

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

TABLA DE CONTENIDO

INTRODUCCIÓN	2
OBJETIVO DEL PLAN	3
ALCANCE	4
MARCO NORMATIVO Y REFERENCIAL	5
TÉRMINOS Y DEFINICIONES	7
CONTEXTO ORGANIZACIONAL Y DE TI	9
PRINCIPIOS DE CONTINUIDAD DEL NEGOCIO EN EPC	11
GOBERNANZA Y RESPONSABILIDADES	12
ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)	15
EVALUACIÓN DE RIESGOS DE CONTINUIDAD OPERATIVA	17
ESTRATEGIA DE CONTINUIDAD DEL NEGOCIO	20
PROCESOS CRÍTICOS INSTITUCIONALES Y DEPENDENCIAS TECNOLÓGICAS	23
RECURSOS, INFRAESTRUCTURA Y CAPACIDADES DE RESPALDO	26
PROCEDIMIENTOS DE ACTIVACIÓN DEL PCN	30
ESTRUCTURA DEL COMITÉ Y EQUIPOS DE CONTINUIDAD	33
GESTIÓN DE COMUNICACIÓN Y COORDINACIÓN INSTITUCIONAL	36
GESTIÓN DE PROVEEDORES Y SERVICIOS EXTERNOS CRÍTICOS	40
PLAN DE RESTABLECIMIENTO DE OPERACIONES PRIORITARIAS	44
PROCEDIMIENTOS DE RETORNO A LA NORMALIDAD	47
MECANISMOS DE MONITOREO Y SEGUIMIENTO DEL PCN	50
PROGRAMA DE PRUEBAS, SIMULACROS Y EJERCICIOS DE CONTINUIDAD	54
CAPACITACIÓN, SENSIBILIZACIÓN Y COMPETENCIAS DEL PERSONAL .	58
GESTIÓN DE CAMBIOS Y CONTROL DE VERSIONES DEL PLAN	61
REVISIÓN, ACTUALIZACIÓN Y MEJORA CONTINUA	64

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Introducción

Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), como entidad descentralizada del orden departamental, tiene la responsabilidad de garantizar la continuidad y confiabilidad de los servicios públicos domiciliarios, así como de los procesos misionales y de apoyo que soportan su gestión institucional, en un entorno cada vez más digital y dependiente de las tecnologías de la información, la ocurrencia de eventos disruptivos como: fallas técnicas, ataques cibernéticos, desastres naturales o incidentes operacionales, puede comprometer la disponibilidad, integridad y confidencialidad de la información, afectando la prestación de los servicios, la toma de decisiones y la confianza de los usuarios y partes interesadas.

En este contexto, el Plan de Continuidad del Negocio (PCN) se constituye en un instrumento técnico y estratégico diseñado para asegurar la capacidad operativa de EPC frente a cualquier interrupción significativa, mediante la definición de procedimientos, recursos y estrategias orientadas a la resiliencia organizacional y la recuperación oportuna de las funciones críticas. Este plan complementa los lineamientos del Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el Plan Estratégico de Tecnologías de la Información (PETI), la Matriz de Riesgos de Seguridad de la Información (GTI-F457) y el Modelo de Seguridad y Privacidad de la Información (MSPI), integrando los procesos de continuidad operativa con la gestión del riesgo, la seguridad digital y el aseguramiento de la información institucional.

El PCN define los principios, roles, responsabilidades y mecanismos de coordinación que permiten garantizar la continuidad de los procesos prioritarios y la disponibilidad de los servicios tecnológicos esenciales, a través de un enfoque sistemático basado en riesgo, el plan incorpora los resultados del Análisis de Impacto al Negocio (BIA) y la Evaluación de Riesgos de Continuidad, estableciendo los Objetivos de Tiempo de Recuperación (RTO) y Puntos de Recuperación de Datos (RPO) que guían las estrategias de prevención, respuesta y restablecimiento.

Asimismo, el plan articula los elementos del Sistema Integrado de Gestión (SIG) con los principios de la ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio, garantizando la trazabilidad de las acciones, la documentación de las evidencias y la mejora continua de los mecanismos de respuesta ante contingencias, su aplicación involucra a todas las áreas de la entidad, bajo la dirección del Coordinador de Tecnologías de la Información y la supervisión del Comité de Continuidad y Seguridad, promoviendo la cultura institucional de preparación, prevención y resiliencia.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

El presente documento se concibe como un instrumento dinámico y evolutivo, sujeto a actualización constante según los cambios tecnológicos, organizacionales o normativos que puedan impactar la operación de EPC, su correcta implementación permitirá reducir la vulnerabilidad institucional ante eventos disruptivos, minimizar los impactos operativos, financieros y reputacionales, y fortalecer la confianza ciudadana en la gestión y los servicios que presta la entidad.

Objetivo del Plan

El objetivo del Plan de Continuidad del Negocio (PCN) es establecer el marco técnico, metodológico y organizacional que permita garantizar la continuidad operativa de los procesos institucionales y la disponibilidad de los servicios tecnológicos críticos frente a la ocurrencia de eventos que puedan interrumpir la operación normal de la entidad.

El plan busca fortalecer la resiliencia organizacional de EPC mediante la identificación de los procesos esenciales, la definición de estrategias de mitigación y la implementación de mecanismos efectivos de respuesta, recuperación y restablecimiento ante incidentes, fallas técnicas, ciberataques, desastres naturales u otras situaciones de riesgo.

Este instrumento tiene como finalidad asegurar que la entidad mantenga la prestación oportuna y confiable de los servicios públicos, la integridad de la información institucional y la protección de los activos de TI, salvaguardando los intereses de los usuarios, las comunidades y las partes interesadas.

La aplicación del PCN se enmarca en los principios y buenas prácticas definidos en las normas ISO 22301:2019 Sistemas de Gestión de Continuidad del Negocio, ISO/IEC 27031:2011 Directrices para la Continuidad de las TIC, y ISO/IEC 27001:2022 Seguridad de la Información, así como en los lineamientos de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Plan Estratégico de Tecnologías de la Información (PETI).

De esta manera, el PCN proporciona una estructura integral para planificar, implementar, mantener y mejorar la capacidad institucional de respuesta ante contingencias, garantizando la coherencia con el Sistema Integrado de Gestión (SIG) y contribuyendo al cumplimiento de los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A. E.S.P.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Alcance

El presente Plan aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación, que intervienen directa o indirectamente en la prestación de los servicios públicos domiciliarios, la gestión administrativa y financiera, la planificación institucional, la atención al usuario y la operación de los sistemas tecnológicos que soportan la gestión corporativa.

El alcance comprende la planificación, ejecución, monitoreo y mejora continua de las acciones orientadas a prevenir, responder y recuperar la operación ante incidentes o desastres que afecten la continuidad de los servicios tecnológicos, los procesos de negocio o la integridad de la información institucional.

El PCN abarca las siguientes dimensiones:

- Procesos institucionales críticos, identificados mediante el Análisis de Impacto al Negocio (BIA) y priorizados de acuerdo con su contribución al cumplimiento de los objetivos estratégicos.
- Infraestructura tecnológica y de comunicaciones, incluyendo centros de datos, redes, servidores, sistemas de almacenamiento, respaldos, servicios en la nube y equipos de usuario final.
- Sistemas de información y aplicaciones corporativas que soportan la gestión misional, administrativa y financiera, tales como el Sistema SIG Planeación, el Sistema de Gestión de Proyectos (SIA), el Sistema Comercial, el Sistema de Gestión Documental, entre otros.
- Recursos humanos esenciales, identificando los roles, competencias y responsabilidades necesarias para la ejecución del plan.
- Proveedores y terceros estratégicos, cuya participación es crítica para garantizar la disponibilidad de servicios, plataformas o infraestructuras contratadas.

El PCN se activa ante cualquier evento que pueda comprometer la continuidad operativa, la seguridad de la información o la prestación de los servicios tecnológicos institucionales, incluyendo, entre otros:

- Fallas en la infraestructura tecnológica o de comunicaciones.
- Ataques cibernéticos, pérdida o corrupción de datos.
- Interrupciones eléctricas prolongadas o fallas de sistemas críticos.
- Daños por incendios, inundaciones, vandalismo o desastres naturales.
- Errores humanos o fallas en procesos operativos esenciales.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

El plan no sustituye los procedimientos operativos o técnicos específicos de cada área, sino que los complementa y articula bajo un esquema común de respuesta y coordinación institucional, su implementación se extiende a todas las sedes administrativas y operativas de EPC, garantizando la cobertura integral de los servicios tecnológicos y de información bajo el alcance definido del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Marco Normativo y Referencial

El Plan de Continuidad del Negocio (PCN) se fundamenta en un conjunto de normas, políticas y lineamientos que establecen los criterios, responsabilidades y mejores prácticas para la gestión de la continuidad operativa, la seguridad digital y la protección de la información, este marco garantiza la coherencia con la legislación vigente en materia de administración pública, gestión del riesgo, tecnologías de la información y gobierno digital.

A nivel nacional, el PCN se desarrolla en concordancia con:

- Constitución Política de Colombia (Artículos 2, 209 y 365): establece el deber del Estado de garantizar la prestación continua, eficiente y segura de los servicios públicos esenciales.
- Ley 87 de 1993: define los lineamientos del control interno y el aseguramiento razonable de la gestión institucional.
- Ley 594 de 2000 (Ley General de Archivos): regula la administración, conservación y disponibilidad de la información pública.
- Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública): establece los principios de divulgación, seguridad y reserva de la información.
- Ley 1581 de 2012: regula la protección de datos personales y el tratamiento seguro de información sensible.
- Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC): define las políticas de seguridad digital, continuidad y gobierno electrónico.
- Decreto 338 de 2022: adopta la Política de Gobierno Digital, que incluye el componente de Seguridad y Privacidad de la Información y la gestión de riesgos asociados al uso de las TIC en las entidades públicas.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025): emitida por el DAFP, establece la metodología para la identificación, análisis, valoración y tratamiento del riesgo en el sector público.
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC: instrumento que orienta la implementación del Sistema de Gestión de

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Seguridad y Privacidad de la Información (SGSPI), incluyendo la gestión de continuidad y recuperación ante incidentes.

A nivel internacional, el plan se fundamenta en los estándares y mejores prácticas adoptadas por la entidad, entre ellas:

- ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio: define los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de continuidad del negocio eficaz.
- ISO/IEC 27031:2011 – Directrices para la Continuidad de las TIC: establece un marco de referencia para la preparación y recuperación de los sistemas de información y comunicación ante incidentes.
- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información: proporciona los controles y requisitos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.
- ISO 31000:2018 – Gestión del Riesgo: orienta la aplicación de principios y procesos para la gestión del riesgo corporativo.
- ISO/IEC 27005:2022 – Gestión de Riesgos de Seguridad de la Información: guía la identificación, análisis y tratamiento de los riesgos asociados a los activos de información.
- COBIT 2019: establece principios y prácticas para el gobierno y la gestión de las Tecnologías de la Información.
- NIST SP 800-34 Rev.1: guía para la planificación de la continuidad y recuperación de operaciones de TI.

A nivel institucional, el PCN se articula con los documentos estratégicos, técnicos y operativos de EPC, entre ellos:

- Plan Estratégico Institucional (PEI) 2024–2028
- Plan Estratégico de Tecnologías de la Información (PETI)
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI)
- Matriz GTI-F457 – Riesgos de Seguridad de la Información
- Matriz PDE-F368 – Contexto Estratégico de la Gestión de TI
- Matriz PDE-F369 – Partes Interesadas del área de TI
- Política General de Seguridad de la Información (GTI-PLT002)
- Modelo de Seguridad y Privacidad de la Información (MSPI)
- Plan de Continuidad de TI y Recuperación ante Desastres (DRP)
- Sistema Integrado de Gestión (SIG)

Este marco normativo y referencial garantiza que el PCN mantenga consistencia con las políticas nacionales de seguridad digital, los principios de gestión pública y las directrices del MinTIC, asegurando que las acciones de continuidad sean medibles,

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

auditables y trazables dentro del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y el SIG de EPC.

Términos y Definiciones

Para efectos de interpretación, aplicación y cumplimiento del Plan de Continuidad del Negocio, se adoptan los siguientes términos y definiciones, los cuales garantizan la uniformidad conceptual en la gestión de la continuidad operativa, tecnológica y de servicios críticos dentro de EPC:

Activo de información: Recurso o elemento que contiene, procesa, transmite o soporta información, cuyo valor es fundamental para el cumplimiento de los objetivos institucionales, puede ser tangible (hardware, documentos, instalaciones) o intangible (software, bases de datos, conocimientos, reputación).

Análisis de Impacto al Negocio (BIA): Proceso sistemático para identificar y evaluar las consecuencias de una interrupción en las actividades críticas, estableciendo prioridades de recuperación y objetivos de tiempo (RTO) y punto (RPO).

Apetito de riesgo: Nivel de riesgo que la entidad está dispuesta a aceptar en la búsqueda del cumplimiento de sus objetivos.

Confidencialidad: Propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella.

Continuidad del negocio: Capacidad de una organización para continuar la entrega de productos o servicios en niveles aceptables durante y después de una interrupción.

Control: Medida técnica, organizacional o procedimental implementada para mitigar riesgos y asegurar la protección de los activos de información.

Criterio de criticidad: Parámetro que define la importancia relativa de un proceso, sistema o servicio, con base en su impacto en la operación y su dependencia tecnológica.

Disponibilidad: Propiedad de la información o servicio de estar accesible y utilizable cuando es requerido por un usuario autorizado.

Evento disruptivo: Suceso no planificado que interrumpe parcial o totalmente la operación normal de la entidad, afectando los procesos, la infraestructura tecnológica o los servicios críticos.

Evaluación de riesgos: Actividad orientada a identificar, analizar y valorar las amenazas, vulnerabilidades y riesgos asociados a la continuidad del negocio, con el propósito de establecer medidas de mitigación y control.

Gestión de continuidad: Conjunto de políticas, procedimientos y recursos diseñados para mantener o restablecer las funciones críticas tras una interrupción.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Impacto: Consecuencia o efecto adverso que un incidente o falla puede generar sobre la operación, la información o la reputación institucional.

Infraestructura tecnológica crítica: Conjunto de componentes físicos y lógicos (redes, servidores, almacenamiento, energía, sistemas de respaldo, aplicaciones) cuya operación continua es esencial para la prestación de servicios institucionales.

Mejora continua: Proceso cíclico de revisión, evaluación y actualización del PCN, orientado a optimizar la capacidad de respuesta, aprendizaje organizacional y resiliencia.

Plan de Continuidad del Negocio (PCN): Instrumento que establece las estrategias, procedimientos, roles y responsabilidades necesarios para mantener la operación institucional y garantizar la disponibilidad de los servicios críticos ante incidentes o desastres.

Plan de Recuperación ante Desastres (DRP): Conjunto de procedimientos técnicos orientados a restaurar la infraestructura tecnológica, los sistemas de información y los servicios TIC tras una interrupción grave.

Punto de recuperación objetivo (RPO): Límite máximo de pérdida de datos aceptable, medido en tiempo, que determina hasta qué momento previo al incidente se puede recuperar la información.

Probabilidad: Posibilidad de que un evento o incidente ocurra, considerando factores históricos, técnicos y ambientales.

Proceso crítico: Actividad institucional cuya interrupción afectaría significativamente la operación, el cumplimiento de los objetivos o la prestación de los servicios públicos.

Recuperación: Proceso mediante el cual se restablecen los servicios, sistemas o funciones afectadas por un incidente hasta alcanzar su nivel operativo normal.

Resiliencia organizacional: Capacidad institucional para anticipar, resistir, adaptarse y recuperarse de los impactos adversos de eventos disruptivos, manteniendo la continuidad de las funciones esenciales.

Riesgo residual: Riesgo que permanece después de aplicar las medidas de control y mitigación definidas en el plan.

Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI): Marco de políticas, procedimientos y controles implementado para proteger los activos de información y garantizar la gestión integral de los riesgos de seguridad.

Tolerancia a la interrupción: Periodo máximo durante el cual un proceso o servicio puede permanecer inactivo sin que se produzcan impactos inaceptables en la operación institucional.

Zona de riesgo: Clasificación de la severidad de un riesgo según su probabilidad e impacto, que permite priorizar la aplicación de controles (baja, media, alta, crítica).

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Contexto Organizacional y de TI

Empresas Públicas de Cundinamarca S.A. E.S.P., es una entidad descentralizada de la orden departamental encargada de la gestión, coordinación y prestación de servicios públicos domiciliarios, principalmente de acueducto, alcantarillado y aseo, así como del desarrollo de proyectos de infraestructura, sostenibilidad ambiental y fortalecimiento institucional en el territorio, su operación se sustenta en una estructura organizacional orientada por procesos y soportada por sistemas tecnológicos que garantizan la continuidad del servicio y la toma de decisiones basada en datos confiables.

Desde la perspectiva organizacional, EPC adopta un Modelo de Operación por Procesos estructurado en cuatro niveles: estratégicos, misionales, de apoyo y de evaluación, los cuales interactúan de manera articulada dentro del Sistema Integrado de Gestión (SIG), los procesos estratégicos definen las políticas, metas y direccionamiento institucional; los misionales materializan el objeto social; los de apoyo suministran los recursos y servicios necesarios para la operación; y los de evaluación fortalecen la gestión, el control y la mejora continua.

La función de planeación y control institucional se desarrolla a través de la Dirección de Planeación, responsable de la formulación del Plan Estratégico Institucional (PEI), la coordinación del Plan Estratégico de Tecnologías de la Información (PETI), la Política de Gobierno Digital, el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), dentro de esta dirección se encuentra el Área de Tecnologías de la Información (TI), que cumple el rol de segunda línea de defensa en la gestión del riesgo tecnológico, la ciberseguridad y la continuidad operativa.

El contexto tecnológico de EPC se compone de una infraestructura híbrida y redundante, integrada por un Centro de Procesamiento de Datos (CPD) ubicado en la sede administrativa principal y servicios en nube privada y pública, que alojan los sistemas de información institucionales.

Esta infraestructura incluye:

- Servidores físicos y virtualizados sobre entornos VMware y Windows Server.
- Equipos de almacenamiento NAS/SAN y dispositivos de respaldo automatizados.
- Sistemas de energía ininterrumpida (UPS) y contingencias de respaldo eléctrico.
- Equipos de seguridad perimetral (firewalls, IDS/IPS, VPN).

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Enlaces de comunicaciones LAN/WAN con redundancia y monitoreo permanente.
- Servicios en la nube para correo institucional, colaboración, respaldo y recuperación (Microsoft 365, DRaaS).

La gestión tecnológica está centralizada en la Mesa de Ayuda (MDA), que agrupa los equipos técnicos de infraestructura, redes y comunicaciones, soporte, seguridad de la información y aplicaciones, garantizando la atención de incidentes, el mantenimiento preventivo y la ejecución de procedimientos de continuidad definidos en el PCN y el DRP.

Los sistemas de información institucionales de mayor criticidad son:

- Sistema SIG Planeación: seguimiento a planes, proyectos e indicadores institucionales.
- Sistema de Gestión de Proyectos (SIA): control de ejecución técnica y financiera de proyectos.
- Sistema Comercial: facturación y atención al usuario.
- Sistema de Gestión Documental: administración del ciclo de vida documental y archivo digital.
- Plataforma de Correo Institucional: comunicación, colaboración y respaldo en la nube.
- Sistema de Tickets MDA: gestión de incidentes y solicitudes tecnológicas.

EPC opera bajo un enfoque de gobernanza de TI basado en riesgo y cumplimiento, en el que la Alta Dirección, a través del Comité de Continuidad y Seguridad, establece los lineamientos estratégicos, aprueba los planes y supervisa los resultados, las áreas líderes de proceso son responsables de identificar sus activos de información críticos y definir los procedimientos de recuperación asociados, en articulación con el Área de TI y el Sistema Integrado de Gestión (SIG).

En el ámbito de seguridad y continuidad, la entidad ha implementado políticas y procedimientos alineados con las normas ISO/IEC 27001:2022 y ISO 22301:2019, integrando la gestión de riesgos (GTI-F457), el contexto estratégico (PDE-F368), las partes interesadas (PDE-F369) y la política general de seguridad (GTI-PLT002), este ecosistema normativo permite establecer una línea de defensa sólida frente a amenazas de origen tecnológico, operativo o ambiental.

Su operación depende en alto grado de la disponibilidad de los sistemas de información y de la infraestructura digital, por ello, el contexto organizacional y de TI definido en este plan constituye la base para la aplicación de estrategias de

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

prevención, respuesta y recuperación, garantizando la resiliencia institucional, la confianza ciudadana y la continuidad de los servicios esenciales que presta la entidad.

Principios de Continuidad del Negocio en EPC

La continuidad del negocio en EPC se fundamenta en un conjunto de principios rectores que orientan la planificación, implementación y mejora de las estrategias de resiliencia institucional, asegurando la sostenibilidad operativa, la protección de la información y la prestación ininterrumpida de los servicios públicos esenciales, estos principios se aplican de manera transversal a todos los procesos estratégicos, misionales, de apoyo y de evaluación, garantizando coherencia con el Sistema Integrado de Gestión (SIG) y con los estándares internacionales en gestión de continuidad y seguridad de la información.

El primer principio es la protección de la misión institucional y del servicio público, entendido como la obligación prioritaria de mantener la prestación continua y confiable de los servicios de EPC y de los procesos administrativos y tecnológicos que los soportan, la continuidad no se limita a la restauración de sistemas, sino que abarca la preservación de la capacidad operativa, la integridad de la información y la confianza de los usuarios.

El segundo principio es la gestión basada en el riesgo, que orienta todas las decisiones relacionadas con la prevención, preparación, respuesta y recuperación ante incidentes, las estrategias de continuidad se sustentan en el análisis de impacto al negocio (BIA) y en la evaluación de riesgos de TI, que permiten determinar las prioridades de recuperación y definir los objetivos de tiempo (RTO) y punto de recuperación (RPO) acordes con la criticidad de los procesos y la tolerancia institucional a la interrupción.

El tercer principio es la integración con la seguridad de la información y la ciberresiliencia, lo que garantiza que la continuidad del negocio no opere de forma aislada, sino articulada con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), de este modo, los controles de prevención, detección, respuesta y recuperación definidos en la ISO/IEC 27001:2022 y en el MSPI se aplican también como mecanismos de soporte a la continuidad tecnológica y operativa.

El cuarto principio es la resiliencia tecnológica y organizacional, concebida como la capacidad institucional de anticipar, resistir y recuperarse ante eventos disruptivos, este principio se materializa en el diseño de infraestructuras redundantes,

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

mecanismos de respaldo, virtualización, soluciones en la nube, automatización de procesos críticos y esquemas de replicación de datos, junto con la capacitación continua del personal en gestión de crisis y respuesta a incidentes.

El quinto principio corresponde a la responsabilidad compartida y la coordinación institucional, que implica que todas las áreas de EPC desde la Alta Dirección hasta los equipos técnicos, participan activamente en la planificación y ejecución del plan, cada proceso tiene la obligación de identificar sus activos de información críticos, evaluar sus dependencias tecnológicas y aplicar los procedimientos definidos en el PCN bajo la supervisión del Comité de Continuidad y Seguridad y del Coordinador de TI.

El sexto principio es la trazabilidad y evidencia documental, orientado a garantizar la transparencia, la rendición de cuentas y la posibilidad de auditoría sobre cada acción ejecutada en el marco del PCN, todos los procedimientos, pruebas, simulacros, activaciones o eventos reales deben quedar debidamente documentados en los sistemas de gestión y archivo institucional, de acuerdo con la política de información documentada del SIG.

El séptimo principio es la proporcionalidad y costo-eficiencia, que establece que las medidas de continuidad deben ser adecuadas al nivel de riesgo, la criticidad del proceso y la capacidad institucional de respuesta, este principio promueve el uso racional de los recursos, la priorización de inversiones tecnológicas con mayor impacto en la resiliencia y la adopción de soluciones escalables y sostenibles.

El octavo principio es la mejora continua, entendido como el compromiso permanente de revisar, evaluar y optimizar los mecanismos de continuidad, a través de auditorías, simulacros, análisis post-incidente y actualizaciones periódicas del plan, EPC fortalece su capacidad de prevención y respuesta, adaptándose a los cambios tecnológicos, regulatorios y organizacionales.

En conjunto, estos principios constituyen la base conceptual del PCN y orientan su implementación como un sistema integral de gestión que fortalece la capacidad institucional de anticipar, resistir, responder y recuperarse ante cualquier evento disruptivo, consolidando a EPC como una entidad resiliente, segura y comprometida con la excelencia en la gestión pública.

Gobernanza y Responsabilidades

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La gobernanza del Plan de Continuidad del Negocio se estructura bajo un modelo de dirección jerárquica, colaborativa y basada en el riesgo, que garantiza la claridad de roles, la trazabilidad de decisiones y la efectividad en la coordinación de las acciones antes, durante y después de un evento disruptivo, este modelo se alinea con el Sistema Integrado de Gestión (SIG) y el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), asegurando la integración de la continuidad con los procesos estratégicos, misionales y de apoyo de la entidad.

La estructura de gobernanza del PCN está compuesta por la Dirección de Planeación, el Comité de Continuidad y Seguridad, el Coordinador de Tecnologías de la Información, los Líderes de Proceso, la Mesa de Ayuda (MDA) y las áreas de soporte institucional, quienes actúan conforme a sus competencias, niveles de autoridad y responsabilidades establecidas.

La Dirección de planeación ejerce el rol de patrocinador institucional del PCN, garantizando su aprobación, asignación de recursos y alineación con los objetivos estratégicos, asimismo, define el nivel de apetito de riesgo institucional, autoriza la activación del plan ante incidentes de severidad crítica y evalúa los resultados de las pruebas, simulacros y auditorías de continuidad.

El Comité de Continuidad y Seguridad actúa como el órgano colegiado responsable de la dirección, supervisión y toma de decisiones durante la ejecución del plan, está conformado por la Alta Dirección, el Coordinador de TI, los líderes de proceso, representantes de las áreas misionales y de apoyo, y los enlaces de seguridad de la información.

Sus principales funciones son:

- Establecer las políticas y prioridades estratégicas de continuidad del negocio.
- Evaluar escenarios de riesgo y autorizar la activación del PCN según el nivel de impacto.
- Coordinar la respuesta institucional ante eventos disruptivos y validar la comunicación interna y externa.
- Supervisar la implementación de los planes de tratamiento y recuperación.
- Validar los informes de seguimiento, lecciones aprendidas y mejoras posteriores a la activación.

El Coordinador de Tecnologías de la Información lidera la ejecución operativa del PCN, siendo responsable de coordinar las acciones de respuesta inmediata, validar los tiempos de recuperación (RTO/RPO), dirigir los equipos técnicos de la Mesa de Ayuda (MDA) y mantener la comunicación permanente con el Comité de Continuidad

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

y Seguridad, además, supervisa la implementación de los controles técnicos definidos en la Matriz GTI-F457 y en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI).

Los Líderes de Proceso son responsables de identificar sus activos críticos, documentar sus dependencias tecnológicas, participar en el análisis de impacto al negocio (BIA) y ejecutar las acciones específicas de recuperación dentro de sus áreas, deben mantener actualizada la información de sus procesos y coordinar con el área de TI la verificación de los servicios durante la activación o simulación del PCN.

La Mesa de Ayuda (MDA) cumple un rol técnico esencial en la restauración de los servicios tecnológicos afectados, está integrada por los equipos de infraestructura, redes y comunicaciones, seguridad de la información y soporte y aplicaciones, este grupo ejecuta los procedimientos definidos en el PCN y el DRP, valida la integridad de la información restaurada, monitorea los sistemas durante la recuperación y emite los reportes técnicos de cierre del evento.

El Área de Comunicaciones se encarga de la gestión de la información institucional durante un incidente, garantizando la emisión oportuna, veraz y controlada de los mensajes internos y externos, en coordinación con el Comité de Continuidad y Seguridad, su función es mantener la transparencia informativa, evitar rumores o desinformación y preservar la reputación institucional.

La Oficina Asesora Jurídica y la Oficina de Control Interno cumplen funciones de asesoría y supervisión, la primera asegura el cumplimiento normativo, contractual y de protección de datos personales; mientras que la segunda verifica la correcta ejecución de los procedimientos, la trazabilidad documental y la conformidad del proceso frente a los lineamientos del SIG y los entes de control.

Estructura de Roles y Responsabilidades

Rol / Cargo	Responsabilidades Principales
Director de Planeación de Planeación	Aprobar el plan, garantizar los recursos y supervisar la efectividad del sistema de continuidad.
Comité de Continuidad y Seguridad	Coordinar, validar y monitorear las acciones estratégicas y operativas durante incidentes.
Coordinador de Tecnologías de la Información	Liderar la activación y ejecución del PCN, coordinar la Mesa de Ayuda (MDA) y mantener comunicación con la Alta Dirección.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Líderes de Proceso	Identificar activos críticos, validar la recuperación de sus procesos y participar en ejercicios de simulación.
Mesa de Ayuda (MDA)	Ejecutar acciones técnicas de restauración, monitoreo y verificación de servicios tecnológicos.
Área de Comunicaciones	Gestionar la información institucional y emitir comunicados oficiales durante el evento.
Oficina Asesora Jurídica	Asegurar la conformidad legal y la trazabilidad documental durante el proceso.
Oficina de Control Interno	Supervisar la ejecución del plan, evaluar el cumplimiento y formular recomendaciones de mejora.

Esta estructura de gobernanza garantiza que la gestión de continuidad en EPC sea coordinada, auditable y sostenible, permitiendo que las decisiones se tomen con base en evidencias, dentro de un marco de responsabilidad compartida, cumplimiento normativo y mejora continua.

Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio (Business Impact Analysis – BIA) es una de las fases más críticas dentro del PCN, ya que permite identificar y priorizar los procesos institucionales y los servicios tecnológicos esenciales para la operación de EPC, su propósito es determinar las consecuencias operativas, financieras, legales, reputacionales y sociales que podrían derivarse de una interrupción parcial o total de dichos servicios, estableciendo los Objetivos de Tiempo de Recuperación (RTO) y los Objetivos de Punto de Recuperación (RPO) que orientan la planificación técnica y operativa de la continuidad.

El BIA se desarrolla de manera coordinada entre la Dirección de Planeación, el Área de Tecnologías de la Información (TI), los líderes de proceso y la Alta Dirección, garantizando una evaluación integral del impacto institucional, su aplicación se apoya en la información contenida en la Matriz de Riesgos de Seguridad de la Información (GTI-F457), el PETI, el PESI y el Mapa de Procesos Institucional, consolidando una visión transversal del entorno operativo y tecnológico.

El proceso metodológico del BIA comprende las siguientes etapas:

1. Identificación de procesos y servicios críticos: Cada líder de proceso identifica las actividades esenciales que deben mantenerse en funcionamiento para cumplir con la misión institucional, se evalúan sus dependencias tecnológicas, recursos humanos, instalaciones, proveedores y requerimientos de información.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

2. **Determinación de impactos:** Se analizan los efectos de una interrupción sobre cinco dimensiones:
 - Operacional: afectación de la capacidad para ejecutar funciones esenciales.
 - Financiera: pérdidas económicas, sobrecostos o retrasos en ejecución presupuestal.
 - Legal o regulatoria: incumplimientos normativos o sanciones.
 - Reputacional: daño a la imagen institucional o pérdida de confianza ciudadana.
 - Seguridad y bienestar: riesgos sobre la integridad del personal o la comunidad.
3. **Evaluación del tiempo máximo tolerable de interrupción (MTD):** Determina el periodo máximo que un proceso puede permanecer inactivo sin generar impactos inaceptables.
4. **Definición del RTO (Recovery Time Objective):** Establece el tiempo máximo permitido para restablecer la operación del proceso o sistema afectado tras un incidente.
5. **Definición del RPO (Recovery Point Objective):** Define el punto en el tiempo hasta el cual deben recuperarse los datos sin comprometer la continuidad operativa.
6. **Priorización de procesos y recursos:** Los procesos y sistemas se clasifican según su criticidad (Alta, Media o Baja), con base en la dependencia tecnológica, la magnitud del impacto y la tolerancia institucional a la interrupción.
7. **Consolidación y validación:** Los resultados del BIA se consolidan en una Matriz de Impacto al Negocio, la cual es validada por el Comité de Continuidad y Seguridad y aprobada por la Alta Dirección.

Componentes de la Matriz de Impacto al Negocio

Campo	Descripción
Proceso o área responsable	Unidad organizacional propietaria del proceso.
Servicio o sistema tecnológico asociado	Plataforma o aplicación crítica para la operación del proceso.
Descripción del proceso o servicio	Breve descripción funcional y su relevancia institucional.
Dependencias críticas	Recursos humanos, tecnológicos o de terceros requeridos para su operación.
Consecuencias de la interrupción	Impactos operativos, financieros, legales o reputacionales.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Nivel de criticidad	Alta, Media o Baja, según la importancia del proceso.
MTD (Máximo Tiempo Tolerable de Inactividad)	Periodo máximo que el proceso puede estar interrumpido.
RTO (Objetivo de Tiempo de Recuperación)	Tiempo meta para la recuperación del proceso o sistema.
RPO (Objetivo de Punto de Recuperación)	Pérdida máxima de datos aceptable, medida en tiempo.
Prioridad de recuperación	Orden de restablecimiento conforme al impacto institucional.
Controles y medidas existentes	Controles técnicos o administrativos aplicables.

Criterios de Evaluación del Impacto

Nivel de Impacto	Descripción General
Alto	Interrupción que afecta gravemente la operación institucional, los usuarios o la prestación de servicios públicos.
Medio	Interrupción que limita parcialmente la operación o afecta procesos de apoyo con impacto moderado.
Bajo	Interrupción que puede manejarse localmente sin consecuencias significativas.

El resultado del BIA se utiliza como insumo principal para la Estrategia de Continuidad del Negocio, definida en los capítulos posteriores del plan, además, sus resultados deben revisarse y actualizarse anualmente o cuando ocurran cambios significativos en los procesos, sistemas tecnológicos o estructura organizacional, asegurando la vigencia del análisis y su alineación con los objetivos estratégicos de EPC.

Evaluación de Riesgos de Continuidad Operativa

La Evaluación de Riesgos de Continuidad Operativa constituye un componente esencial del PCN, cuyo propósito es identificar, analizar y valorar los eventos que pueden afectar la capacidad de EPC para mantener la continuidad de sus operaciones y servicios críticos, este proceso permite definir medidas preventivas, predictivas y correctivas que reduzcan la probabilidad de ocurrencia de incidentes o mitiguen su impacto sobre los procesos misionales, de apoyo y estratégicos.

Metodología General

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

El proceso de evaluación de riesgos de continuidad comprende cinco fases principales:

1. Identificación de activos y procesos críticos: Se reconocen los sistemas de información, infraestructuras tecnológicas, servicios, ubicaciones, personal y proveedores esenciales para la operación institucional, los activos se clasifican según su importancia en las dimensiones de Confidencialidad, Integridad y Disponibilidad (CID).
2. Identificación de amenazas: Se identifican los eventos potenciales, de origen interno o externo, que podrían interrumpir los servicios esenciales. Estas amenazas pueden ser:
 - Tecnológicas: fallas en hardware, software, bases de datos, redes, respaldos o energía.
 - Cibernéticas: ataques de ransomware, phishing, denegación de servicio (DDoS), accesos no autorizados.
 - Operativas: errores humanos, fallos en procesos, ausentismo o pérdida de personal clave.
 - Ambientales: incendios, inundaciones, terremotos o desastres naturales.
 - Contractuales: incumplimientos de proveedores o terceros críticos.

Identificación de vulnerabilidades: Se determinan las debilidades que podrían ser explotadas por las amenazas, tales como configuraciones inadecuadas, falta de mantenimiento, ausencia de controles de seguridad, insuficiencia de respaldo o dependencia de un único proveedor.

3. Valoración del riesgo inherente: Se evalúa la probabilidad y el impacto potencial de cada evento disruptivo, utilizando criterios cualitativos y cuantitativos definidos por EPC, conforme a las tablas de riesgo establecidas en la Guía de Gestión Integral del Riesgo.

Nivel de Probabilidad	Descripción
Muy Alta (5)	El evento ocurre frecuentemente o con alta certeza.
Alta (4)	Ocurre al menos una vez al año o es probable bajo condiciones normales.
Media (3)	Puede presentarse ocasionalmente o con causas controlables.
Baja (2)	Evento poco frecuente o con baja posibilidad de ocurrencia.
Muy Baja (1)	Evento improbable o sin antecedentes históricos.
Nivel de Impacto	Descripción

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Catastrófico (5)	Interrupción total de servicios, pérdida de datos o afectación institucional grave.
Mayor (4)	Interrupción significativa con afectación a procesos misionales o financieros.
Moderado (3)	Interrupción parcial o temporal de operaciones.
Menor (2)	Afectación limitada, manejable por el área responsable.
Leve (1)	Impacto mínimo sin consecuencias sobre la operación.

4. El nivel de riesgo inherente se calcula mediante la fórmula: $\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$, lo que permite ubicarlo dentro de una matriz de severidad con cuatro zonas de clasificación:
 - Zona Crítica: Requiere tratamiento inmediato.
 - Zona Alta: Necesita medidas preventivas prioritarias.
 - Zona Media: Debe ser monitoreado y controlado.
 - Zona Baja: Riesgo aceptable dentro del apetito institucional.
5. Identificación y aplicación de controles: Una vez priorizados los riesgos, se definen los controles existentes y propuestos, seleccionados del Anexo A de la norma ISO/IEC 27001:2022, así como los controles administrativos del MSPI y las políticas internas de EPC. Estos controles se clasifican como:
 - Preventivos: buscan evitar la ocurrencia del evento (copias de seguridad, autenticación multifactor, redundancia de red).
 - Predictivos: detectan señales tempranas o anomalías (monitoreo, alertas, SIEM).
 - Correctivos: restauran la operación tras un incidente (recuperación de servicios, restauración de respaldos).

Riesgo Residual y Planes de Tratamiento

Después de la implementación de controles, se determina el riesgo residual, que representa la exposición remanente.

Cuando este nivel se mantiene dentro del apetito de riesgo institucional, se considera aceptable; de lo contrario, se deben aplicar medidas adicionales de tratamiento, clasificadas en:

- Reducir: implementar nuevos controles o fortalecer los existentes.
- Transferir: delegar el riesgo a terceros mediante contratos o pólizas.
- Aceptar: asumir el riesgo si su impacto es mínimo o su mitigación no es costo-eficiente.
- Evitar: eliminar la causa del riesgo mediante la suspensión o modificación del proceso.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Cada riesgo tratado se documenta en el Plan de Acción de Continuidad, el cual detalla las acciones específicas, responsables, plazos de implementación y mecanismos de seguimiento.

Integración con la Gestión de Continuidad y Seguridad

La evaluación de riesgos de continuidad se encuentra plenamente integrada con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), asegurando que los riesgos tecnológicos, de información y operacionales sean tratados de manera coordinada, el proceso se revisa de forma anual, o cuando ocurran cambios significativos en los sistemas, procesos o entornos de operación.

La Evaluación de Riesgos de Continuidad Operativa proporciona la base analítica y técnica para el diseño de las estrategias de continuidad del negocio, priorizando los activos, procesos y recursos que requieren protección inmediata, y garantizando que las medidas implementadas sean proporcionales al nivel de riesgo y alineadas con los objetivos estratégicos de EPC.

Estrategia de Continuidad del Negocio

La Estrategia de Continuidad del Negocio establece el marco técnico y metodológico que orienta la preparación, respuesta y recuperación ante incidentes o interrupciones que afecten los servicios esenciales de EPC, su propósito es mantener la operación institucional en niveles aceptables, garantizar la disponibilidad de los servicios críticos y reducir los impactos operacionales, financieros y reputacionales derivados de eventos disruptivos.

Esta estrategia integra los resultados del Análisis de Impacto al Negocio (BIA), la Evaluación de Riesgos de Continuidad y la Matriz GTI-F457 de Seguridad de la Información, con el fin de definir los escenarios de contingencia y las medidas apropiadas para cada tipo de riesgo, se basa en cuatro pilares fundamentales: prevención, preparación, respuesta y recuperación, aplicados de forma progresiva y coordinada entre las áreas responsables.

Enfoque General

EPC adopta un enfoque preventivo y resiliente, sustentado en los siguientes principios operativos:

- Gestión proactiva del riesgo: los escenarios de interrupción se anticipan mediante el monitoreo continuo de amenazas y vulnerabilidades.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Redundancia y diversificación: la infraestructura crítica se diseña con capacidad de respaldo local y remoto para garantizar la disponibilidad continua.
- Automatización y respaldo digital: los sistemas y datos esenciales se protegen con mecanismos de copias de seguridad programadas bajo el esquema 3-2-1-1-0 (tres copias, dos medios distintos, una fuera del sitio, una inmutable, y cero errores verificados).
- Ciberresiliencia: las estrategias de continuidad integran controles de ciberseguridad, como segmentación de red, autenticación multifactor (MFA), gestión de parches, detección de intrusiones (IDS/IPS) y monitoreo SIEM.
- Capacidad operativa mínima: se establecen configuraciones alternativas y procedimientos manuales o semiautomatizados que permitan mantener los servicios esenciales durante la contingencia.
- Retorno progresivo: los servicios se restablecen de manera gradual, priorizando los sistemas con mayor impacto sobre la operación y los usuarios.

Componentes Estratégicos

La estrategia de continuidad se estructura en cinco componentes interdependientes que aseguran una respuesta eficaz y sostenible ante eventos disruptivos:

a) Estrategia de Prevención: Incluye todas las acciones orientadas a reducir la probabilidad de ocurrencia de incidentes, tales como:

- Implementación de políticas de seguridad, acceso y uso aceptable de la información.
- Mantenimiento preventivo de equipos, sistemas eléctricos y de climatización.
- Ejecución periódica de pruebas de respaldo y restauración de datos.
- Auditorías técnicas y revisiones de vulnerabilidades.
- Fortalecimiento de controles físicos y lógicos de acceso a instalaciones y sistemas.

b) Estrategia de Preparación: Busca asegurar la disponibilidad de recursos, competencias y documentación necesaria para la activación del PCN:

- Capacitación del personal en gestión de incidentes, continuidad y recuperación.
- Actualización anual del BIA, la matriz de riesgos y los inventarios de activos críticos.
- Establecimiento de roles y responsabilidades claramente definidos.
- Pruebas de conectividad, replicación y accesibilidad a los entornos alternos.
- Aseguramiento de contratos con proveedores estratégicos que incluyan cláusulas de continuidad y recuperación.

c) Estrategia de Respuesta: Define los procedimientos de actuación inmediata ante un evento disruptivo, con el fin de contener el impacto y restablecer la funcionalidad básica:

- Activación formal del PCN por parte del Comité de Continuidad y Seguridad.
- Evaluación de la severidad del incidente y priorización de acciones.
- Comunicación inicial a los líderes de proceso, proveedores y personal clave.
- Implementación de medidas de contingencia (conmutación, acceso remoto, respaldo temporal).
- Monitoreo en tiempo real del estado de los sistemas y la infraestructura.

d) Estrategia de Recuperación: Comprende las acciones técnicas y administrativas necesarias para restaurar los servicios afectados y retornar a las condiciones normales de operación:

- Ejecución de los procedimientos definidos en el Plan de Recuperación ante Desastres (DRP).
- Validación de la integridad de los datos recuperados.
- Reincorporación progresiva de servicios y usuarios.
- Verificación de niveles de desempeño y cumplimiento de los RTO/RPO establecidos.
- Elaboración de informes post-incidente y registro de lecciones aprendidas.

e) Estrategia de Mejora Continua

Asegura la revisión periódica de los resultados de las pruebas, incidentes y auditorías, con el fin de fortalecer la efectividad del PCN:

- Evaluación anual de la madurez del sistema de continuidad.
- Actualización de las estrategias según nuevas amenazas o cambios tecnológicos.
- Integración de indicadores de desempeño (KPI) para medir la eficacia del plan.
- Retroalimentación de los resultados al Comité de Continuidad y Seguridad.

Escenarios de Aplicación: La estrategia se activa ante cualquier evento que comprometa la disponibilidad de los servicios críticos, incluyendo:

- Fallas totales o parciales en la infraestructura tecnológica.
- Ataques cibernéticos de alta severidad.
- Interrupciones prolongadas del suministro eléctrico o de comunicaciones.
- Desastres naturales o siniestros en las instalaciones.
- Errores humanos o sabotaje interno.
- Fallos de proveedores o servicios en la nube.

Cada escenario cuenta con procedimientos de actuación documentados que definen responsables, tiempos de respuesta, mecanismos de comunicación y protocolos de recuperación.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La Estrategia de Continuidad del Negocio de EPC permite garantizar la sostenibilidad operativa, la integridad de la información y la confianza institucional, consolidando una infraestructura tecnológica y organizacional capaz de anticipar, resistir y recuperarse de los eventos que puedan afectar la misión institucional.

Procesos Críticos Institucionales y Dependencias Tecnológicas

La identificación y priorización de los procesos críticos es una etapa esencial dentro del PCN, ya que permite establecer las actividades que deben mantenerse o restablecerse en el menor tiempo posible ante una interrupción, asegurando la continuidad de la operación institucional y la prestación de los servicios públicos.

Los procesos críticos se determinan con base en tres criterios fundamentales:

1. Su impacto en el cumplimiento de la misión institucional.
2. Su nivel de dependencia tecnológica respecto de los sistemas de información, infraestructura y comunicaciones.
3. La tolerancia máxima a la interrupción (MTD) establecida en el BIA.

Cada proceso cuenta con servicios tecnológicos, bases de datos y aplicaciones que constituyen sus dependencias operativas, la interrupción de cualquiera de estos componentes puede afectar la ejecución de funciones esenciales o generar impactos financieros, regulatorios y reputacionales para EPC.

Procesos Estratégicos

Proceso	Dependencias Tecnológicas Principales	Sistemas / Aplicaciones Asociadas	Impacto ante Interrupción
Planeación y Direccionamiento Estratégico	Infraestructura de red, servidores institucionales, bases de datos del SIG Planeación	Sistema SIG Planeación, Power BI, Microsoft 365	Afecta la toma de decisiones, seguimiento al plan estratégico y reporte a entes de control.
Gestión de la Información y la Comunicación	Conectividad, servidores de intranet y correo, almacenamiento compartido	Correo institucional, Microsoft Teams, portal web EPC	Interrumpe la comunicación interna, coordinación de procesos y

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

			divulgación institucional.
Evaluación y Control Estratégico	Sistemas de reporte y monitoreo, integraciones con el SIG	SIG Planeación, Power BI	Dificulta el control de metas, evaluación de indicadores y cumplimiento normativo.
Estructuración de Nuevos Negocios y Proyectos	Plataforma de proyectos, bases de datos de inversión y estudios técnicos	Sistema de Gestión de Proyectos (SIA), SharePoint	Afecta la planeación y formulación de nuevos proyectos estratégicos y de infraestructura.

Procesos Misionales

Proceso	Dependencias Tecnológicas Principales	Sistemas / Aplicaciones Asociadas	Impacto ante Interrupción
Gestión de Servicios Públicos	Servidores operativos, redes de campo, sistemas SCADA o de monitoreo	Sistema Comercial, SIG Operativo, base de datos de usuarios	Afecta la prestación de servicios de acueducto, alcantarillado y aseo, generando impacto ciudadano y financiero.
Gestión de Proyectos de Infraestructura	Plataforma de gestión de proyectos, bases de datos de contratistas y supervisión	Sistema SIA, Microsoft Project, SharePoint	Retrasa ejecución de obras, genera incumplimientos contractuales y afecta la imagen institucional.
Gestión Ambiental y de Sostenibilidad	Sistemas de información ambiental, sensores y monitoreo de calidad del agua	Sistema de Control Ambiental, bases de datos geográficas	Impide la vigilancia ambiental y el cumplimiento de normas regulatorias.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Atención al Usuario y Comunidad	Plataformas de atención y comunicación, líneas de servicio	Sistema Comercial, Chat Institucional, página web EPC	Interrumpe la atención ciudadana, recepción de peticiones, quejas y reclamos.
---------------------------------	--	---	---

Procesos de Apoyo

Proceso	Dependencias Tecnológicas Principales	Sistemas / Aplicaciones Asociadas	Impacto ante Interrupción
Gestión Financiera	Servidores financieros, bases de datos contables, autenticación segura	SIIF Territorial, banca electrónica	Afecta pagos, registros contables y ejecución presupuestal.
Gestión Contractual	Servidores documentales, sistema SECOP, correo institucional	SECOP II, Sistema de Gestión Documental, Microsoft 365	Afecta la contratación pública y cumplimiento de plazos legales.
Gestión del Talento Humano	Sistema de nómina y control de personal	Software de Nómina, SIGEP II	Genera retrasos en pagos y cumplimiento de obligaciones laborales.
Gestión Administrativa y Logística	Equipos de red, servidores de archivo y control de inventarios	Sistema de Inventarios, control vehicular, sistema de correspondencia	Dificulta la adquisición de bienes y servicios, y la trazabilidad administrativa.
Gestión de la Información y Seguridad Digital	Servidores virtualizados, respaldo de datos, plataformas en nube	Consola de administración MDA, NAS, DRaaS, SIEM	Interrumpe la protección de información y gestión de incidentes.

Procesos de Evaluación y Control

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Proceso	Dependencias Tecnológicas Principales	Sistemas / Aplicaciones Asociadas	Impacto ante Interrupción
Control Interno	Plataforma de auditoría, sistemas de registro y seguimiento SIG	SIG Planeación, Sistema de Mejoramiento, Power BI	Impide la trazabilidad de auditorías y planes de mejora.
Jurídico y Cumplimiento	Sistema de gestión de procesos legales, correo institucional	Sistema Jurídico EPC, Microsoft 365	Afecta la gestión jurídica y atención a procesos legales.
Comunicaciones y Transparencia	Portal web, sistemas de publicación y control de acceso	Portal EPC, sitio web institucional, intranet	Limita la divulgación de información y compromete la transparencia pública.

Dependencias Transversales de Tecnología

Todos los procesos institucionales dependen de una base común de servicios tecnológicos y de infraestructura, cuya indisponibilidad puede tener impacto global:

- Centro de Procesamiento de Datos (CPD): Servidores, virtualización, almacenamiento, energía y climatización.
- Red de Comunicaciones: Enlaces LAN/WAN, VPN y acceso remoto seguro.
- Correo Institucional y Colaboración: Microsoft 365, Teams y SharePoint.
- Sistema de Respaldo y Recuperación (DRaaS): Copias de seguridad locales y en nube.
- Seguridad de la Información: Firewalls, IDS/IPS, antivirus corporativo, SIEM.
- Mesa de Ayuda (MDA): Soporte técnico, atención de incidentes y ejecución de planes de continuidad.

La correcta identificación de los procesos críticos y sus dependencias tecnológicas permite definir las prioridades de recuperación y establecer los mecanismos adecuados para garantizar la continuidad operativa. Estos resultados sirven como base para la elaboración del Plan de Restablecimiento de Operaciones y del Plan de Recuperación ante Desastres (DRP), fortaleciendo la resiliencia institucional y la capacidad de respuesta de EPC.

Recursos, Infraestructura y Capacidades de Respaldo

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La resiliencia operativa de EPC depende directamente de la robustez, disponibilidad y redundancia de sus recursos tecnológicos, humanos, físicos y logísticos, que en conjunto conforman la base para garantizar la continuidad de los servicios institucionales en caso de incidentes, fallas o desastres, este capítulo describe los elementos críticos que soportan la infraestructura tecnológica, las capacidades de respaldo y los mecanismos de recuperación disponibles.

Recursos Tecnológicos Críticos

Los recursos tecnológicos comprenden los sistemas de información, equipos, plataformas, redes y servicios de comunicación que soportan la operación institucional.

EPC cuenta con una arquitectura híbrida y redundante, estructurada en los siguientes componentes:

- Centro de Procesamiento de Datos (CPD): ubicado en la sede administrativa principal, dotado con servidores físicos y virtualizados (VMware), sistemas de almacenamiento NAS/SAN, dispositivos de respaldo automatizado y controles de acceso físico y ambiental (energía ininterrumpida, UPS, climatización redundante, extinción automática y monitoreo CCTV).
- Infraestructura de Red: compuesta por enlaces LAN/WAN redundantes, segmentación por VLAN, conexiones VPN seguras, balanceadores de carga y monitoreo constante mediante herramientas de diagnóstico.
- Plataforma de Correo y Colaboración: basada en Microsoft 365, con servicios de correo institucional, SharePoint, OneDrive y Teams, que permiten continuidad operativa y acceso remoto durante contingencias.
- Sistemas de Información Corporativos: Sistema SIG Planeación, Sistema de Gestión de Proyectos (SIA), Sistema Comercial, Sistema de Gestión Documental y aplicaciones misionales y de apoyo interconectadas mediante autenticación centralizada (AD) y MFA.
- Plataformas de Respaldo y Recuperación: implementadas bajo el esquema 3-2-1-1-0, que garantiza tres copias de seguridad en dos tipos de medios diferentes, una fuera del sitio (off-site), una inmutable en nube y cero errores verificados mediante pruebas automáticas de integridad.
- Infraestructura de Seguridad Digital: compuesta por firewalls de nueva generación, sistemas de detección y prevención de intrusiones (IDS/IPS), gestión centralizada de eventos (SIEM), antivirus corporativo, políticas de control de acceso y cifrado de información sensible.
- Servicios en la Nube y DRaaS: contratación de proveedores certificados que ofrecen servicios de continuidad de negocio y recuperación ante desastres

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

(Disaster Recovery as a Service), con disponibilidad garantizada bajo Acuerdos de Nivel de Servicio (SLA $\geq$ 99.9%).

Recursos Humanos y Competencias

La continuidad operativa depende del personal clave que posee conocimientos técnicos y operativos necesarios para activar y ejecutar el PCN. Los recursos humanos se clasifican según su rol dentro del plan:

- Coordinador de TI: lidera la activación del PCN, la coordinación técnica y la comunicación con la Alta Dirección.
- Mesa de Ayuda (MDA): ejecuta tareas técnicas de recuperación, soporte de infraestructura, redes, seguridad y aplicaciones.
- Líderes de Proceso: garantizan la continuidad funcional de sus áreas, aplican procedimientos alternos y validan la restauración de servicios.
- Comité de Continuidad y Seguridad: toma decisiones estratégicas, supervisa la respuesta y autoriza el retorno a la normalidad.
- Área de Comunicaciones: asegura la difusión controlada de información interna y externa durante la contingencia.

El personal asignado al PCN debe contar con capacitación técnica certificada, conocimiento de los procedimientos del plan, acceso controlado a los recursos críticos y entrenamiento en simulacros y escenarios de recuperación.

Recursos Físicos y Logísticos

Los recursos físicos garantizan las condiciones necesarias para la operación y recuperación de servicios durante una contingencia. Incluyen:

- Sedes alternas operativas: espacios designados para la reubicación temporal del personal crítico en caso de indisponibilidad del edificio principal.
- Equipos de respaldo: computadores portátiles configurados con acceso VPN, periféricos esenciales y dispositivos móviles institucionales.
- Sistemas de energía de respaldo: UPS con autonomía mínima de 30 minutos y plantas eléctricas de emergencia con capacidad para mantener el CPD y los servicios prioritarios.
- Climatización redundante: equipos de aire acondicionado dual con control automático de temperatura y humedad para el CPD.
- Conectividad de contingencia: enlaces redundantes de diferentes proveedores para asegurar disponibilidad de comunicaciones.
- Equipos de impresión y escaneo alternos: habilitados para mantener el flujo documental durante interrupciones.

Recursos Contractuales y de Proveedores

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La continuidad del negocio depende también del cumplimiento de los acuerdos de nivel de servicio (SLA) y acuerdos de continuidad (OLA) suscritos con los proveedores de servicios tecnológicos y operativos.

EPC mantiene contratos activos con proveedores estratégicos que cubren:

- Servicios de Internet y comunicaciones.
- Mantenimiento y soporte de infraestructura tecnológica.
- Almacenamiento y respaldo en nube.
- Licenciamiento y soporte de software crítico.
- Servicios de energía y climatización.
- DRaaS y servicios de soporte técnico remoto.

Cada contrato incluye cláusulas de confidencialidad, disponibilidad y continuidad, así como tiempos máximos de respuesta ante incidentes, el cumplimiento de estas obligaciones es supervisado por el Coordinador de TI y reportado al Comité de Continuidad y Seguridad.

Capacidad de Respaldo y Redundancia

EPC implementa una estrategia integral de respaldo basada en los principios de redundancia, distribución geográfica y replicación síncrona/asíncrona:

- Redundancia de infraestructura: servidores y dispositivos críticos configurados en clústeres activos-activos y activos-pasivos.
- Replicación de datos: sincronización de información entre el CPD principal y la nube institucional.
- Backups automáticos: ejecución diaria con retención de versiones históricas y verificación automática de integridad.
- Recuperación automatizada: mediante scripts y herramientas de orquestación que reducen los tiempos de restauración.
- Verificación periódica: pruebas de restauración programadas trimestralmente con registro de resultados en el SIG.

En conjunto, los recursos tecnológicos, humanos, físicos y contractuales de EPC conforman una infraestructura robusta, resiliente y preparada para responder ante contingencias, asegurando la continuidad de las operaciones y la protección de la información institucional.

La correcta gestión y actualización de estos recursos es responsabilidad compartida entre la Dirección de Planeación, el Área de TI, los Líderes de Proceso y el Comité de Continuidad y Seguridad, quienes deben garantizar su disponibilidad, mantenimiento y mejora continua.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Procedimientos de Activación del PCN

Los Procedimientos de Activación del Plan de Continuidad del Negocio (PCN) establecen el conjunto de pasos formales y operativos que deben seguirse para declarar, ejecutar y controlar la respuesta ante una interrupción significativa de los servicios institucionales o tecnológicos, su aplicación garantiza una actuación coordinada, documentada y eficiente, evitando la improvisación y reduciendo el impacto sobre los procesos críticos de EPC.

La activación del plan puede originarse por la detección de un incidente, una interrupción no planificada, o la notificación de un evento de riesgo que comprometa la continuidad operativa o tecnológica, los procedimientos definidos a continuación establecen las condiciones, responsabilidades, comunicación y flujo de decisión necesarios para activar, mantener y cerrar el PCN.

Condiciones de Activación

El PCN podrá activarse cuando ocurra cualquiera de las siguientes situaciones:

- Interrupción total o parcial de los servicios tecnológicos críticos (servidores, red, correo, sistemas misionales).
- Ataques cibernéticos que comprometan la integridad o disponibilidad de la información.
- Fallas graves en el suministro de energía, climatización o comunicaciones.
- Daños estructurales o físicos en las instalaciones del CPD o la sede principal.
- Pérdida o corrupción de datos institucionales.
- Eventos naturales o externos (inundaciones, incendios, sismos, actos vandálicos, sabotaje).
- Incumplimientos contractuales de proveedores que afecten la operación esencial.
- Recomendación de activación emitida por el Comité de Continuidad y Seguridad o la Alta Dirección.

Niveles de Severidad del Evento

Los eventos se clasifican según su magnitud y efecto sobre la operación institucional, con el fin de definir la respuesta proporcional y los recursos requeridos:

Nivel	Descripción del Evento	Responsable de Activación	Acciones Generales
Nivel 1 – Bajo	Incidente controlado localmente sin afectación significativa.	Mesa de Ayuda (MDA)	Registrar el evento, aplicar control correctivo,

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

			notificar al Coordinador de TI.
Nivel 2 – Medio	Interrupción parcial o temporal de uno o varios sistemas institucionales.	Coordinador de TI	Evaluar impacto, activar equipo técnico, informar al Comité de Continuidad y Seguridad.
Nivel 3 – Alto	Fallo que afecta servicios críticos o impide la operación normal.	Coordinador de TI y Comité de Continuidad y Seguridad	Activar PCN, escalar a Alta Dirección, ejecutar procedimientos de recuperación.
Nivel 4 – Crítico	Evento mayor o desastre que compromete la infraestructura principal o la seguridad institucional.	Alta Dirección	Declarar contingencia total, activar sedes alternas y DRP, comunicar externamente y coordinar retorno a la normalidad.

Fases del Proceso de Activación

La activación del PCN se desarrolla en cinco fases secuenciales, cada una con objetivos, responsables y resultados definidos:

Fase 1: Detección y Notificación

- Identificación inicial del evento por parte del Mesa de Ayuda (MDA).
- Registro del incidente en el sistema de gestión de tickets.
- Evaluación preliminar de impacto y clasificación del nivel de severidad.
- Notificación inmediata al Coordinador de TI y al Comité de Continuidad y Seguridad.

Fase 2: Evaluación y Declaratoria

- Análisis del evento, su alcance y afectación sobre los servicios.
- Validación de la necesidad de activar el PCN por parte del Coordinador de TI.
- Comunicación formal de activación al Comité de Continuidad y Seguridad.
- Autorización de la Alta Dirección en caso de eventos de nivel 3 o 4.

Fase 3: Ejecución del Plan

- Activación de los equipos técnicos y funcionales.
- Implementación de las medidas de contención y recuperación inicial.
- Comunicación institucional interna (correo, canales oficiales).
- Monitoreo continuo del estado de los servicios críticos.
- Coordinación con proveedores externos, si aplica.

Fase 4: Seguimiento y Control

- Registro de avances, decisiones y acciones ejecutadas.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Validación de los tiempos RTO/RPO y control de riesgos residuales.
- Evaluación del impacto residual sobre los procesos y usuarios.
- Comunicación de estado al Comité de Continuidad y Seguridad.

Fase 5: Cierre y Retorno a la Normalidad

- Validación de la recuperación completa de los servicios.
- Reincorporación progresiva del personal y procesos a las operaciones normales.
- Desactivación formal del PCN.
- Elaboración de informe técnico y administrativo del evento.
- Registro de lecciones aprendidas y plan de mejora posterior al incidente.

Comunicación Durante la Activación

Durante la ejecución del PCN, toda comunicación debe seguir los protocolos definidos por el Área de Comunicaciones y el Comité de Continuidad y Seguridad, asegurando la emisión oportuna, precisa y verificable de la información.

Las notificaciones se emitirán en el siguiente orden:

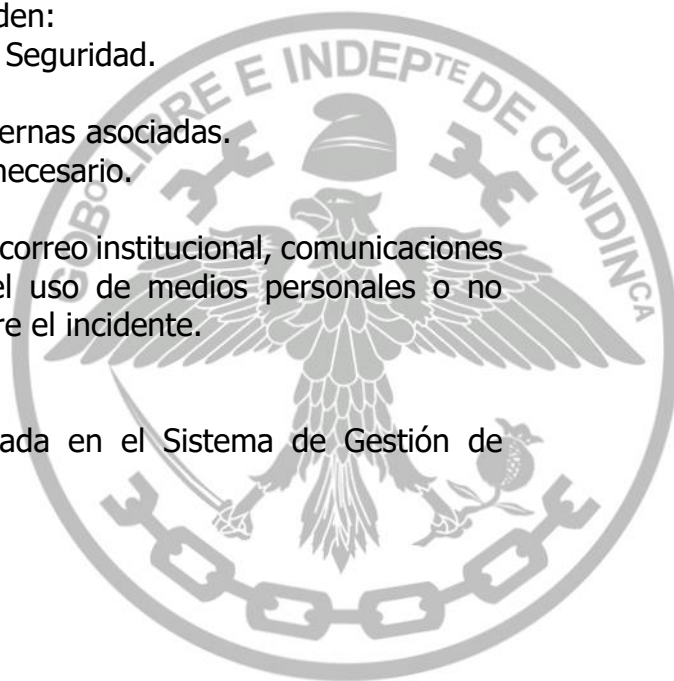
1. Alta Dirección y Comité de Continuidad y Seguridad.
2. Líderes de proceso y personal clave.
3. Proveedores estratégicos y entidades externas asociadas.
4. Usuarios internos y público, cuando sea necesario.

Se utilizarán los canales institucionales oficiales (correo institucional, comunicaciones internas y portal web), quedando prohibido el uso de medios personales o no controlados para la difusión de información sobre el incidente.

Registro y Documentación

Cada activación del PCN debe quedar registrada en el Sistema de Gestión de Incidentes o en el SIG Planeación, incluyendo:

- Fecha y hora del evento.
- Causa y descripción del incidente.
- Nivel de severidad.
- Sistemas y procesos afectados.
- Acciones ejecutadas y responsables.
- Tiempos de recuperación (RTO/RPO alcanzados).
- Evidencias documentales y registros técnicos.
- Lecciones aprendidas y acciones de mejora.



	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Toda esta información se consolida en el Informe de Activación del PCN, documento obligatorio que servirá como insumo para auditorías internas, revisiones de continuidad y actualización del plan.

Estos procedimientos garantizan una respuesta estructurada y controlada ante cualquier evento disruptivo, minimizando los tiempos de inactividad, los impactos financieros y operativos, y fortaleciendo la capacidad institucional de respuesta y resiliencia.

Estructura del Comité y Equipos de Continuidad

La estructura de continuidad define la organización jerárquica y funcional responsable de la activación, coordinación, ejecución y supervisión del PCN, este modelo está basado en el principio de responsabilidad compartida, asegurando la participación de todas las áreas institucionales y garantizando que las decisiones se tomen de forma oportuna, trazable y alineada con los objetivos estratégicos de EPC.

La estructura está compuesta por tres niveles de actuación:

1. Nivel Estratégico: Dirección general y Comité de Continuidad y Seguridad.
2. Nivel Operativo: Coordinador de TI, líderes de proceso y equipos técnicos.
3. Nivel de Soporte: áreas transversales de comunicación, jurídica y control interno.

Cada nivel cumple funciones específicas orientadas a la dirección, ejecución técnica y control de las acciones de continuidad, asegurando la coordinación efectiva durante todas las fases del plan.

Comité de Continuidad y Seguridad

El Comité de Continuidad y Seguridad es la máxima instancia de dirección del PCN. Está conformado por representantes de la Alta Dirección, el Coordinador de TI, líderes de proceso, responsables de seguridad de la información y enlaces de apoyo institucional.

Su principal función es tomar decisiones estratégicas durante la activación, coordinar las acciones institucionales y autorizar el retorno a la normalidad una vez superada la contingencia.

Funciones principales:

- Aprobar la activación o desactivación del PCN y supervisar su ejecución.
- Evaluar el impacto institucional y determinar prioridades de recuperación.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Coordinar la comunicación con los entes de control, proveedores y ciudadanía.
- Validar los informes técnicos y administrativos de los eventos.
- Aprobar los planes de mejora y acciones preventivas derivadas de incidentes.

Integrantes permanentes:

- Gerente General.
- Coordinador de Tecnologías de la Información.
- Dirección de Planeación.
- Dirección de Gestión Financiera.
- Dirección de Gestión Contractual.
- Dirección de Talento Humano.
- Asesor Jurídico.
- Control Interno.
- Comunicaciones Institucionales.

El Comité podrá convocar, de manera temporal, a otros funcionarios o contratistas especializados según la naturaleza del evento o los sistemas afectados.

Coordinador de Tecnologías de la Información

El Coordinador de TI es el responsable operativo del PCN, dirige la ejecución técnica del plan, coordina los equipos de recuperación, mantiene comunicación permanente con la Alta Dirección y reporta el avance de las acciones al Comité de Continuidad y Seguridad.

Funciones específicas:

- Activar los procedimientos del PCN según el nivel de severidad del evento.
- Coordinar las labores de diagnóstico, contención y restauración de servicios.
- Validar la integridad de los datos y el cumplimiento de los RTO/RPO definidos.
- Documentar el proceso de activación y elaborar el informe técnico final.
- Garantizar la comunicación continua entre la Mesa de Ayuda (MDA) y los líderes de proceso.

Líderes de Proceso

Los Líderes de Proceso son responsables de garantizar la continuidad de las actividades en sus áreas de competencia, durante una contingencia, deben aplicar los procedimientos alternos definidos, priorizar las funciones críticas y coordinar con el Coordinador de TI la validación del restablecimiento de los servicios.

Funciones principales:

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Identificar los activos críticos de su proceso y mantenerlos actualizados.
- Ejecutar los procedimientos manuales o de contingencia cuando los sistemas no estén disponibles.
- Comunicar de inmediato cualquier afectación al Coordinador de TI.
- Validar la recuperación de la información y el restablecimiento de los servicios.
- Participar en simulacros, ejercicios y revisiones periódicas del plan.

Mesa de Ayuda (MDA)

La Mesa de Ayuda (MDA) constituye el equipo técnico responsable de ejecutar las acciones de recuperación y restauración de servicios durante la activación del PCN.

Está conformada por los siguientes subequipos especializados:

- Infraestructura: encargado del restablecimiento de servidores, almacenamiento, respaldos, energía y climatización del CPD.
- Seguridad de la Información: valida la integridad de los datos, analiza los registros de auditoría y aplica controles de protección durante la recuperación.
- Redes y Comunicaciones: restablece la conectividad LAN/WAN, VPN y servicios de comunicación interna y externa.
- Soporte y Aplicaciones: restaura los sistemas de información, bases de datos, aplicativos institucionales y servicios en nube.

Funciones de la MDA:

- Ejecutar las tareas técnicas de restauración conforme a los procedimientos del DRP.
- Monitorear la disponibilidad y estabilidad de los sistemas durante la recuperación.
- Registrar las evidencias técnicas y documentar las acciones ejecutadas.
- Coordinar con los proveedores externos en la activación de servicios contratados (DRaaS, nube, telecomunicaciones).
- Informar al Coordinador de TI sobre el avance y resultados de la restauración.

Áreas de Soporte Institucional

Durante la ejecución del PCN, las áreas de soporte transversal cumplen funciones específicas que complementan la gestión técnica y operativa:

Área	Responsabilidades durante la activación del PCN
Comunicaciones Institucionales	Gestionar la emisión de comunicados oficiales, coordinar la información interna y externa, evitar difusión no autorizada.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Oficina Jurídica	Asesora	Asesorar sobre cumplimiento normativo, contratos, confidencialidad y manejo de datos personales durante la contingencia.
Oficina de Control Interno		Supervisar la correcta aplicación de los procedimientos, documentar hallazgos y emitir recomendaciones para la mejora.
Talento Humano		Garantizar la disponibilidad del personal clave, coordinar turnos y apoyo logístico para la atención del evento.
Gestión Administrativa y Logística		Asegurar la disponibilidad de sedes alternas, equipos de respaldo y suministros críticos.

Cadena de Comunicación y Escalamiento

La comunicación durante la activación del PCN seguirá la siguiente jerarquía:

1. Mesa de Ayuda (MDA) detecta y reporta el incidente al Coordinador de TI.
2. El Coordinador de TI evalúa el impacto y comunica la situación al Comité de Continuidad y Seguridad.
3. El Comité determina el nivel de severidad y notifica a la Alta Dirección.
4. El Área de Comunicaciones emite los comunicados institucionales.
5. Los Líderes de Proceso informan a su personal operativo y activan los planes específicos.

Toda la comunicación debe registrarse en los medios institucionales (correo, OSTicket), preservando trazabilidad y evidencia documental.

Esta estructura organizacional garantiza que el Plan de Continuidad del Negocio se ejecute con coordinación, responsabilidad y trazabilidad, permitiendo que las acciones técnicas, administrativas y comunicacionales se desarrollen de manera integrada y eficiente ante cualquier evento disruptivo.

Gestión de Comunicación y Coordinación Institucional

La gestión de comunicación y coordinación institucional durante la activación del PCN tiene como objetivo garantizar el flujo oportuno, veraz y controlado de la información entre los diferentes niveles de la organización, los proveedores estratégicos, las autoridades competentes y, cuando sea necesario, la ciudadanía.

Una comunicación adecuada minimiza la incertidumbre, facilita la toma de decisiones, fortalece la confianza institucional y evita la difusión de información no autorizada o contradictoria.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Principios de Comunicación durante Contingencias

La comunicación institucional en el marco del PCN se rige por los siguientes principios:

- Oportunidad: la información debe emitirse de manera inmediata una vez validada por las autoridades competentes.
- Veracidad: todos los comunicados deben basarse en información confirmada y verificable.
- Coherencia: los mensajes deben ser consistentes entre todas las áreas y voceros institucionales.
- Confidencialidad: la información sensible o clasificada debe manejarse conforme a los lineamientos del MSPI y las políticas de protección de datos personales.
- Trazabilidad: todas las comunicaciones deben registrarse formalmente en los medios institucionales autorizados.
- Accesibilidad: los mensajes deben transmitirse por canales que aseguren su recepción efectiva por los destinatarios.

Estructura de Comunicación Interna

Durante la activación del PCN, la comunicación interna seguirá una estructura jerárquica definida para garantizar la coordinación fluida entre todos los actores involucrados:

Nivel / Rol	Medio de Comunicación Autorizado	Responsabilidad
Alta Dirección y Comité de Continuidad y Seguridad	Reuniones de emergencia, OsTicket, correo institucional	Tomar decisiones estratégicas y aprobar comunicados externos.
Coordinador de TI	OsTicket, correo institucional, línea telefónica prioritaria	Informar estado técnico de los servicios, coordinar respuesta con MDA y líderes de proceso.
Mesa de Ayuda (MDA)	Sistema de tickets, OsTicket, radio institucional, WhatsApp corporativo (controlado)	Reportar incidentes, actualizar estado de recuperación y mantener comunicación técnica constante.
Líderes de Proceso	OsTicket, correo institucional, reuniones virtuales	Informar afectaciones operativas, ejecutar planes alternos y coordinar con el personal bajo su cargo.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Talento Humano y Logística	Correo institucional y comunicaciones internas	Garantizar disponibilidad del personal y soporte operativo durante la contingencia.
----------------------------	--	---

Toda comunicación interna deberá ser centralizada a través del Coordinador de TI y el Área de Comunicaciones Institucionales, evitando la emisión de mensajes directos no autorizados sobre el estado de la emergencia.

Comunicación Externa

La comunicación externa durante la activación del PCN será responsabilidad del Área de Comunicaciones Institucionales, bajo la supervisión del Comité de Continuidad y Seguridad y la Alta Dirección.

Esta comunicación se realizará únicamente cuando sea necesario informar a los siguientes actores externos:

- Usuarios y ciudadanía: cuando los servicios públicos o plataformas institucionales presenten afectaciones que impacten su atención o uso.
- Entes de control y supervisión: Contraloría, Procuraduría, MinTIC, Gobernación de Cundinamarca, entre otros, cuando los eventos afecten el cumplimiento de obligaciones institucionales.
- Proveedores estratégicos: para coordinar acciones de soporte técnico, continuidad contractual y restablecimiento de servicios.
- Medios de comunicación: únicamente por canales oficiales y mediante comunicados validados por la Gerencia y el Comité de Continuidad y Seguridad.

Canales oficiales de comunicación externa:

- Página web institucional (<https://epc.com.co/>).
- Correo institucional (bajo dominio oficial @epc.com.co).
- Boletines de prensa y comunicados oficiales.
- Redes sociales institucionales (Facebook, X/Twitter, Instagram) administradas por Comunicaciones.
- Oficios o circulares firmados por la Gerencia General o su delegado.

Coordinación Interinstitucional

Durante la atención de una contingencia, la coordinación institucional entre áreas internas y externas es clave para garantizar la eficacia del PCN.

EPC mantiene mecanismos de coordinación con:

- Proveedores tecnológicos: para activación de servicios de respaldo, nube, comunicaciones, DRaaS y soporte remoto.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Autoridades locales y departamentales: para la gestión de emergencias que comprometan la infraestructura física o los servicios públicos.
- Entidades aliadas: como la Gobernación de Cundinamarca, Empresas Públicas municipales, y organismos de control que requieran reportes de continuidad.
- Entes de control: en caso de incidentes con impacto financiero, contractual o reputacional, conforme a las obligaciones de reporte del SIG.

La coordinación se gestiona a través del Comité de Continuidad y Seguridad, que actuará como canal único de enlace con las entidades externas y supervisará la trazabilidad de la información compartida.

Protocolos de Comunicación durante la Contingencia

Durante la ejecución del PCN, se aplicarán los siguientes protocolos:

1. Comunicación inicial del incidente: notificación inmediata por parte de la Mesa de Ayuda al Coordinador de TI.
2. Confirmación de evento y nivel de severidad: validación por el Comité de Continuidad y Seguridad.
3. Comunicación de activación: mensaje oficial emitido por el Área de Comunicaciones y avalado por la Alta Dirección.
4. Actualizaciones periódicas: cada 30 minutos o según el avance del evento, mediante Teams o correo institucional.
5. Comunicación de cierre y retorno: informe final y comunicado de normalización de servicios.

Registro y Trazabilidad de la Comunicación

Toda comunicación interna y externa relacionada con la activación del PCN debe quedar documentada en los sistemas institucionales, asegurando trazabilidad y evidencia para auditoría.

Los principales registros son:

- Registro de Activación del PCN.
- Registro de Comunicaciones Emitidas (interna/externa).
- Informe de Estado de la Contingencia.
- Acta de Cierre y Retorno a la Normalidad.

Estos documentos deberán ser almacenados en el Sistema de Gestión Documental Institucional y vinculados al expediente digital del PCN en el SIG Planeación, conforme a los procedimientos de gestión documental de la entidad.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La gestión de comunicación y coordinación institucional garantiza que, ante cualquier contingencia, EPC mantenga un flujo informativo confiable, ordenado y transparente, preservando la reputación institucional y asegurando que las decisiones se tomen con base en información verificable, bajo control y trazabilidad permanente.

Gestión de Proveedores y Servicios Externos Críticos

La Gestión de Proveedores y Servicios Externos Críticos tiene como propósito garantizar que los terceros que suministran bienes o servicios tecnológicos, operativos o estratégicos a EPC, contribuyan al cumplimiento de los objetivos de continuidad y resiliencia institucional.

Los proveedores son parte integral del ecosistema de operación y deben incorporar controles, niveles de servicio y mecanismos de contingencia acordes con los requerimientos establecidos por la entidad en su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y el Sistema Integrado de Gestión (SIG).

Enfoque de Gestión de Proveedores

EPC adopta un enfoque de gestión basado en riesgo y cumplimiento, que prioriza la selección, contratación y monitoreo de proveedores estratégicos según su nivel de impacto sobre la operación institucional.

Este enfoque se apoya en los siguientes principios:

- Evaluación previa de riesgos: todo proveedor es evaluado en materia de seguridad de la información, continuidad del servicio, experiencia técnica y cumplimiento legal antes de su contratación.
- Responsabilidad compartida: los terceros deben cumplir las políticas institucionales de seguridad, confidencialidad y continuidad, conforme al alcance del servicio contratado.
- Alineación normativa: los contratos deben incorporar cláusulas que aseguren el cumplimiento de los estándares internacionales (ISO 22301, ISO 27001, ISO 27036) y la normatividad nacional en materia de seguridad digital y protección de datos personales.
- Trazabilidad y monitoreo: los compromisos de los proveedores se supervisan de manera continua mediante informes, auditorías y revisiones técnicas o contractuales.

Clasificación de Proveedores

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Los proveedores se clasifican según su nivel de criticidad e impacto sobre la continuidad operativa:

Categoría	Tipo de Servicio o Suministro	Nivel de Impacto en Continuidad	Ejemplos
Críticos	Soporte tecnológico, servicios en nube, comunicaciones, energía, respaldo y DRaaS.	Alto – su interrupción afecta directamente la operación institucional.	Proveedores de nube, telecomunicaciones, soporte y mantenimiento CPD.
Importantes	Servicios de soporte, mantenimiento, aplicaciones, licencias, seguridad y software de gestión.	Medio – su falla afecta áreas específicas, pero no detiene la operación global.	Mantenimiento de software, licencias antivirus, hosting web.
Complementarios	Proveedores de insumos, logística o consultoría no tecnológica.	Bajo – su interrupción puede diferirse o reemplazarse temporalmente.	Proveedores de papelería, transporte, consultoría administrativa.

Los proveedores críticos e importantes son monitoreados directamente por el Coordinador de TI y el Comité de Continuidad y Seguridad, quienes evalúan periódicamente su cumplimiento técnico y contractual.

Cláusulas de Continuidad y Seguridad en los Contratos

Los contratos con proveedores estratégicos deben incluir, como mínimo, las siguientes cláusulas específicas de continuidad y seguridad:

1. Disponibilidad del servicio: garantizar niveles de disponibilidad (SLA) mínimos del 99.9% y establecer tiempos máximos de recuperación (RTO/RPO) acordes con los procesos críticos.
2. Continuidad operativa: obligación del proveedor de contar con su propio plan de continuidad o recuperación ante desastres (BCP/DRP) validado por EPC.
3. Notificación de incidentes: reporte inmediato de eventos que afecten la prestación del servicio o la seguridad de la información.
4. Confidencialidad y protección de datos: cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre tratamiento de datos personales.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

5. Soporte y mantenimiento: disponibilidad de personal técnico especializado para atención de emergencias y soporte remoto o presencial 24/7 cuando sea requerido.
6. Auditorías y supervisión: derecho de EPC a realizar auditorías o requerir informes técnicos de continuidad.
7. Cláusula de sustitución o respaldo: obligación de disponer de proveedores alternos o mecanismos de sustitución temporal en caso de contingencia grave.
8. Responsabilidad contractual: definición de penalizaciones o compensaciones por incumplimiento de niveles de servicio que afecten la continuidad operativa.

Proveedores Críticos Identificados

A partir del inventario de activos de información y los contratos vigentes, se identifican los siguientes proveedores críticos para la continuidad tecnológica y operativa de EPC:

Proveedor de Servicio /	Área Responsable	Tipo de Servicio Tecnológico /	Nivel de Impacto	Estrategia de Continuidad
Proveedor de Nube y DRaaS	TI	Almacenamiento y respaldo en nube, recuperación ante desastres	Alto	Replicación automática y respaldo fuera de sitio (off-site).
Proveedor de Internet y Comunicaciones	TI / Administrativa	Conectividad LAN/WAN y VPN institucional	Alto	Redundancia de enlaces y doble proveedor.
Proveedor de Licenciamiento	TI	Correo institucional, colaboración y almacenamiento	Alto	Alta disponibilidad y acceso remoto seguro.
Proveedor de Energía y Climatización CPD	Administrativa	Energía ininterrumpida y climatización redundante	Alto	Plantas eléctricas y UPS configuradas para

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

				autonomía extendida.
Proveedor de Seguridad Perimetral	TI	Firewall, IDS/IPS y monitoreo de red	Medio-Alto	Mantenimiento preventivo trimestral y soporte remoto certificado.
Proveedor de Hosting y Web Institucional	Comunicaciones / TI	Portal institucional y publicación de información pública	Medio	DRP configurado y respaldo diario de contenido.

Seguimiento y Evaluación del Desempeño de Proveedores

El Coordinador de TI, en conjunto con los responsables de proceso y el Comité de Continuidad y Seguridad, realiza seguimiento periódico a los proveedores mediante:

- Evaluaciones semestrales de desempeño según indicadores de cumplimiento técnico, tiempos de respuesta, soporte y calidad del servicio.
- Revisión de informes de continuidad, resultados de pruebas o simulacros y cumplimiento de los SLA.
- Registro de incidentes y reportes de falla, documentados en el sistema de tickets de la Mesa de Ayuda (MDA).
- Reuniones de revisión contractual para ajustar cláusulas o actualizar mecanismos de respaldo y recuperación.

Los resultados de cada evaluación se documentan en el Informe de Desempeño de Proveedores Críticos, el cual se integra como evidencia en las revisiones del PCN y el PESI, asegurando la trazabilidad contractual y técnica dentro del SIG.

Estrategia de Sustitución o Transferencia de Riesgo

Cuando un proveedor crítico no pueda garantizar la continuidad del servicio dentro de los tiempos establecidos, EPC aplicará medidas de sustitución o transferencia de riesgo, tales como:

- Contratación de proveedor alternativo de emergencia.
- Activación de respaldo en la nube o infraestructura propia.
- Uso de pólizas o seguros de continuidad tecnológica (cyber insurance).
- Suspensión temporal del contrato y activación de cláusulas de contingencia.

Estas medidas se aplican bajo supervisión del Comité de Continuidad y Seguridad y del Área Jurídica, garantizando la protección de los intereses institucionales y la continuidad de los servicios críticos.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

La gestión integral de proveedores y servicios externos críticos fortalece la capacidad de EPC para prevenir interrupciones, reducir la dependencia tecnológica directa y asegurar la estabilidad operativa, consolidando relaciones contractuales basadas en la confianza, la transparencia y el cumplimiento de los estándares internacionales en materia de continuidad y seguridad digital.

Plan de Restablecimiento de Operaciones Prioritarias

El Plan de Restablecimiento de Operaciones Prioritarias define los procedimientos, fases, recursos y criterios necesarios para recuperar de manera ordenada, segura y controlada los servicios institucionales y tecnológicos que resulten afectados por un evento disruptivo.

Su propósito es garantizar que los procesos críticos retomen su funcionalidad dentro de los tiempos definidos en los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) establecidos en el Análisis de Impacto al Negocio (BIA), minimizando los impactos sobre la operación institucional, la información y los usuarios.

Objetivos del Plan de Restablecimiento

- Restablecer de forma prioritaria los servicios tecnológicos, operativos y de comunicación esenciales.
- Asegurar la integridad y disponibilidad de los datos institucionales tras el incidente.
- Minimizar el tiempo de interrupción de los procesos misionales y estratégicos.
- Implementar mecanismos seguros de validación y verificación antes del retorno total a la normalidad.
- Documentar cada fase del restablecimiento, garantizando trazabilidad y cumplimiento normativo.

Fases del Restablecimiento de Operaciones

El proceso de restablecimiento se estructura en cuatro fases secuenciales, cada una con actividades, responsables y resultados definidos:

Fase 1: Evaluación y Validación del Entorno Afectado

- Evaluar el estado de los sistemas, infraestructura, redes y aplicaciones comprometidas.
- Identificar la causa raíz del incidente y confirmar que se haya contenido la amenaza.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Validar la integridad física y lógica de los activos de información.
- Determinar el alcance de la recuperación y los servicios afectados.
- Elaborar un informe inicial de impacto técnico-operativo.

Responsables: Mesa de Ayuda (MDA) – Coordinador de TI.

Resultados: Diagnóstico validado, alcance definido y autorización del Comité de Continuidad y Seguridad para iniciar recuperación.

Fase 2: Activación de Procedimientos de Recuperación

- Implementar los procedimientos de restauración establecidos en el DRP y el PESI.
- Restaurar los sistemas a partir de copias de seguridad validadas (locales o en nube).
- Recuperar la infraestructura tecnológica crítica (servidores, bases de datos, redes, energía).
- Priorizar los servicios según el nivel de criticidad del proceso afectado.
- Coordinar con los proveedores estratégicos (DRaaS, telecomunicaciones, nube).

Responsables: MDA – Coordinador de TI – Proveedores de soporte.

Resultados: Servicios y sistemas críticos restaurados en ambiente controlado, con validación inicial de disponibilidad y conectividad.

Fase 3: Validación de Integridad y Funcionalidad

- Verificar la integridad de la información restaurada (checksum, logs, auditorías).
- Comprobar el correcto funcionamiento de las aplicaciones, autenticaciones y conexiones.
- Validar los RTO/RPO alcanzados frente a los definidos en el BIA.
- Aplicar controles de seguridad reforzada (antivirus, SIEM, monitoreo, aislamiento temporal).
- Autorizar la reincorporación gradual de los usuarios y procesos a los sistemas restaurados.

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

Resultados: Servicios operativos validados y listos para el restablecimiento gradual de usuarios.

Fase 4: Retorno Controlado a la Operación Normal

- Reintegrar los servicios tecnológicos y procesos operativos a su entorno habitual.
- Monitorear el comportamiento de los sistemas y el desempeño de los servicios por un periodo mínimo de 72 horas.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Registrar los tiempos de recuperación reales y las incidencias residuales.
- Elaborar el Informe de Restablecimiento y Cierre de Contingencia.
- Presentar el informe al Comité de Continuidad y Seguridad y a la Alta Dirección para su validación y cierre.

Responsables: Coordinador de TI – Comité de Continuidad y Seguridad – Oficina de Control Interno.

Resultados: Operación normal validada, documentación consolidada y cierre formal del evento.

Priorización de Servicios y Sistemas Críticos

Los servicios tecnológicos se restaurarán en el siguiente orden de prioridad, conforme al impacto operativo definido en el BIA:

Prioridad	Servicio / Sistema Crítico	Área Responsable	RTO (Horas)	RPO (Horas)
1	Sistema SIG Planeación	Planeación / TI	6	2
2	Sistema de Gestión de Proyectos (SIA)	Planeación / TI	8	4
3	Sistema Comercial y Atención al Usuario	Misional / TI	8	4
4	Correo Institucional y Microsoft 365	TI	12	6
5	Sistema de Gestión Documental	Archivo / TI	24	6
6	Portal Web Institucional	Comunicaciones / TI	24	8
7	Herramientas de Monitoreo y Seguridad	TI	4	2

Validación Técnica Post-Restauración

Una vez restablecidos los servicios, se debe ejecutar una validación técnica post-evento, que incluya:

- Pruebas funcionales completas del sistema y aplicaciones.
- Validación de conectividad y desempeño.
- Revisión de logs de auditoría y trazabilidad.
- Confirmación de replicación y respaldo posterior al restablecimiento.
- Documentación de resultados en el Informe Técnico de Recuperación.

Documentación y Evidencias del Proceso

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Toda la información generada durante el restablecimiento deberá documentarse y almacenarse en el SIG Planeación o en el Sistema de Gestión Documental, incluyendo:

- Registro del evento y nivel de severidad.
- Cronología de acciones ejecutadas.
- Recursos humanos y técnicos involucrados.
- Reportes de los proveedores y contratistas.
- Resultados de pruebas, validaciones y auditorías.
- Lecciones aprendidas y recomendaciones de mejora.

Evaluación Post-Evento

Una vez completado el restablecimiento, el Comité de Continuidad y Seguridad debe realizar una revisión post-evento para analizar:

- Cumplimiento de los tiempos RTO y RPO.
- Efectividad de las estrategias aplicadas.
- Brechas identificadas en recursos o procedimientos.
- Acciones correctivas o preventivas a implementar.
- Actualización del PCN y los documentos complementarios (PESI, DRP, BIA, GTI-F457).

El Plan de Restablecimiento de Operaciones Prioritarias garantiza que EPC pueda reanudar sus funciones esenciales de forma estructurada, segura y auditable, reduciendo los tiempos de inactividad y asegurando la protección de la información y los recursos tecnológicos institucionales.

Procedimientos de Retorno a la Normalidad

Los Procedimientos de Retorno a la Normalidad tienen como objetivo asegurar una transición ordenada y controlada desde el estado de contingencia hacia la operación normal institucional, garantizando que los sistemas, procesos y servicios restaurados operen de forma segura, estable y conforme a las condiciones previas al evento. Esta etapa representa la fase final del ciclo de continuidad, y su éxito depende de la validación técnica, la revisión funcional de los procesos, la confirmación de la integridad de la información y la documentación completa de las actividades ejecutadas durante la contingencia.

Objetivos Específicos

- Confirmar que todos los sistemas y servicios críticos han sido recuperados y funcionan con normalidad.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Validar que no existan riesgos residuales ni vulnerabilidades activas posteriores al restablecimiento.
- Garantizar la reintegración progresiva de los procesos y usuarios a la operación habitual.
- Documentar los resultados del restablecimiento y las lecciones aprendidas.
- Actualizar los planes, procedimientos y controles a partir de la experiencia del evento.

Criterios de Retorno a la Normalidad

El retorno a la normalidad podrá declararse únicamente cuando se cumplan los siguientes criterios técnicos y administrativos:

1. Todos los sistemas y servicios críticos se encuentran restaurados y validados conforme a los RTO y RPO definidos.
2. No existen alertas activas ni incidentes asociados en los sistemas de monitoreo o seguridad (SIEM, antivirus, IDS/IPS).
3. La integridad y disponibilidad de los datos restaurados ha sido verificada mediante pruebas de validación cruzada.
4. Los usuarios funcionales y líderes de proceso confirman la correcta operación de sus aplicaciones y servicios.
5. El Comité de Continuidad y Seguridad aprueba formalmente el cierre técnico del evento y autoriza la transición operativa.
6. Se ha generado el Informe de Restablecimiento y Cierre de Contingencia, con el detalle de acciones, resultados y responsables.

Fases del Retorno a la Normalidad

El proceso de retorno se estructura en tres fases principales:

Fase 1: Validación Operativa

- Realizar pruebas funcionales finales de los sistemas críticos.
- Confirmar la conectividad, el rendimiento y la interoperabilidad entre plataformas.
- Validar la sincronización de datos entre entornos de producción y respaldo.
- Verificar la actualización y consistencia de los registros operativos y contables.
- Garantizar que los usuarios autorizados puedan acceder normalmente a los servicios.

Responsables: Mesa de Ayuda (MDA), Coordinador de TI, Líderes de Proceso.
Resultado: Informe técnico de validación operativa con evidencias de funcionamiento estable.

Fase 2: Reincorporación Progresiva de Procesos y Personal

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Comunicar oficialmente el restablecimiento de servicios a toda la entidad.
- Reincorporar los procesos institucionales en orden de prioridad, iniciando por los misionales.
- Habilitar gradualmente el acceso de usuarios, validando el desempeño y carga del sistema.
- Restaurar el esquema de control de accesos, roles y privilegios según la operación normal.
- Supervisar durante al menos 72 horas el comportamiento del entorno operativo.

Responsables: Coordinador de TI, Comité de Continuidad y Seguridad, Área de Comunicaciones.

Resultado: Reintegración completa del personal y reanudación normal de las operaciones.

Fase 3: Cierre Técnico y Administrativo

- Elaborar el Informe Final de Restablecimiento y Retorno a la Normalidad, consolidando:
 - Descripción del evento.
 - Tiempos reales de recuperación (RTO/RPO alcanzados).
 - Controles aplicados.
 - Recursos utilizados.
 - Lecciones aprendidas y recomendaciones.
- Validar el informe ante el Comité de Continuidad y Seguridad.
- Registrar el evento cerrado en el SIG Planeación y en el Sistema de Gestión Documental.
- Programar auditorías internas o revisiones técnicas si se identificaron desviaciones.

Responsables: Coordinador de TI, Comité de Continuidad y Seguridad, Oficina de Control Interno.

Resultado: Evento cerrado formalmente y actualizado en el historial del PCN.

Comunicación del Cierre de la Contingencia

La comunicación oficial del retorno a la normalidad debe ser aprobada por el Comité de Continuidad y Seguridad y emitida por el Área de Comunicaciones Institucionales, asegurando que todos los grupos de interés conozcan el estado final del evento.

El comunicado debe incluir:

- Descripción breve del incidente.
- Fecha y hora del restablecimiento total.
- Medidas implementadas y controles aplicados.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Confirmación de normalidad operativa.
- Agradecimiento a las áreas y usuarios por la colaboración durante la contingencia.

La comunicación se difundirá a través de los canales oficiales (correo institucional, intranet, portal web y redes sociales, según el caso).

Lecciones Aprendidas y Mejora Continua

Una vez completado el retorno, el Comité de Continuidad y Seguridad debe liderar una sesión de revisión post-evento (Post-Incident Review) con los equipos técnicos y líderes de proceso, con el fin de:

- Analizar las causas raíz del evento y su gestión.
- Identificar fortalezas, oportunidades de mejora y deficiencias detectadas.
- Actualizar los procedimientos del PCN y DRP.
- Incorporar las lecciones aprendidas al ciclo de mejora continua del SIG.
- Reforzar las acciones de capacitación y simulacros en base a los hallazgos.

Actualización del Plan y Reentrenamiento

Todo evento real de activación del PCN debe generar una revisión inmediata del plan, especialmente en los apartados de:

- BIA (Análisis de Impacto al Negocio).
- Matriz GTI-F457 de Riesgos de Seguridad de la Información.
- Procedimientos de recuperación y comunicación.
- Listado de contactos y proveedores críticos.
- Roles y responsabilidades actualizadas.

Además, se deberá reentrenar al personal clave involucrado en la respuesta y recuperación, con base en las nuevas condiciones tecnológicas o de riesgo identificadas.

El retorno a la normalidad no constituye únicamente el fin de una contingencia, sino el inicio de un nuevo ciclo de aprendizaje y fortalecimiento del sistema de continuidad institucional.

Con esta etapa, EPC reafirma su compromiso con la resiliencia digital, la eficiencia operativa y la mejora continua de sus capacidades de respuesta ante incidentes, consolidando la confianza ciudadana y el cumplimiento de su misión institucional.

Mecanismos de Monitoreo y Seguimiento del PCN

El monitoreo, la evaluación y el seguimiento del Plan de Continuidad del Negocio constituyen un componente esencial del ciclo de mejora continua, estos mecanismos

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

permiten garantizar que las estrategias, procedimientos y controles establecidos sean eficaces, se mantengan actualizados y respondan a las condiciones reales de operación y riesgo de la entidad.

El seguimiento permanente contribuye a fortalecer la resiliencia operativa, la trazabilidad de la información y el cumplimiento normativo, asegurando la sostenibilidad tecnológica e institucional de EPC.

Objetivos del Monitoreo y Seguimiento

- Evaluar la eficacia de las estrategias de continuidad y los tiempos de recuperación alcanzados (RTO/RPO).
- Verificar el cumplimiento de los controles técnicos, administrativos y de seguridad definidos en el PCN.
- Detectar desviaciones, incidentes o deficiencias en la ejecución del plan.
- Garantizar la trazabilidad documental y la transparencia de los resultados.
- Generar información para la toma de decisiones y la mejora continua del sistema.

Estructura de Monitoreo

El monitoreo del PCN se realiza a través de tres niveles de control complementarios:

Nivel	Responsable	Alcance	Frecuencia
Operativo	Coordinador de TI / Mesa de Ayuda (MDA)	Supervisión técnica continua de sistemas, respaldos, incidentes y servicios críticos.	Diario / Semanal
Táctico	Comité de Continuidad y Seguridad	Evaluación de resultados de pruebas, simulacros y eventos reales.	Trimestral
Estratégico	Alta Dirección / Control Interno	Revisión de desempeño general del PCN, auditorías y cumplimiento del SIG.	Semestral / Anual

Indicadores de Desempeño del PCN

Para medir la eficacia y madurez del sistema de continuidad, se establecen indicadores cuantitativos y cualitativos que permiten evaluar los resultados del plan.

Código	Indicador	Descripción	Fórmula Unidad Medida	/ de	Meta Frecuencia
--------	-----------	-------------	-----------------------------	---------	--------------------

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

PCN-01	Cumplimiento de los RTO definidos	Mide el porcentaje de servicios que se recuperaron dentro del tiempo objetivo.	(Servicios recuperados dentro del RTO / Total de servicios críticos) × 100	≥ 95% / Trimestral
PCN-02	Eficacia de respaldos verificados	Evalúa la integridad y restaurabilidad de las copias de seguridad.	(Backups validados / Backups ejecutados) × 100	100% / Mensual
PCN-03	Cumplimiento de simulacros anuales	Mide la ejecución de pruebas y simulacros de continuidad.	(Simulacros ejecutados / Simulacros programados) × 100	100% / Anual
PCN-04	Incidentes críticos con impacto en continuidad	Registra el número de eventos que interrumpieron servicios esenciales.	Conteo / Periodo	≤ 2 / Semestral
PCN-05	Cumplimiento de actualizaciones del PCN	Mide la frecuencia y oportunidad en la revisión y actualización del plan.	(Revisiones ejecutadas / Revisiones planificadas) × 100	100% / Anual
PCN-06	Satisfacción de usuarios tras contingencias	Evalúa la percepción de las áreas afectadas sobre la gestión del evento.	(Respuestas positivas / Total encuestas) × 100	≥ 85% / Post-evento

Instrumentos de Seguimiento

Para garantizar la trazabilidad de la información y la disponibilidad de evidencias, se emplean los siguientes instrumentos de monitoreo:

- Registro de Monitoreo Continuo de Servicios: herramienta de seguimiento a disponibilidad, rendimiento y seguridad de los sistemas críticos.
- Bitácora de Eventos y Activaciones del PCN: documento que consolida todos los incidentes, pruebas y activaciones reales.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Formato de Evaluación Post-Evento: plantilla para analizar la efectividad de la respuesta y los tiempos de recuperación.
- Informe Trimestral de Continuidad: reporte técnico que consolida los indicadores, hallazgos y acciones de mejora.
- Matriz de Seguimiento a Planes de Mejora: registro formal de las acciones correctivas y preventivas derivadas de auditorías o simulacros.

Auditoría y Revisión Interna del PCN

El PCN debe someterse a procesos de auditoría interna y revisión por la dirección, conforme a las políticas del SIG y los requisitos de la norma ISO 22301.

Durante estas auditorías se verificará:

- Cumplimiento de los procedimientos establecidos.
- Evidencia documental de simulacros, pruebas y eventos reales.
- Eficacia de los controles implementados.
- Cumplimiento de los acuerdos de nivel de servicio (SLA/OLA).
- Alineación con las políticas de seguridad de la información y protección de datos.
- Conformidad con los resultados de las evaluaciones de riesgos y el BIA.

Los hallazgos, observaciones o recomendaciones derivadas de las auditorías deben documentarse en el Plan de Mejoramiento del PCN, asignando responsables, plazos y evidencias de cierre.

Integración con el Sistema Integrado de Gestión (SIG)

El proceso de monitoreo y seguimiento del PCN se articula directamente con el SIG Planeación, garantizando la gestión documental, la trazabilidad y el cumplimiento de los compromisos institucionales.

Esta integración permite:

- Registrar incidentes y activaciones en el módulo de gestión de riesgos.
- Asociar indicadores de desempeño al tablero de control institucional.
- Incorporar las acciones de mejora en el Plan de Mejoramiento Institucional (PMI).
- Facilitar la revisión por la Alta Dirección durante los comités estratégicos.

Reporte y Comunicación de Resultados

El Coordinador de TI consolidará los resultados de monitoreo y seguimiento en un Informe de Desempeño del PCN, el cual incluirá:

- Resumen ejecutivo del periodo.
- Cumplimiento de indicadores.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Hallazgos y desviaciones identificadas.
- Acciones correctivas y preventivas aplicadas.
- Plan de trabajo siguiente.

Este informe será presentado al Comité de Continuidad y Seguridad, que evaluará los resultados y aprobará las acciones de mejora, comunicándolas a la Alta Dirección y a las áreas correspondientes.

Mejora Continua del Sistema

Los resultados del monitoreo, las auditorías y los ejercicios de simulación alimentan el ciclo de mejora continua del PCN, garantizando que el plan evolucione conforme a los cambios tecnológicos, normativos o institucionales.

Las actualizaciones deben incluir:

- Revisión de riesgos y nuevos escenarios de amenaza.
- Ajuste de estrategias y procedimientos de respuesta.
- Inclusión de tecnologías emergentes (IA, ciberdefensa, automatización de recuperación).
- Retroalimentación del personal participante en eventos o simulacros.

El Coordinador de TI y el Comité de Continuidad y Seguridad son los responsables de asegurar la implementación y seguimiento de estas mejoras, con evidencia documentada en el SIG.

Con estos mecanismos de monitoreo, evaluación y seguimiento, EPC consolida un modelo de continuidad proactivo, auditable y sostenible, garantizando la efectividad del sistema frente a eventos reales y fortaleciendo la capacidad institucional para anticipar, responder y recuperarse de manera eficiente ante cualquier contingencia.

Programa de Pruebas, Simulacros y Ejercicios de Continuidad

El Programa de Pruebas, Simulacros y Ejercicios de Continuidad constituye un componente esencial para validar la eficacia del PCN, garantizar la preparación del personal y verificar la operatividad de los procedimientos, recursos y controles definidos en el plan, estos ejercicios permiten detectar fallas, debilidades o brechas en los tiempos de respuesta, y sirven como insumo para fortalecer la resiliencia operativa y tecnológica de EPC.

El programa se estructura bajo un enfoque planificado, progresivo y medible, que cubre desde pruebas técnicas específicas hasta ejercicios integrales de simulación institucional, asegurando la mejora continua del sistema.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Objetivos del Programa

- Verificar la efectividad de las estrategias y procedimientos del PCN en escenarios simulados o reales.
- Evaluar la capacidad de respuesta y coordinación del personal técnico y operativo.
- Comprobar la disponibilidad y funcionalidad de los sistemas, respaldos y comunicaciones.
- Identificar oportunidades de mejora en los controles, tiempos de recuperación y procesos de decisión.
- Fortalecer la cultura organizacional de continuidad y respuesta ante emergencias.

Tipos de Pruebas y Simulacros

El programa contempla diferentes tipos de ejercicios, clasificados según su alcance y complejidad:

Tipo de Prueba / Simulacro	Descripción	Objetivo Principal	Frecuencia Recomendada
Pruebas Técnicas de Recuperación (DRP Test)	Validan la restauración de sistemas, copias de seguridad y recuperación de datos en ambientes controlados.	Asegurar la disponibilidad y confiabilidad de los sistemas críticos.	Trimestral
Pruebas Parciales de Continuidad (Functional Test)	Evalúan procedimientos específicos de procesos o áreas críticas.	Comprobar la ejecución técnica y funcional de un componente del PCN.	Semestral
Simulacros Integrales (Full Simulation)	Simulan una interrupción total para evaluar el tiempo real de respuesta y recuperación.	Validar la coordinación global entre áreas, proveedores y Alta Dirección.	Anual
Pruebas de Comunicación	Validan la efectividad de los canales y tiempos de respuesta de notificaciones internas y externas.	Garantizar la trazabilidad y oportunidad en la comunicación.	Trimestral

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Ejercicios de Mesa (Tabletop)	Simulaciones teóricas en reuniones donde se analizan escenarios hipotéticos.	Revisar la toma de decisiones y roles en un ambiente no operativo.	Semestral
--------------------------------------	--	--	-----------

Planeación del Programa

El Coordinador de TI, en conjunto con el Comité de Continuidad y Seguridad, será responsable de la planeación y ejecución del programa anual de pruebas y simulacros, el cual deberá contemplar:

1. Objetivo del ejercicio (qué se desea validar).
2. Alcance y escenarios de prueba (procesos, sistemas o servicios involucrados).
3. Recursos requeridos (tecnológicos, humanos y logísticos).
4. Cronograma de ejecución (fechas, duración y responsables).
5. Criterios de éxito (tiempos de recuperación, disponibilidad y desempeño).
6. Mecanismos de evaluación (formularios, listas de chequeo, reportes técnicos).
7. Plan de comunicación y documentación (avisos, registro de resultados y evidencias).

La planeación debe integrarse con el Programa Anual de Gestión de Riesgos y Seguridad de la Información, asegurando la coherencia entre el PCN, el PESI y los procesos del SIG.

Ejecución de Pruebas y Simulacros

Durante la ejecución de los ejercicios, se deben cumplir los siguientes lineamientos:

- Realizar pruebas controladas en entornos seguros, minimizando el impacto sobre la operación real.
- Contar con la supervisión del Coordinador de TI y el acompañamiento de Control Interno como observador.
- Registrar las incidencias, hallazgos y desviaciones detectadas.
- Evaluar los resultados mediante indicadores (RTO, RPO, tiempo de respuesta, nivel de coordinación).
- Elaborar un Informe Técnico de Resultados al cierre de cada ejercicio.

21.5 Evaluación y Resultados

Los resultados de cada prueba o simulacro se analizarán con base en los siguientes criterios:

Criterio	Descripción
Eficacia Técnica	Capacidad de los sistemas para recuperarse dentro del RTO y RPO definidos.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Eficiencia Operativa		Rapidez y coordinación del personal en la ejecución de tareas.
Cumplimiento de Procedimientos	de	Grado de adherencia a los protocolos definidos en el PCN.
Comunicación y Coordinación	y	Fluidez y trazabilidad en la comunicación interna y externa.
Documentación y Evidencias	y	Calidad y completitud de los registros y reportes generados.

Cada simulacro deberá finalizar con un Informe de Evaluación de Continuidad, que incluirá:

- Escenario probado.
- Resultados y métricas alcanzadas.
- No conformidades o fallas detectadas.
- Acciones de mejora y responsables.
- Recomendaciones técnicas y administrativas.

Registro, Documentación y Mejora Continua

Toda la información generada durante los ejercicios de continuidad debe registrarse en el SIG Planeación o en el Sistema de Gestión Documental Institucional, conforme a los procedimientos del Sistema Integrado de Gestión.

Los principales registros son:

- Plan de Ejecución de Simulacros y Pruebas.
- Listas de asistencia y roles de participación.
- Reportes técnicos de desempeño.
- Registro de hallazgos, tiempos reales y evidencias fotográficas.
- Actas de evaluación y planes de mejora derivados.

El Comité de Continuidad y Seguridad consolidará los resultados en el Informe Anual de Pruebas y Simulacros, el cual será presentado ante la Alta Dirección y utilizado como insumo para actualizar el PCN, el DRP y los planes de tratamiento de riesgos.

Mejora del Programa

A partir de los resultados obtenidos, el programa deberá ajustarse anualmente para:

- Incluir nuevos escenarios de riesgo o cambios tecnológicos.
- Incorporar mejoras detectadas en ejercicios anteriores.
- Reentrenar al personal clave con base en hallazgos o deficiencias.
- Optimizar los procedimientos y controles técnicos.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

El éxito del programa depende del compromiso institucional, la participación activa de todos los niveles organizacionales y la integración con los demás instrumentos de gestión de seguridad y continuidad.

Con la ejecución sistemática de pruebas, simulacros y ejercicios, EPC valida su capacidad real de respuesta y recuperación, fortaleciendo la confianza operativa y garantizando la protección de la información, la continuidad del servicio público y la sostenibilidad de su infraestructura tecnológica.

Capacitación, Sensibilización y Competencias del Personal

La capacitación y sensibilización del personal son pilares fundamentales para garantizar la efectividad del PCN, el éxito de las estrategias de continuidad depende en gran medida del conocimiento, compromiso y competencias de los funcionarios y contratistas responsables de ejecutar los procedimientos definidos en el plan.

EPC reconoce que la preparación continua del talento humano es esencial para fortalecer la resiliencia institucional y la respuesta coordinada ante incidentes, interrupciones o desastres tecnológicos, asegurando que cada colaborador conozca su rol, las responsabilidades asignadas y las acciones a ejecutar en situaciones de contingencia.

Objetivos del Programa de Capacitación

- Fortalecer las competencias técnicas, operativas y administrativas del personal en materia de continuidad, recuperación y seguridad de la información.
- Garantizar que los funcionarios conozcan los procedimientos, responsabilidades y canales de comunicación definidos en el PCN.
- Sensibilizar sobre la importancia de la prevención, la gestión del riesgo y la respuesta organizada ante emergencias.
- Promover una cultura institucional de resiliencia digital y gestión proactiva del riesgo.
- Cumplir con los requisitos de formación establecidos por las normas ISO 22301 e ISO 27001 en materia de capacitación y concienciación.

Estructura del Programa de Capacitación

El Programa de Capacitación y Sensibilización en Continuidad del Negocio se estructura en tres niveles, según el rol y nivel de responsabilidad dentro del PCN:

Nivel	Dirigido a	Objetivo de Formación	de	Modalidad / Frecuencia
-------	------------	-----------------------	----	------------------------

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Nivel 1 Estratégico	–	Alta Dirección y Comité de Continuidad y Seguridad	Fortalecer las competencias en toma de decisiones, gestión de crisis y liderazgo institucional.	Seminarios presenciales / Anual
Nivel 2 Operativo	–	Coordinador de TI, Mesa de Ayuda (MDA), Líderes de Proceso	Desarrollar habilidades técnicas en ejecución de procedimientos, recuperación y comunicación durante incidentes.	Talleres prácticos y simulacros / Semestral
Nivel 3 General / Sensibilización	–	Todo el personal institucional	Promover la cultura de continuidad, la seguridad digital y la protección de la información.	Cursos virtuales, charlas o cápsulas informativas / Trimestral

Contenidos Temáticos del Programa

El programa contempla los siguientes módulos temáticos, ajustables anualmente según las necesidades institucionales y los resultados de las auditorías o simulacros:

1. Fundamentos del PCN y su integración con el SIG y el MSPI.
2. Gestión de riesgos y análisis de impacto al negocio (BIA).
3. Roles y responsabilidades durante la activación del PCN.
4. Uso de los canales de comunicación institucional durante contingencias.
5. Seguridad digital y buenas prácticas en el manejo de la información.
6. Recuperación de servicios y actuación ante incidentes tecnológicos.
7. Procedimientos de retorno a la normalidad y lecciones aprendidas.
8. Ejercicios prácticos de respuesta y simulación de escenarios reales.

Cada módulo incluirá sesiones teóricas, ejercicios de simulación y evaluaciones de desempeño, garantizando el aprendizaje activo y la aplicación práctica de los conocimientos.

Mecanismos de Sensibilización Institucional

Además de las capacitaciones técnicas, EPC desarrollará campañas de sensibilización y cultura de continuidad dirigidas a todo el personal, mediante:

- Boletines informativos sobre seguridad digital y continuidad operativa.
- Infografías y videos de orientación publicados en la intranet.
- Charlas institucionales y sesiones informativas periódicas.
- Simulacros de respuesta ante incidentes.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Reconocimiento a las buenas prácticas y participación destacada.

Estas estrategias buscan reforzar la conciencia institucional sobre la importancia de la preparación y la respuesta proactiva ante eventos que puedan afectar la operación.

Evaluación de Competencias

El Coordinador de TI, en conjunto con el Área de Talento Humano y el Comité de Continuidad y Seguridad, evaluará periódicamente las competencias y desempeño del personal involucrado en el PCN mediante:

- Evaluaciones teóricas y prácticas post-capacitación.
- Seguimiento del desempeño durante simulacros y ejercicios de continuidad.
- Retroalimentación individual y colectiva.
- Registro de cumplimiento en el SIG Planeación y en los expedientes de capacitación institucional.

Los resultados de estas evaluaciones se utilizarán para definir necesidades de formación adicionales y actualizar los planes de capacitación anuales.

Registro y Evidencia de Formación

Toda actividad de capacitación o sensibilización deberá quedar documentada en el SIG Planeación, incluyendo:

- Nombre del curso o evento.
- Fecha y modalidad de ejecución.
- Participantes y roles.
- Evaluaciones aplicadas y resultados obtenidos.
- Materiales utilizados.
- Certificados o constancias de participación.

El cumplimiento del programa será objeto de verificación por parte de la Oficina de Control Interno y reportado en las revisiones del Comité de Continuidad y Seguridad.

Mejora Continua del Programa de Capacitación

El programa de capacitación deberá revisarse anualmente, teniendo en cuenta:

- Los resultados de simulacros, auditorías o eventos reales.
- Cambios tecnológicos o normativos.
- Actualización de roles y estructura organizacional.
- Lecciones aprendidas y sugerencias del personal.

EPC se compromete a mantener un proceso de aprendizaje continuo, adaptativo y orientado a resultados, que garantice el fortalecimiento de las competencias institucionales en continuidad, seguridad y gestión del riesgo.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Con la implementación de este programa, EPC asegura la preparación integral de su personal, fomentando una cultura organizacional resiliente, consciente de los riesgos y capaz de responder eficazmente ante eventos que amenacen la continuidad del servicio público y la seguridad de la información.

Gestión de Cambios y Control de Versiones del Plan

La Gestión de Cambios y Control de Versiones garantiza que el Plan de Continuidad del Negocio (PCN) se mantenga actualizado, vigente y coherente con las condiciones tecnológicas, organizacionales y normativas de la entidad, este proceso busca asegurar que las modificaciones en la infraestructura, los sistemas de información, la estructura institucional o los riesgos identificados se reflejen oportunamente en el plan, preservando su integridad, trazabilidad y eficacia.

La actualización periódica del PCN es una práctica esencial de gobernanza que permite mantener la alineación con los objetivos estratégicos de EPC y con los lineamientos de seguridad, continuidad y resiliencia tecnológica definidos por el Estado colombiano.

Objetivos de la Gestión de Cambios

- Mantener el PCN actualizado frente a los cambios tecnológicos, normativos u organizativos.
- Garantizar que toda modificación sea documentada, evaluada y aprobada por las instancias competentes.
- Preservar la trazabilidad y la integridad del historial de versiones del plan.
- Asegurar la coherencia entre el PCN, el DRP, el PESI, el PETI y la Matriz de Riesgos de Seguridad de la Información.
- Cumplir con los lineamientos de control documental establecidos en el Sistema Integrado de Gestión (SIG).

Causales de Actualización del PCN

El plan deberá actualizarse cuando se presente alguna de las siguientes situaciones:

1. Cambios en la estructura organizacional o roles clave del Comité de Continuidad y Seguridad.
2. Modificación de procesos misionales, estratégicos o de apoyo.
3. Adquisición o reemplazo de sistemas de información, infraestructura tecnológica o servicios en nube.
4. Resultados de auditorías internas, simulacros o eventos reales que generen acciones de mejora.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

5. Cambios normativos, regulatorios o de política pública en materia de continuidad y seguridad digital.
6. Revisión o actualización de documentos asociados (PESI, DRP, BIA, GTI-F457).
7. Revisión programada anual conforme al cronograma del SIG.

Procedimiento de Gestión de Cambios

El proceso de gestión de cambios del PCN se compone de las siguientes etapas:

Etapas	Descripción	Responsable	Evidencia Generada
Identificación del Cambio	Detección de una modificación o necesidad de actualización en el PCN.	Coordinador de TI / Comité de Continuidad y Seguridad	Formato de Solicitud de Cambio PCN (SIG).
Evaluación del Impacto	Análisis técnico, operativo y documental del cambio propuesto.	Comité de Continuidad y Seguridad	Informe de Evaluación del Cambio.
Aprobación del Cambio	Validación formal del cambio por la Alta Dirección o Comité de Continuidad.	Alta Dirección / Comité	Acta de Aprobación.
Implementación y Actualización	Ejecución del cambio en el documento maestro del PCN.	Coordinador de TI	Versión actualizada del plan en el SIG.
Comunicación y Difusión	Socialización del cambio a las áreas involucradas.	Coordinador de TI / Comunicaciones	Circular o correo institucional.
Registro Documental	Archivo del historial de versiones y control documental.	Área de Planeación	Control de Versiones del PCN.

Revisión y Aprobación Periódica

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

El PCN será objeto de revisión y aprobación formal por parte del Comité de Continuidad y Seguridad al menos una vez al año o cada vez que se identifique un cambio sustancial.

El proceso incluirá:

- Revisión técnica de contenido.
- Verificación de vigencia de roles, contactos y proveedores.
- Validación de indicadores y resultados de pruebas o simulacros.
- Incorporación de acciones correctivas y preventivas derivadas de auditorías o eventos reales.

Una vez aprobado, el documento actualizado deberá publicarse en el repositorio documental del SIG Planeación y notificarse a todas las áreas involucradas mediante comunicación institucional.

Conservación y Trazabilidad Documental

Para garantizar la conservación y autenticidad del PCN, se aplicarán los lineamientos de la Política de Gestión Documental Institucional, asegurando que:

- Solo exista una versión vigente del documento.
- Las versiones anteriores se archiven con control de acceso restringido.
- Los cambios estén sustentados con evidencia formal (actas, informes, aprobaciones).
- Se mantenga un registro histórico que facilite la trazabilidad para auditorías internas y externas.

Responsabilidades en la Actualización

- Coordinador de TI: líder del proceso de actualización, responsable de gestionar, implementar y documentar los cambios.
- Comité de Continuidad y Seguridad: encargado de evaluar, validar y aprobar los cambios propuestos.
- Área de Planeación: responsable del control documental y la publicación de la versión vigente en el SIG.
- Oficina de Control Interno: realiza seguimiento al cumplimiento del procedimiento de actualización y control de versiones.
- Todas las Áreas: deben reportar oportunamente modificaciones en procesos, infraestructura o personal que puedan impactar la continuidad operativa.

Alineación con la Mejora Continua

La gestión de cambios y el control de versiones forman parte del ciclo PHVA (Planear, Hacer, Verificar, Actuar) del SIG, asegurando que el PCN evolucione conforme a la madurez institucional y tecnológica de EPC, los resultados de auditorías, simulacros

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

y evaluaciones de desempeño alimentan este ciclo, garantizando la actualización permanente y la mejora continua del sistema de continuidad.

Revisión, Actualización y Mejora Continua

La revisión, actualización y mejora continua del Plan de Continuidad del Negocio (PCN) garantizan su vigencia, efectividad y coherencia frente a los cambios tecnológicos, organizacionales y normativos que impactan a la entidad, este proceso asegura que el plan evolucione de manera dinámica, manteniendo su alineación con los objetivos estratégicos institucionales, el Plan Estratégico de Tecnologías de la Información (PETI), el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y la Matriz de Riesgos de Seguridad de la Información.

La mejora continua es un principio transversal de la gestión de continuidad que permite fortalecer la resiliencia institucional, optimizar los tiempos de recuperación y garantizar la sostenibilidad de los servicios esenciales ante cualquier eventualidad.

Objetivos de la Revisión y Mejora

- Asegurar que el PCN mantenga su pertinencia y aplicabilidad frente a los cambios del entorno operativo y tecnológico.
- Incorporar los resultados de auditorías, simulacros y eventos reales de activación.
- Ajustar las estrategias, procedimientos y roles con base en las lecciones aprendidas.
- Promover la cultura de mejora continua y aprendizaje organizacional.
- Mantener la conformidad con los requisitos de la norma ISO 22301 y las políticas de gobierno digital.

Enfoque Metodológico de Mejora Continua

El proceso de mejora del PCN se basa en el ciclo PHVA, utilizado en el SIG institucional y reconocido como estándar internacional de gestión:

Fase PHVA	Descripción Aplicada al PCN	Responsable Principal
Planear (P)	Identificación de riesgos, análisis de impacto (BIA), definición de estrategias de continuidad y actualización documental.	Coordinador de TI / Comité de Continuidad y Seguridad

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Hacer (H)	Implementación de las estrategias, ejecución de simulacros y aplicación de procedimientos de respuesta.	Mesa de Ayuda (MDA) / Líderes de Proceso
Verificar (V)	Monitoreo, auditoría y evaluación de resultados mediante indicadores y revisión por la dirección.	Control Interno / Alta Dirección
Actuar (A)	Aplicación de acciones correctivas, actualización del plan y reentrenamiento del personal.	Coordinador de TI / Comité de Continuidad

Revisión Periódica del PCN

El Comité de Continuidad y Seguridad realizará una revisión formal del PCN al menos una vez al año, o antes si ocurren cambios significativos en:

- Infraestructura tecnológica o arquitecturas críticas.
- Proveedores estratégicos o servicios tercerizados.
- Estructura organizacional o funciones de las áreas.
- Procesos misionales o de apoyo esenciales.
- Regulaciones y políticas nacionales de seguridad digital.
- Resultados de auditorías o simulacros institucionales.

La revisión incluirá:

- Análisis de efectividad de estrategias y procedimientos.
- Cumplimiento de RTO/RPO definidos.
- Validación de los indicadores de desempeño (PCN-01 a PCN-06).
- Evaluación de los mecanismos de comunicación y activación del plan.
- Verificación de la integración del PCN con el DRP, PESI y PETI.

Los resultados se documentarán en el Informe de Revisión Anual del PCN, firmado por el Coordinador de TI y avalado por la Alta Dirección.

Incorporación de Lecciones Aprendidas

Cada simulacro, auditoría o activación real del PCN debe generar un conjunto de lecciones aprendidas, las cuales serán registradas en el Repositorio de Continuidad del SIG Planeación.

Estas lecciones permitirán:

- Identificar oportunidades de mejora en procedimientos y tiempos de respuesta.
- Reforzar las competencias del personal clave.
- Optimizar los mecanismos de comunicación y coordinación institucional.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

- Actualizar controles técnicos y administrativos.
- Prevenir la repetición de incidentes o errores operativos.

El Coordinador de TI consolidará estas lecciones en un informe y presentará las acciones correctivas o preventivas al Comité de Continuidad y Seguridad para su validación y ejecución.

Actualización Documental y Control de Cambios

La actualización del PCN debe efectuarse siguiendo el procedimiento de Gestión de Cambios, garantizando que toda modificación:

- Sea documentada y aprobada antes de su implementación.
- Se publique en el repositorio oficial del SIG Planeación.
- Se comunique oportunamente a las áreas involucradas.
- Cuenten con respaldo y trazabilidad documental.

Las versiones obsoletas se conservarán con acceso restringido para fines de auditoría y consulta histórica, conforme a la Política de Gestión Documental institucional.

Evaluación de la Madurez del PCN

Para fortalecer la gobernanza del sistema, EPC implementará un modelo de madurez del PCN, que permitirá evaluar anualmente su nivel de avance con base en cinco dimensiones:

Nivel	Dimensión Evaluada	Descripción del Estado
1	Inicial	La entidad cuenta con un plan básico de continuidad, pero sin pruebas regulares ni revisión formal.
2	Gestionado	Existen procedimientos documentados, roles definidos y simulacros ocasionales.
3	Implementado	El PCN se encuentra activo, probado y alineado con los sistemas de gestión y riesgos.
4	Optimizado	Se ejecutan simulacros regulares, indicadores de desempeño y revisiones sistemáticas.
5	Maduro y Resiliente	La continuidad está integrada en la cultura organizacional, con mejora continua y respuesta automatizada.

El objetivo institucional es alcanzar y mantener un nivel 4 – Optimizado, garantizando un equilibrio entre robustez operativa, eficiencia de recursos y sostenibilidad tecnológica.

	Plan de Continuidad del Negocio (PCN)	Código: GTI-PI020
		Versión:0
		Fecha: 16/12/2025

Responsabilidades en la Mejora Continua

- Coordinador de TI: liderar la revisión, actualización y documentación del plan.
- Comité de Continuidad y Seguridad: evaluar la eficacia del PCN, aprobar mejoras y supervisar su implementación.
- Área de Planeación: custodiar la versión vigente y garantizar su integración al SIG.
- Alta Dirección: validar los resultados y asegurar la asignación de recursos para la mejora continua.
- Oficina de Control Interno: verificar el cumplimiento de los procesos de revisión, seguimiento y actualización.

Cierre del Ciclo de Mejora

La mejora continua culmina con la evaluación institucional del desempeño del PCN, donde se consolidan los resultados anuales de monitoreo, auditorías, simulacros y actualizaciones, estos resultados se presentan en el Informe Global de Continuidad del Negocio, que incluye:

- Resumen ejecutivo de actividades anuales.
- Cumplimiento de objetivos e indicadores.
- Hallazgos y acciones de mejora implementadas.
- Recomendaciones para el siguiente periodo.

El informe se entrega a la Alta Dirección, la Oficina de Control Interno y al Comité de Continuidad y Seguridad, garantizando la trazabilidad y el compromiso institucional con la sostenibilidad del sistema de continuidad.

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