notificará oficialmente la nueva versión a los líderes de proceso, con un resumen de los cambios y su impacto operativo.
 - En caso de modificaciones significativas, se realizará una sesión de socialización y capacitación.

Control de Versiones

Cada versión del plan deberá estar debidamente codificada, fechada y documentada, incluyendo un historial detallado de cambios, el control de versiones se llevará mediante la tabla estándar del SIG Planeación, con la siguiente estructura:

Versión	Fecha de Emisión	Descripción del Cambio	Elaboró / Revisó / Aprobó	Observaciones

 EMPRESAS PÚBLICAS DE CUNDINAMARCA S.A. E.S.P.	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

v1.0	Enero 2025	Versión inicial del Plan de Recuperación ante Desastres.	Área de TI / Dirección de Planeación	Documento base alineado con MSPI.
v1.1	Junio 2025	Actualización del inventario de activos críticos y esquema de respaldo 3-2-1-1-0.	MDA / Coordinador de TI	Derivado del simulacro de recuperación.
v1.2	Diciembre 2025	Inclusión del nuevo sistema SIG Planeación y ajustes de proveedores de DRaaS.	Coordinador de TI / Dirección de Planeación	Aprobado mediante Acta DRP-F16.

Mecanismos de Control Documental

- El documento oficial del DRP se conservará en el SIG Planeación, módulo "Continuidad y Seguridad de la Información", bajo acceso restringido al personal autorizado.
- Las versiones previas se archivarán como históricos no vigentes s.
- Todo documento impreso deberá llevar sello de "Copia Controlada" o "Copia No Controlada", según la política de gestión documental de EPC.
- Ningún funcionario podrá editar o distribuir versiones del DRP sin autorización expresa del Coordinador de TI y la Dirección de Planeación.

Actualización Derivada de Auditorías y Simulacros

Cada vez que se realice una auditoría interna o externa, o un simulacro integral del DRP, los hallazgos y recomendaciones deberán evaluarse y, de ser necesarios, incorporarse como cambios documentales, el seguimiento de estos cambios se realizará en el Plan de Mejoramiento del DRP, hasta su cierre formal en el SIG Planeación.

Control de Acceso y Seguridad de la Información

Para proteger la confidencialidad e integridad del documento:

- El DRP será clasificado como documento reservado interno, de conformidad con la Ley 1712 de 2014.
- El acceso al documento digital se limitará al Coordinador de TI, la Dirección de Planeación, y los funcionarios que participen directamente en su ejecución.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Se implementarán registros de control de acceso y trazabilidad sobre todas las ediciones, descargas o modificaciones realizadas.
- Los respaldos del DRP se almacenarán de forma cifrada, tanto en el CPD principal como en el repositorio de contingencia.

Frecuencia de Revisión y Actualización

El DRP deberá ser revisado y actualizado:

- De manera anual, como parte del ciclo de gestión institucional.
- Cada vez que ocurra un evento significativo, como cambios tecnológicos, estructurales o normativos.
- Después de cada simulacro o evento real, para incorporar las lecciones aprendidas y los ajustes requeridos.

Control de Distribución

La distribución controlada del DRP se gestionará mediante el *Registro de Distribución de Documentos DRP-F17*, que identificará:

- Nombres y cargos de los funcionarios con acceso autorizado.
- Fecha de entrega o notificación de actualización.
- Medio de entrega (digital o físico).
- Confirmación de recepción o lectura.

La lista de distribución será revisada y actualizada periódicamente por la Dirección de Planeación, garantizando que solo el personal activo y autorizado disponga de copias vigentes.

Revisión, Actualización y Mejora Continua del DRP

El DRP es un instrumento dinámico que debe mantenerse actualizado conforme evolucionan los servicios tecnológicos, las amenazas y los requisitos institucionales. La revisión y mejora continua se ejecutan bajo el ciclo PHVA, integrado al Sistema Integrado de Gestión (SIG Planeación) y al Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). Su propósito es garantizar que los procedimientos, roles, tiempos de recuperación (RTO/RPO) y mecanismos de respaldo sigan siendo efectivos y coherentes con los objetivos de continuidad institucional.

Frecuencia y Criterios de Revisión

El DRP será revisado y actualizado al menos una vez al año, o cuando se presenten:

- Cambios en la infraestructura tecnológica o los sistemas de información.
- Actualizaciones normativas o lineamientos del MinTIC y del MSPI.
- Resultados de simulacros, auditorías o incidentes reales.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

- Modificaciones en los roles o proveedores críticos.

Las actualizaciones serán lideradas por el Coordinador de TI, validadas por la Mesa de Ayuda (MDA) y aprobadas por la Dirección de Planeación, garantizando trazabilidad documental en el SIG Planeación.

26.3 Fuentes y Mecanismos de Mejora

La mejora continua se fundamenta en:

- Lecciones aprendidas de simulacros y pruebas del DRP.
- Resultados de auditorías internas y externas.
- Recomendaciones del Plan de Mejoramiento Institucional.
- Indicadores de desempeño (cumplimiento de RTO/RPO, disponibilidad, eficacia de recuperación).

Cada acción de mejora se registra y da seguimiento mediante el *Formato DRP-F19 – Plan de Mejoramiento del DRP*, con responsables, fechas y evidencias de cierre.

Control de Versiones y Comunicación

Cada actualización generará una nueva versión codificada del DRP, con descripción de los cambios, fecha de aprobación y responsables, la versión vigente se publicará en el SIG Planeación, conservando las anteriores como históricos por un mínimo de cinco años, toda modificación será comunicada a los líderes de proceso y personal técnico mediante circular interna o sesión informativa.

Indicadores de Seguimiento

Indicador	Meta	Frecuencia
Cumplimiento del ciclo anual de revisión	100 %	Anual
Implementación de acciones de mejora	≥ 85 %	Trimestral
Actualización oportuna tras eventos o auditorías	100 %	Según ocurrencia

La Revisión, Actualización y Mejora Continua del DRP permite mantener su pertinencia, efectividad y conformidad con las normas de gestión de continuidad y seguridad de la información, consolidando la resiliencia tecnológica de EPC y su compromiso con la estabilidad de los servicios públicos que presta.

	Plan de Recuperación ante Desastres (DRP)	Código: GTI-PI019
		Versión: 0
		Fecha: 16/12/2025

CONTROL DE CAMBIOS				
VERSIÓN	FECHA	DESCRIPCION DEL CAMBIO	RESPONSABLE	CARGO
0	16/12/2025	Versión inicial	Diego Ernesto Guevara Forero	Director de Planeación

PROYECTÓ	REVISÓ	APROBÓ
Nombre: Héctor Gil	Nombre: Luz Enith Barbosa	Nombre: Diego Guevara
Cargo: Coordinador TI – Contratista	Cargo: Contratista Dirección de Planeación	Cargo: Director de Planeación
Dirección: Planeación	Dirección: Planeación	Dirección: Planeación
Fecha: 16/12/2025	Fecha: 16/12/2025	Fecha: 16/12/2025

