1. Introducción

El Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM) presenta este Plan de Continuidad del Negocio, como parte de la gestión del riesgo, con el fin de mitigar la pérdida de capacidad operativa para responder a su misionalidad y responsabilidades legales ante un escenario o situaciones que alteren el normal funcionamiento institucional. En este documento se establecen los lineamientos para la gestión de continuidad en el Instituto, en articulación con el Sistema de Gestión Integrado (SGI)

2. Objetivos

2.1. Objetivo general

Establecer lineamientos para garantizar el cumplimiento de las actividades misionales y administrativas de la entidad, en el caso de presentarse una situación calificada como emergencia y que ponga en riesgo la seguridad de las personas, la información y/o cumplimiento de las obligaciones legales de la entidad.

2.2. Objetivos específicos

- Disminuir el impacto de la materialización de una situación de emergencia, buscando el cumplimiento de las actividades misionales de la entidad.
- Disminuir los tiempos de interrupción y mantener en niveles aceptables las actividades misionales, en caso ocurrencia de una emergencia, esto a través de la identificación de las actividades críticas, los recursos y los procedimientos necesarios.
- Generar una pronta recuperación de los servicios en caso de una emergencia.
- Dar la protección de las personas dentro de las instalaciones de la entidad en caso de que se materialice una emergencia.

3. Alcance

El Plan de Continuidad del Negocio (PCN) inicia con la identificación de escenarios de emergencia, la definición de actividades, responsables y recursos necesarios para atender la materialización de dichos escenarios, y culmina con la evaluación de la estrategia de recuperación y/o planes de emergencia y respuesta implementados. Para esta primera fase, se han priorizado las siguientes dependencias: (1) Grupo de Gestión Documental y Centro De Documentación, Correspondencia y Archivo, (2) Oficina del Servicio de Pronósticos y Alertas (OSPA), (3) Oficina Asesora de Planeación (OAP), (4) Grupo de Servicios Administrativos y (5) Oficina de Informática (TI).

La priorización de estas dependencias obedece a su impacto transversal en la operación institucional, su nivel de criticidad en la prestación de servicios esenciales, y su rol estratégico en la gestión de información y soporte técnico.

4. Definiciones

- **Acuerdo de Nivel de Servicio (ANS / SLA):** Compromiso formal entre el IDEAM y un proveedor o área interna, que establece los tiempos de respuesta, disponibilidad y niveles de servicio mínimos aceptables para garantizar la continuidad operativa.
- **Análisis de Impacto en el Negocio (BIA):** Proceso que identifica las actividades críticas de la entidad y evalúa las consecuencias operativas, legales, financieras y reputacionales ante la interrupción de cada una, determinando tiempos máximos de recuperación y recursos esenciales.
- **Análisis de Impacto al Negocio - Business Impact Analysis (BIA):** Metodología para evaluar el impacto temporal de la interrupción de funciones o procesos críticos de negocio, crucial para identificar qué procesos y sistemas que son vitales para el IDEAM y cómo una interrupción afectaría sus operaciones, ayudando a planificar la recuperación y continuidad del negocio (PCN).

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema en el IDEAM.
- **Plan de Continuidad del Negocio (PCN):** Conjunto de lineamientos, procedimientos y estrategias que permiten mantener la operación institucional en niveles aceptables frente a eventos disruptivos, garantizando el cumplimiento de la misionalidad del IDEAM.
- **Contingencia:** Situación inesperada que altera el funcionamiento normal de los procesos institucionales y que requiere activar medidas especiales de respuesta, operación alterna o recuperación.
- **Centro de Trabajo Alterno:** Lugar físico temporal que permite continuar con la operación de procesos críticos cuando las instalaciones principales se encuentran inhabilitadas o restringidas.
- **Equipo de Gestión de Crisis:** Grupo interdisciplinario responsable de la toma de decisiones estratégicas durante una contingencia, articulando acciones entre dependencias, gestionando la información y coordinando recursos institucionales
- **Evento Disruptivo:** Incidente, interno o externo, que afecta la continuidad de los servicios institucionales. Puede ser de origen natural, tecnológico, humano, sanitario o por fallas en proveedores.
- **Plan de Recuperación de Desastres - Disaster Recovery Plan (DRP):** Conjunto de actividades técnicas para restaurar infraestructura tecnológica, sistemas de información, bases de datos y servicios críticos de TI, conforme a los tiempos de recuperación definidos.
- **Recuperación y Restablecimiento:** Fase del PCN en la que se restituye la operación normal, se reactivan los sistemas afectados, se recupera la infraestructura o se reincorpora el personal, posterior a la mitigación del evento disruptivo.
- **Riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad, causando daño o desviación del resultado esperado. Combinación de las consecuencias de un evento y la probabilidad asociada de ocurrencia.

- **Trabajo Remoto o en Casa:** Modalidad de ejecución de actividades institucionales fuera de las instalaciones del IDEAM, activada cuando existen riesgos para el acceso o permanencia del personal en sedes físicas.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. Siglas

- **ANS:** Acuerdo de nivel de servicio, término para referirse al tiempo que se acuerda con el proveedor para responder ante un servicio.
- **BCP:** Las siglas en inglés, hacen referencia a Business Continuity Plan, en español plan de continuidad del negocio u operación.
- **BIA:** Las siglas en inglés, Business Impact Analysis, en español Análisis de Impacto en el Negocio.
- **DRP:** Las siglas en inglés, Disaster Recovery Plan, en español Plan de Recuperación de desastres.
- **IDEAM:** Instituto de Hidrología, Meteorología y Estudios Ambientales.
- **OAP:** Ofician Asesora de Planeación.
- **OSPA:** Oficina del Servicio de Pronósticos y Alertas.
- **SLA:** Service Level Agreement, término en inglés para referirse a un acuerdo de nivel de servicio.
- **SST:** Seguridad y salud en el trabajo.
- **TI:** Tecnología de la información.
- **VPN:** Sigla en inglés de virtual private network, Red privada virtual.

6. Marco normativo

El desarrollo del Plan de Contingencia y Continuidad de Negocio para el IDEAM se fundamenta en la necesidad de preservar la disponibilidad y continuidad de los servicios que presta la entidad articulada con el Modelo Integrado de Planeación y Gestión – MIPG, a través de la 3ª. Dimensión: Gestión con valores

para resultados. Así mismo, su contenido se estructura en consideración al siguiente marco legal:

- Ley 1253 de 2012 "Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones", en su Artículo 2°. De la responsabilidad. La gestión del riesgo es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano. En cumplimiento de esta responsabilidad, las entidades públicas, privadas y comunitarias desarrollarán y ejecutarán los procesos de gestión del riesgo, entiéndase: conocimiento del riesgo, reducción del riesgo y manejo de desastres, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres.
- Decreto 1078 de 2015, "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1955 de 2018, "por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", en su Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros.
- NTC/ISO 22301:2012 Norma internacional para la gestión de continuidad del negocio
- NTC 5722 Norma colombiana que especifica los mismos requisitos para un SGCN que la ISO 22301.

6.1. Lineamientos

El Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM, consciente de su responsabilidad misional frente al país y del impacto que pueden tener las interrupciones en sus procesos estratégicos, misionales y de apoyo, establece los siguientes Lineamientos de Continuidad del Negocio:

1. Compromiso institucional

El IDEAM se compromete a implementar, mantener y mejorar de manera continua un Plan de Gestión de Continuidad del Negocio alineado con la norma ISO 22301, la normativa nacional aplicable y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

2. Gestión de riesgos

La entidad identificará, evaluará y mitigará los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información, los servicios y la infraestructura crítica necesaria para cumplir sus funciones.

3. Protección de personas e infraestructura

Se garantizará la seguridad de los funcionarios y contratistas, así como la protección de los activos físicos, tecnológicos y ambientales en cualquier escenario de emergencia o desastre.

4. Planes de respuesta y recuperación

El IDEAM desarrollará, documentará y mantendrá planes específicos de respuesta, operación alterna y recuperación, que permitan reanudar en tiempos aceptables las operaciones críticas de la entidad y cumplir con las responsabilidades legales y misionales.

5. Pruebas y mejora continua

La oficina de informática designará un asesor interno o externo que realizará de manera periódica y de acuerdo con sus capacidades simulacros, pruebas y

ejercicios de validación de los planes de continuidad, documentando los resultados y aplicando las lecciones aprendidas para fortalecer la efectividad del sistema.

6. Responsabilidad compartida

La continuidad del negocio es responsabilidad de todas las dependencias y funcionarios del IDEAM, quienes deberán cumplir los lineamientos definidos en este plan, participar en su actualización y apoyar activamente en las actividades de pruebas y entrenamiento.

7. El trabajo remoto o en casa

El trabajo remoto o en casa, es cualquier actividad que se realice fuera de las instalaciones del IDEAM, puede ser con recursos propios del funcionario, contratista o tercero o con los recursos del Instituto, lo que se busca priorizar es la continuidad de la operación.

La estrategia de trabajo remoto o en casa se activa cuando no es posible acceder a las instalaciones del instituto o estás no son seguras para las personas, de acuerdo con el escenario identificado.

7. Roles y responsabilidades

A continuación, se presenta los roles y responsabilidades para la gestión de la continuidad del negocio:

Rol	Responsabilidad	Representantes	Mecanismos
Comité Institucional de Gestión y Desempeño	Aprueba el Plan de Continuidad de Negocio. Liderar y articular recursos y esfuerzos relacionados con el plan de continuidad de negocio.	Miembros del comité	Reuniones extraordinarias, actas y evidencias de las decisiones que se toman. Aplicar las guías y metodologías institucionales.

	Efectuar recomendaciones de acuerdo con el análisis de la información.		Metodología de riesgos. La aprobación es a través del plan, y la activación de rutas estará en la documentación de respuesta, que revisa o evalúa el equipo de crisis.
Líder de Continuidad del Negocio	Garantizar la comunicación entre dependencias necesarias para el PCN. Coordinar y hacer seguimiento a la implementación de los instrumentos de gestión de continuidad de negocio y articularlos a este instrumento estratégico y al SGI.	Oficina Asesora de Planeación	Activación de planes relacionados con el PCN
Equipo de Gestión de Crisis	Toma decisiones operativas durante la contingencia. Articulación con el Grupo de administración y desarrollo del talento humano en temas de seguridad y salud en el trabajo (SST). Evaluación del impacto de incidente	Dirección de General Oficina Asesora de Planeación. Oficina de Informática (TI). Oficina Asesora Jurídica. Grupo de Comunicaciones y Prensa. Grupo de Administración y Desarrollo del Talento Humano.	Activación de protocolos, reuniones de emergencia, coordinación con áreas técnicas. Activación de protocolos relacionados con SST

		Líderes de dependencias afectadas	
Equipo de Tecnología	Ejecuta el **SGI-PN006 Plan de recuperación de desastre** (DRP) tecnológicos Realiza respaldos, recuperación de sistemas y redes y restaura información con respaldo. Monitorea incidentes.	Oficina de Informática (TI)	Procedimientos técnicos, herramientas de monitoreo, ejecución de planes de recuperación.
Equipo de Gestión de las comunicaciones (Interna/Externa)	Define canales oficiales. Controla la emisión de mensajes y gestiona la proliferación de rumores o comunicación imprecisa Coordina la comunicación y vocería con Equipo de Gestión de Crisis.	Grupo de comunicaciones y prensa	Comunicados oficiales, gestión de medios, coordinación con voceros institucionales.
Lideres de proceso o jefes o directivos de área.	Identificación de riesgos, controles detectivos y correctivos. Asegurar la capacitación y conocimiento del plan de continuidad. Participación activa en simulacros y pruebas preventivas donde cada participante	Primera línea de defensa	Talleres, capacitaciones y sensibilizaciones. Simulacros y pruebas preventivas l. Gestión de riesgos.

	debe actuar de acuerdo con la responsabilidad real.		

8. Descripción metodológica

El Plan de Contingencia y Continuidad del Negocio busca coordinar acciones orientadas a mantener el funcionamiento aceptable de la misionalidad del IDEAM y de la prestación de sus servicios frente a situaciones declaradas de emergencia no permiten el normal funcionamiento de los procesos de la entidad durante un tiempo determino.

La gestión de continuidad se articula con la gestión de riesgos, documentada a través de la política y metodología de riesgos, así como en la matriz institucional de riesgos, que incluye los controles preventivos, detectivos y correctivos de acuerdo con el aseguramiento de la gestión institucional. A continuación, se identifican los escenarios de afectación de continuidad de negocio o de interrupción de operación que pueden afectar al Instituto, así como las acciones estratégicas de respuesta de las dependencias priorizadas en el alcance de este documento.

8.1. Identificación de escenarios de perdida de continuidad

Esta parte inicial, identifica los aspectos generales del plan, estos como: la identificación del riesgo de la no continuidad del negocio por proceso, el escenario en que puede incurrir y su descripción, las posibles causas de la perdida de continuidad, sus consecuencias, el responsable de generar la respuesta dentro del plan y la definición del equipo de trabajo para la ejecución del plan (quienes deben estar preparados en caso de presentarse un evento inesperado). Lo anterior en atención a los siguientes escenarios de interrupción o indisponibilidad:

Escenario de interrupción	Amenazas o factores de riesgo	Operación en contingencia	Líder de la gestión en continuidad
Ausencias de personal	Asonadas, cierre de vías de acceso Accidente, enfermedad o muerte, manifestaciones públicas, accidentes de tránsito	Cuadros de sucesión temporal, roles alternos o listas de reemplazo Trabajo remoto o en casa.	Secretario (a) General
Imposibilidad de uso o acceso a instalaciones	Pandemias o emergencias sanitarias decretadas, Desastres naturales Incendios Inundaciones Fugas de gas Ataques violentos o terroristas Adecuaciones y/o mantenimiento Daños a activos y bienes institucionales	Trabajo en casa con uso de herramientas colaborativas institucionales. Conexión a través de VPN segura Centro de Trabajo Alterno Privilegiar canales de atención diferentes al presencial. Activación de pólizas e instrumentos de aseguramiento.	Secretario (a) General
Indisponibilidad activos de TIC (Sistemas de información y bases de datos y canales)	Error humano, ataque cibernético, fallos tecnológicos, fallas eléctricas, Desastres naturales Inundaciones e incendios	Plan de Recuperación de Desastres Restauración de copias de seguridad	Jefe Oficina de Informática
Indisponibilidad de servicios gestionados con terceros (proveedores)	Error humano, ataque cibernético, fallos tecnológicos, fallas eléctricas, Desastres naturales Inundaciones e incendios	Acuerdos de Nivel de Servicio específicos para los Sistemas de Gestión de Continuidad de Negocio, de los proveedores.	Jefe Oficina de Informática

	Ataques terroristas, Pandemias o emergencias sanitarias	Restauración de copias de seguridad	

8.2. Detección

En esta fase se involucra la identificación de las alertas y su confirmación, generando acciones de preparación de las áreas para iniciar una contingencia y la articulación de la gestión institucional en los diferentes procesos de la entidad.

8.3. Activación

La activación del Plan de Continuidad del Negocio se realizará conforme al escenario identificado y será autorizado por el Líder del Continuidad del Negocio y Equipo de Gestión de Crisis, en cumplimiento de las funciones asignadas en el presente plan. El comité evaluará la situación, determinará el nivel de afectación, declarará la activación del plan y asignará las responsabilidades necesarias para la operativización de las contingencias y atención a emergencias.

El canal de comunicación del Equipo de Gestión de Crisis puede ser vía WhatsApp, Teams o correo electrónico de acuerdo con lo que sea más eficiente, en el canal de comunicaciones. En este canal solo deben estar los representantes del equipo de gestión de crisis, para una toma de decisiones oportuna de acuerdo con la necesidad. Las decisiones deben ser informadas al líder del Plan de Continuidad de Negocio, para establecer lecciones aprendidas que acciones se ejecutaron y cuales faltaron.

Responsabilidades del líder de continuidad:

- Evaluar el incidente y determinar si cumple con los criterios para activar el plan.
- Declarar formalmente la activación del Plan de Contingencia y Continuidad del Negocio.
- Asignar responsables y equipos operativos según el tipo de contingencia y procesos afectados.

- Coordinar la comunicación interna y externa conforme a los protocolos definidos.
- Autorizar la movilización de recursos, instalaciones alternas, respaldos y procedimientos alternativos.
- Supervisar la ejecución de las acciones iniciales para el control y mitigación del impacto.
- Hacer seguimiento continuo del incidente y decidir su escalamiento o desactivación.

Responsabilidades del equipo de gestión de crisis:

- Ejecutar las acciones asignadas por el Líder para la activación del plan.
- Implementar procedimientos alternativos en los procesos afectados.
- Apoyar la coordinación operativa en la movilización de recursos y uso de instalaciones alternas.
- Mantener comunicación constante con el Líder sobre el avance de las acciones y el estado del incidente.
- Documentar las actividades realizadas y los resultados obtenidos durante la contingencia.
- Participar en la evaluación del impacto y en la propuesta de medidas correctivas.

Una vez activado el plan, los líderes de procesos, bajo la coordinación del Comité realizarán las acciones operativas definidas en los procedimientos de contingencia, para garantizar la continuidad mínima del servicio hasta su restablecimiento total en la operación.

8.4. Plan de operación alterno

En esta fase, se definen las tareas que se ejecutarán para mantener la operación de los servicios institucionales en niveles aceptables (buscando disminuir los tiempos de interrupción) mientras exista la emergencia activa. Se activan los planes de operación alterna y las acciones al alcance de la entidad para resolver

las afectaciones que generó la situación de emergencia, dando como primera medida el trabajo remoto para las personas esenciales, para el personal que requiera trabajo en instalación física se evaluará cuál sede cuenta con la capacidad de operación para trasladarlos, redistribución temporal de funciones entre el personal disponible, activación de suplencias, priorización de servicios esenciales y suspensión temporal de actividades no críticas.

Dichos mecanismos de activación se producen cuando el líder del proceso o Líder de Continuidad del Negocio tienen conocimiento del evento o incidente que genera la interrupción del servicio,

Para la recuperación de los servicios a nivel tecnológico se debe tener en cuenta el documento **SGI-PN006 Plan de recuperación de desastre**, donde se describe el Proceso de Copias de Respaldo de Seguridad, para reestablecer la Tecnología de la Información.

8.5. Recuperación y restablecimiento - resolución del incidente

En este momento, se define todas las actividades necesarias para retomar las actividades en su estado normal de funcionamiento una vez se han superado las situaciones que generaron la emergencia, se han restablecido los sistemas y servicios afectados o se han reparado las estructuras afectadas.

8.6. Plan de comunicación externa

Con el fin de garantizar una comunicación clara, oportuna y segura durante la activación del Plan de Continuidad del Negocio (PCN), se establece que el único canal oficial de comunicación externa será el Grupo de Comunicaciones y Prensa de acuerdo con los procedimientos definidos y vocerías establecidas.
Para la comunicación interna el Equipo de Gestión de Crisis, será el responsable de articular y comunicar todos los protocolos definidos.

8.6.1. Acciones clave de la estrategia

- **Activación del canal oficial**: Toda comunicación externa relacionada con el PCN será gestionada exclusivamente por el Equipo de Gestión de las comunicaciones.
- **Definición de voceros institucionales**: Se establecen portavoces autorizados para emitir mensajes oficiales, en coordinación con el Equipo de Gestión de Crisis.
- **Uso de medios institucionales**: Se utilizarán únicamente los medios definidos por el Equipo de Gestión de las comunicaciones (correo institucional, intranet, boletines, comunicados oficiales, redes sociales institucionales).
- **Mensajes estructurados y validados**: Todo mensaje será previamente validado por el Equipo de Gestión de Crisis antes de su difusión.
- **Prevención de rumores**: Se implementarán mecanismos de monitoreo y respuesta rápida ante información no oficial o malinterpretada.
- **Actualización periódica**: Se garantizará la emisión de comunicados periódicos con el estado de la contingencia, medidas adoptadas y recomendaciones para el personal.
- **Coordinación con áreas técnicas**: el Equipo de Gestión de las Comunicaciones trabajará de forma articulada con la Oficina de Informática Oficina Asesora Jurídica, Grupo de administración y desarrollo del talento humano y demás áreas involucradas en el **PCN**.

8.6.2. Escenarios de aplicación

Esta estrategia se aplicará en todos los escenarios contemplados en el BCP, incluyendo:

- Desastres naturales.
- Manifestaciones, asonadas y/o estallidos sociales.
- Emergencias sanitarias.
- Fallas técnicas o tecnológicas.
- Interrupciones en servicios esenciales.

- Eventos de seguridad informática.
- Accidentes o daños físicos.
- Ausencia o indisponibilidad del personal.
- Mantenimiento locativo.
- Fallas en proveedores o terceros.
- Cualquier situación que afecte la prestación de los servicios de la entidad.

9. Construcción de plan de continuidad del negocio

9.1. Análisis del entorno institucional

A partir de las funciones y obligaciones normativas del IDEAM, los compromisos con los diferentes grupos de valor y partes interesadas, y los datos históricos de la operación institucional, se consolidan los factores que pueden afectar el desarrollo adecuado de las actividades, representadas así:

9.1.1. Factores del Contexto Externo que pueden afectar el funcionamiento del IDEAM

- **Políticos:** Cambios o decisiones de gobierno, legislación, políticas públicas y regulación (Cambios en la administración central y territorial que genera cambios en los planes).
- **Económicos y financieros:** Restricciones de orden económico que pueden afectar el funcionamiento de la entidad o la ejecución de los proyectos, Cambios en la asignación presupuestal de la entidad o para el proyecto por cambio de prioridades de la administración.
- **Sociales y culturales:** Demografía, responsabilidad social y orden público
- **Tecnológicos:** Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
- **Ambientales:** Emisiones y residuos, energía, catástrofes naturales y desarrollo sostenible. Cambio de las políticas que propendan por disminuir

la afectación ambiental a través de procesos de mitigación de impacto ambiental, Manejo de residuos y Contribución al desarrollo sostenible

- **Legales y Reglamentarios:** Normatividad externa (leyes, decretos). Nuevas disposiciones legales que afecten a la entidad (laborales, contratación, manejo de procesos misionales, sectoriales).

9.1.2. Factores del Contexto Interno que pueden afectar el funcionamiento del IDEAM

- **Personal y estructura de la entidad:** Competencia del personal, disponibilidad, seguridad y salud ocupacional.
- **Procesos:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- **Tecnología y seguridad de la información:** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- **Estratégicos:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
- **Comunicación interna y/o relación con partes interesadas:** Canales utilizados y su efectividad, flujo de la información adecuado.

9.1.3. Factores del Contexto del Proceso que pueden afectar el funcionamiento del IDEAM

- **Diseño del proceso:** claridad en la descripción del alcance y objetivo del proceso.
- **Interacciones con otros procesos:** relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- **Transversalidad:** procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- **Procedimientos asociados:** pertinencia en los procedimientos que desarrollan los procesos.

- **Responsables del proceso:** grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- **Comunicación entre los procesos:** efectividad en los flujos de información determinados en la interacción de los procesos.
- **Activos de Seguridad de la Información del proceso:** información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

10. Estrategia para las dependencias seleccionadas en el alcance

10.1. Estrategia para el Grupo de Gestión Documental y Centro de documentación, correspondencia y archivo ante un desastre o evento disruptivo

La estrategia para este grupo busca garantizar la preservación, disponibilidad, integridad y confidencialidad de la información institucional, tanto en formato físico como digital, asegurando su recuperación en caso de interrupciones operativas o desastres. Se articula con los lineamientos del Archivo General de la Nación (AGN) y se gestiona en coordinación con esta dependencia. Esta estrategia se activa cuando se vea una afectación a la preservación de la información o la operación de la dependencia.

10.1.1. Acciones estratégicas

- Almacenamiento externo seguro mediante discos duros externos institucionales (IDEAM) para respaldo de información crítica, la custodia de los discos duros es del Grupo de Gestión Documental.
- Como última medida de restablecimiento de información se solicita la información transferida al Archivo General de la Nación, con respaldo de los datos transferidos. El tiempo estimado de recuperación ha sido mínimo de seis meses.
- El Grupo de Gestión Documental reestablece los documentos según la Tabla de Retención Documental (TRD) y la Tabla de Valoración Documental

(TVD), clasificando la información por series y subseries para definir su disposición final.

- El restablecimiento debe realizarse según el tipo de información:
  - Información contable: 20 años.
  - Informes de gestión: 5 años (se conserva el consolidado anual).
  - Historias laborales: 80 años, custodiadas en el archivo central del IDEAM, compartido con Talento Humano.
  - Información misional: custodia en el Archivo Técnico del IDEAM.
- Cuando se realice el restablecimiento de la información se deben tener en cuenta los lineamientos y continuar con la gestión de Control físico de conservación mediante unidades de almacenamiento que cumplen con los criterios del AGN: cajas y carpetas desacidificadas, estantería industrial, sin elementos abrasivos.
- El Grupo de Gestión Documental debe solicitar a la Oficina Informática la copia de respaldo conforme al procedimiento 8.13 "Copia de seguridad de la información". Ver GTI-P007 Procedimiento Back Up en caso de pérdida de datos o información.
- Después del restablecimiento se debe continuar con el control digital documentado en el procedimiento “Manual para la gestión de documentos y expedientes electrónicos.pdf GD-M001”.
- Después del restablecimiento, se debe activar Inventario Único documental mediante el Formato Único de Inventario Documental (FUID) para el archivo técnico evaluando condiciones y afectaciones.
- Priorización del traslado de personal técnico clave a las instalaciones, según la criticidad de los servicios afectados y la necesidad de intervención física y la aplicación del instructivo para la prevención y atención de desastres en depósitos de archivos del IDEAM GD-I003.
- Levantar registro fotográfico del siniestro, la zona afectada, el material, condiciones de interna, como parte del informe de contingencia.

- Notificar a AGN a través de formulario de identificación de archivos ante situaciones de desastre, adjuntando registro e informe inicial de daños y afectaciones.
- Estabilizar entorno (levantamiento de escombros, motobombas, baldes, paños) y asegurar condiciones ambientales adecuadas (ventilación, deshumidificadores).
- Reubicación temporal de documentos mojados a lugar seco, aislados del área de desastre y ejecutar procedimiento de secado.
- Activación de gestión de radicación manual en caso de indisponibilidad del SGD Orfeo, llevar registro para que al momento de restablecimiento se pueda actualizar el repositorio respectivo.

10.1.2. Recursos críticos

- Sistema de información de gestión documental ORFEO.
- Infraestructura física: archivos técnico y centralizado.
- Espacio de almacenamiento en servidores institucionales.
- Acceso físico y lógico a la información histórica y actual.
- Recurso humano especializado en gestión documental.
- Insumos especializados: cajas, carpetas desacidificadas, papelería técnica.

10.1.3. Riesgos de interrupción

- Confidencialidad: riesgo en documentos sensibles como historias laborales, flora y fauna.
- Integridad: posibilidad de alteración o pérdida de información.
- Disponibilidad: riesgo de inaccesibilidad temporal o permanente de documentos físicos o digitales o a repositorios digitales o al gestor documental ORFEO.

10.1.4. Aplicaciones de estrategia en escenarios

- Desastres naturales: incendios, inundaciones, sismos que afecten archivos físicos.
- Fallas tecnológicas: pérdida de acceso a servidores, fallos en discos duros o sistemas de respaldo.
- Emergencias sanitarias: que impidan el acceso físico a los archivos.
- Interrupciones de servicios esenciales: energía, conectividad, climatización.
- Accidentes físicos: daños estructurales en las áreas de archivo.

10.1.5. Amenazas y vulnerabilidades de seguridad

- Robo, vandalismo, acceso no autorizado.
- Ausencia de personal clave: por enfermedad, huelga o rotación no planificada.
- Fallas en proveedores: retrasos o incumplimientos en servicios de digitalización, almacenamiento o mantenimiento documental.

10.2. Estrategia para la OSPA ante un desastre o evento disruptivo

Las estrategia y acciones frente a desastres ante eventos disruptivos que puedan afectar la operación de la OSPA, se implementarán las siguientes medidas:

10.2.1. Acciones estratégicas

- Activación de trabajo remoto o en casa mediante el uso de VPN segura para garantizar la transferencia de información y la continuidad de la operación.
- Priorización del traslado de funcionarios clave a las instalaciones de la entidad, según la criticidad de sus funciones.
- Provisión de transporte institucional para garantizar la seguridad sanitaria y la salud del personal durante desplazamientos en situaciones de emergencia.

- Reestablecer copias de respaldo, con acceso controlado, para asegurar la disponibilidad de la información crítica, de acuerdo con el BIA. O Activar centro de datos alterno para reestablecer servicios de alertas y avisos.
- Activar comunicación alterna con el SGRD a través de telefonía celular o radioteléfono.
- Activar plan de recuperación de proceso de acuerdo con el BIA por ser proceso crítico.
- Activar gestión de incidente para herramientas TIC del proceso.

10.2.2. Recursos críticos

- Equipos de cómputo, con los sistemas de información (Licencias para pronósticos, software libre para alertas de deslizamiento e incendios)
- Sistemas de información especializados (SMARTMET, RADIOSONDEOS, radares, modelos, etc.), se encuentra documentado en los Protocolos de la operación
- Hardware (Radiosondeos y radares, estaciones)
- Acceso a fuentes de información (Datos de estaciones, modelo, satélites, etc.)
- Recurso humano

10.2.3. Riesgos de interrupción

Existe riesgo de pérdida temporal de acceso a la información, indisponibilidad de sistemas de información y aplicaciones y afectación a la integridad de los datos. La operación podría continuar, aunque con tecnología limitada, lo que impactaría el nivel de certeza en los pronósticos meteorológicos, así como la oportunidad en la transmisión de datos asociados a la gestión de riesgos SNGRD.

10.2.4. Aplicaciones de estrategia en escenarios

- Desastres naturales: Terremotos, inundaciones, tormentas eléctricas, incendios forestales. Afectación directa a la infraestructura física o a los sistemas de información.

- Emergencias sanitarias o de salud pública como pandemias, brotes epidemiológicos, fumigaciones por vectores. Requieren aislamiento, trabajo remoto o en casa y medidas de bioseguridad.
- Fallas técnicas o tecnológicas, caídas de servidores, fallos en el hardware (radares, radiosondeos, estaciones).
- Pérdida temporal de acceso a sistemas críticos o a la información.
- Interrupciones en servicios esenciales como cortes de energía eléctrica, fallos en la conectividad de red, pérdida de acceso a internet.
- Requiere respaldo energético, acceso remoto y redundancia en la infraestructura.
- Eventos de seguridad informática como ciberataques, accesos no autorizados, pérdida de integridad de datos.
- Activación de protocolos de respaldo, recuperación y aislamiento de sistemas.
- Accidentes o daños físicos como incendios en las instalaciones, explosiones, daños por vandalismo.
- Requiere reubicación temporal del personal y activación de copias en la nube.
- Ausencia o indisponibilidad del personal como paros, huelgas, enfermedades, vacaciones no programadas.
- Activación de personal de respaldo, trabajo remoto o en casa y redistribución de funciones.
- Mantenimiento o adecuaciones locativas como remodelaciones, fumigaciones, reparaciones estructurales.
- Requiere trabajo remoto o en casa temporal y acceso remoto a sistemas.
- Fallas en proveedores o terceros como incumplimiento de SLA, fallas en servicios contratados (limpieza, soporte técnico).
- Activación de proveedores alternos o medidas internas de contingencia.

10.2.5. Amenazas y vulnerabilidades de seguridad

Dentro de las amenazas se identificó el daño físico, Eventos naturales, Pérdidas de los servicios esenciales, perturbación debida a la radiación, Fallas técnicas y Acciones no autorizadas,

Dentro de las vulnerabilidades se identificó el Mantenimiento insuficiente, Ausencia de esquemas de reemplazo periódico, Sensibilidad a la radiación electromagnética, Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad), Almacenamiento sin protección, Falta de cuidado en la disposición final, Copia no controlada, Ausencia del personal, Entrenamiento insuficiente, Falta de conciencia en seguridad, Ausencia de políticas de uso aceptable, Trabajo no supervisado de personal externo o de limpieza y Ausencia de acuerdos de nivel de servicio (ANS o SLA).

10.3. Estrategia para la Grupo de Servicios Administrativos ante un desastre o evento disruptivo

Las estrategia y acciones frente a desastres ante eventos disruptivos que puedan afectar la operación de Gestión Administrativa está basada en un enfoque en la identificación del estado real de la infraestructura y estaciones para la toma de decisiones oportunas que garanticen la continuidad operativa ante eventos adversos. Se implementan medidas preventivas, correctivas y de respuesta rápida para proteger los recursos físicos, tecnológicos y humanos de la entidad.

10.3.1. Acciones estratégicas

- Una vez se reestablezcan los activos debe continuarse con el mantenimiento preventivo regular a sistemas eléctricos, UPS, generadores y aires acondicionados, con cronogramas definidos.
- Una vez se reestablezcan los activos debe continuarse con la Gestión de contratos vigentes y comunicación con proveedores especializados para el mantenimiento de infraestructura crítica.

- Activación de trabajo en casa, avalado por la Secretaría General y el Grupo de Administración y Desarrollo del Talento Humano, cuando las condiciones lo requieran.
- En caso de una contingencia deben usarse los espacios resilientes, incluyendo zonas seguras, sistemas contra incendios y sistemas de detección temprana.
- Redundancia de servicios esenciales, como planta eléctrica y tanques de reserva de agua.
- Gestión y comunicación del contrato de vigilancia permanente, sin interrupciones, con personal capacitado.
- En la medida de lo posible debe continuar el monitoreo 24/7 mediante sistemas de CCTV y alarmas conectadas a centros de control, dependiendo de la afectación se busca la forma más efectiva de comunicación con la empresa de vigilancia, pero en todos los casos el canal es Grupo de Servicios Administrativos incluso en una contingencia.
- Una vez termine la contingencia debe reestablecerse el procedimiento de control de acceso, incluyendo sistemas biométricos, credenciales y zonas restringidas.
- Procedimientos establecidos para atención de siniestros, con roles definidos y rutas de evacuación. Con relación a siniestro se encuentra GSA-P001 Procedimiento trámite en siniestros SGI-PN001 Plan para la atención de urgencias, emergencias, contingencias y desastres.
- Informar a equipo de gestión de emergencias y crisis y activar los protocolos de respuesta a emergencias, contingencias y desastres.
- Aislamiento de zonas afectadas y que no generen condiciones de trabajo seguras.
- Activación de pólizas de los activos aseguradas para el diagnóstico de daños y cubrimiento.
- Gestión de recursos y planificación de acciones de adecuación, reconstrucción o reforma. Articular con la planeación institucional.

- **Consultar los documentos** SGI-PN001 Plan para la atención de urgencias, emergencias, contingencias y desastres, GSA-P001 Procedimiento trámite en siniestros.

10.3.2. Recursos críticos

- Sistema contra incendios (extintores, rociadores, detectores de humo)
- UPS y generadores eléctricos
- Infraestructura de respaldo TI (servidores alternos, nube, respaldo físico)
- Espacio alterno identificado – Trabajo en casa
- Suministro de agua alternativo (tanques o acceso externo)
- Personal de seguridad capacitado y turnos de emergencia
- Documentación digital y electrónica:
- Planos de las sedes
- Planes de mantenimiento
- Contratos con proveedores para los mantenimientos de infraestructura
- Contrato de servicio de vigilancia
- Contrato de programa de seguro

10.3.3. Riesgos de interrupción

- No hay afectación en confidencialidad baja, hay integridad media, disponibilidad Alta
- Riesgo de pérdida de acceso a la información y un riesgo relacionado con integridad.

Aplicaciones de estrategia en escenarios:

- Desastres naturales: sismos, inundaciones, tormentas, incendios.
- Emergencias sanitarias: brotes epidemiológicos, fumigaciones, condiciones de insalubridad.
- Fallas técnicas: cortes eléctricos, fallos en sistemas de climatización, daños en infraestructura TI.
- Interrupciones de servicios esenciales: agua, energía, conectividad.

- Accidentes físicos: incendios, explosiones, daños estructurales.
- Amenazas de seguridad: vandalismo, intrusiones, sabotaje.
- Ausencia de personal clave: por enfermedad, huelga, vacaciones no programadas.
- Mantenimiento locativo o remodelaciones: que impidan el acceso o uso de espacios críticos.
- Fallas en proveedores o terceros: incumplimiento de SLA, ausencia de personal de vigilancia o mantenimiento.

10.3.4. Amenazas y vulnerabilidades de seguridad

- **Vulnerabilidades**: Mantenimiento insuficiente, Ausencia de esquemas de reemplazo periódico, Sensibilidad a la radiación electromagnética, Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad), Almacenamiento sin protección, Falta de cuidado en la disposición final, Copia no controlada, Ausencia del personal, Entrenamiento insuficiente, Falta de conciencia en seguridad, Ausencia de políticas de uso aceptable, Trabajo no supervisado de personal externo o de limpieza y Ausencia de acuerdos de nivel de servicio (ANS o SLA).
- **Amenazas**: Daño físico, Eventos naturales, Pérdidas de los servicios esenciales, perturbación debida a la radiación, Fallas técnicas y Acciones no autorizadas.

10.4. Estrategia para la OAP ante un desastre o evento disruptivo:

10.4.1. Acciones estratégicas

Las estrategias y acciones frente a desastres ante eventos disruptivos que puedan afectar la operación de la Oficina Asesora de Planeación (OAP), se implementarán las siguientes medidas:

- Trabajo en casa o remoto mediante el uso de VPN segura o herramientas colaborativas para garantizar el acceso a sistemas de planeación,

seguimiento institucional y bases de datos estratégicas desde ubicaciones remotas.

- Provisión de transporte institucional para garantizar la seguridad sanitaria y la salud del personal durante desplazamientos en situaciones de emergencia.
- Evaluar afectación de información, herramientas o activos del proceso, solicitar reactivación de copias de respaldo del último back up a la Oficina de Informática y activar acciones de recuperación de información generada fuera de línea o en almacenada en borrador en herramientas colaborativas.
- Recursos disponibles para la continuidad:
  - Equipos de cómputo asignados al equipo
  - Herramientas de software para análisis de datos, seguimiento de indicadores y planificación estratégica.
  - Acceso a fuentes de información externas: bases de datos públicas, sistemas de reporte y control del sector público.
  - Recurso humano capacitado, con roles definidos para la gestión de emergencias y continuidad operativa.

10.4.2. Recursos críticos

- Infraestructura física
  - Oficinas administrativas y espacios de archivo.
  - Almacenes y bodegas para insumos y equipos.
  - Vehículos institucionales para transporte logístico.
- Recursos tecnológicos
  - Sistemas de gestión de la dependencia (SIGEP, SIIF, SIRECI, SUIT VISIÓN).
  - Equipos de cómputo asignados al personal administrativo.
  - Conectividad de red y acceso a internet.
  - Plataformas de gestión documental y correspondencia.
- Información crítica

- Bases de datos de contratos, proveedores, inventarios y órdenes de compra.
- Documentación del SGI
- Registros de solicitudes, trámites y autorizaciones internas.

- Recurso humano
  - Personal administrativo con funciones clave .
- Proveedores estratégicos
  - Empresas contratadas para servicios de limpieza, vigilancia, transporte, mantenimiento locativo y soporte técnico.
  - SLA (Acuerdos de Nivel de Servicio) vigentes para garantizar respuesta en contingencias.
- Recursos logísticos
  - Insumos de oficina, papelería, elementos de bioseguridad.
  - Equipos de respaldo (UPS, generadores, mobiliario alterno).

10.4.3. Riesgos de interrupción

Evaluación de impacto en caso de desastre:

La dependencia identifica riesgos que podrían afectar el acceso a la información estratégica, afectación a la integridad de datos de seguimiento institucional y retrasos en la toma de decisiones. La operación podría continuar, aunque con limitaciones en el impacto a la eficiencia y oportunidad de los reportes. Estos riesgos se asocian a seguridad de la información y la disponibilidad de la herramienta que soporta el SGI de la entidad a través de la plataforma Suite visión y se documentan en la matriz de riesgos de procesos de la entidad.

10.4.4. Aplicaciones de estrategia en escenarios

Escenarios donde se puede aplicar esta estrategia:

- Desastres naturales: Terremotos, inundaciones, tormentas que afecten la infraestructura física o tecnológica.

- Emergencias sanitarias: Pandemias, brotes epidemiológicos, fumigaciones que requieran aislamiento y trabajo remoto o en casa.
- Fallas técnicas: Caídas de servidores, fallos en hardware o software institucional.
- Interrupciones en servicios esenciales: Cortes de energía, fallos en conectividad o pérdida de acceso a internet.
- Eventos de seguridad informática: Ciberataques, accesos no autorizados, pérdida de integridad de datos.
- Accidentes físicos: Incendios, explosiones, vandalismo en instalaciones.
- Ausencia de personal: Paros, huelgas, emergencia sanitaria,
- Mantenimiento locativo: Remodelaciones, fumigaciones, reparaciones estructurales.
- Fallas en proveedores: Incumplimiento de SLA, fallas en servicios contratados como soporte técnico o mantenimiento.

10.4.5. Amenazas y vulnerabilidades de seguridad

Vulnerabilidades identificadas:

- Ausencia de mecanismos de monitoreo para brechas en la seguridad
- Asignación errada de los derechos de acceso

Amenazas potenciales:

- Error en el uso o abuso de derechos
- Uso no autorizado del equipo

Principios de seguridad aplicados:

- Disponibilidad alta: Se prioriza el acceso continuo a sistemas de planeación y seguimiento.
- Integridad media: Se implementan controles para minimizar alteraciones no autorizadas en la información institucional.

10.5. Estrategia para la Oficina de Informática (TI) ante un desastre o evento disruptivo

10.5.1. Acciones estratégicas

Las estrategias y acciones frente a desastres o eventos disruptivos que puedan afectar la operación del proceso de Gestión de Tecnología de la Información y Comunicaciones (TI) se implementarán de la siguiente manera:

- Activación del **SGI-PN006 Plan de recuperación de desastre** (DRP) para garantizar la restauración priorizada de servicios tecnológicos críticos, conforme a los tiempos de recuperación definidos.
- Habilitación de acceso remoto seguro mediante VPN institucional para asegurar la continuidad operativa del equipo técnico desde ubicaciones externas.
- Priorización del traslado de personal técnico clave a las instalaciones, según la criticidad de los servicios afectados y la necesidad de intervención física.
- Disponibilidad de infraestructura tecnológica redundante, incluyendo servidores, almacenamiento y conectividad, para mitigar interrupciones prolongadas.
- Reestablecer las copias de respaldo automáticas y programadas, tanto locales como en la nube, con acceso controlado para garantizar la disponibilidad e integridad de la información institucional ver GTI-P007 Procedimiento Back Up.
- Coordinación con el Equipo de Gestión de Crisis y el CSIRT para la atención de incidentes de seguridad informática y activación de protocolos de respuesta.
- Recursos disponibles para la continuidad:
    - Equipos de cómputo asignados al personal técnico.
    - Plataformas de monitoreo y gestión de incidentes.
    - Sistemas de respaldo y recuperación.
    - Acceso a proveedores estratégicos y soporte especializado.

- Personal capacitado en recuperación ante desastres y gestión de incidentes.

10.5.2. Recursos críticos

Dispositivos activos de red

- Al activar el **SGI-PN006 Plan de recuperación de desastre (DRP)**, se requiere como mínimo el establecimiento de los equipos de comunicación tales como:
- Firewall
- Switches
- Router suministrado por el Proveedor
- VPN – Site to Site
- VPN - Client
- Servicio de conectividad de acuerdo con el contrato vigente
- Canal de conectividad cuya capacidad esté de acuerdo con la necesidad del personal crítico incluido en el Análisis de Impacto al Negocio, este servicio es requerido con dos Proveedores diferentes, para asegurar disponibilidad.

Sistemas operativos

- Como requisito se deben tener los medios de instalación de los sistemas operativos que están instalados en los servidores críticos.
- Así mismo, es requisito mínimo contar con el backup teniendo cuenta el **GTI-P007 Procedimiento Back Up** para las configuraciones del sistema operativo de los servicios críticos, según los RPO's definidos. ***Ver* SGI-PN006 Plan de recuperación de desastre.**

Aplicaciones

- Las aplicaciones están configuradas y no requieren modificación o configuración específica. Se requiere contar backup de las configuraciones y parametrización de las aplicaciones críticas. Por ejemplo, datos de conexión, servicios web, parámetros, entre otros.

Bases de datos

- Al activar el **SGI-PN006 Plan de recuperación de desastre** (DRP), se requieren modificaciones a nivel de configuración de bases de datos. Así mismo, es necesario efectuar la restauración de acuerdo con el **GTI-P007 Procedimiento Back Up**. En el numeral 19 del documento **SGI-PN006 Plan de recuperación de desastre** se encuentran las bases de datos de estos aplicativos, en el numeral 17 del mismo documento, se encuentran las aplicaciones y servicios organizados por criticidad.
- Así mismo, es requisito mínimo contar con el backup de las configuraciones de base de datos. En este caso, se deben mantener respaldadas tanto las configuraciones como los datos de la aplicación de acuerdo con el RPO definido para cada aplicación. ***Ver* SGI-PN006 Plan de recuperación de desastre.**

10.5.3. Riesgos de interrupción

Pérdida de disponibilidad, confidencialidad e integridad de los servicios tecnológicos críticos del IDEAM debido a fallas en la infraestructura, eventos catastróficos, errores de configuración, accesos no autorizados, interrupciones en la conectividad institucional o fallos en los mecanismos de respaldo y recuperación, lo que podría comprometer la continuidad operativa institucional.

10.5.4. Aplicaciones de estrategia en escenarios

- Desastres naturales: Terremotos, inundaciones, tormentas que afecten la infraestructura tecnológica.
- Emergencias sanitarias: Pandemias o brotes que impidan el acceso físico del personal técnico.

  NOTA: para los escenarios anteriores deberá inicialmente seguir el plan de emergencia y contingencia – sede
- Fallas técnicas: Caídas de servidores, fallos en hardware o software institucional.

- Interrupciones en servicios esenciales: Cortes de energía, fallos en conectividad o pérdida de acceso a internet.
- Eventos de seguridad informática: Ciberataques, accesos no autorizados, pérdida de integridad de datos.
- Accidentes físicos: Incendios, explosiones, vandalismo en instalaciones tecnológicas.
- Ausencia de personal técnico: Enfermedades, paros o vacaciones no programadas.
- Mantenimiento locativo: Remodelaciones o adecuaciones que afecten el centro de datos.
- Fallas en proveedores: Incumplimiento de SLA o fallas en servicios contratados de soporte técnico.

10.5.5. Amenazas y vulnerabilidades de seguridad

Dentro de las vulnerabilidades identificadas se destacan:

- Dependencia de infraestructura física centralizada.
- Ausencia de esquemas de redundancia en algunos servicios.
- Limitada capacidad de respuesta ante múltiples incidentes simultáneos.
- Falta de acuerdos de nivel de servicio (SLA) con algunos proveedores.

Dentro de las amenazas detectadas

- Fallas técnicas en servidores, redes o sistemas de almacenamiento.
- Ciberataques dirigidos a la infraestructura institucional.
- Desastres naturales que afecten el centro de datos.
- Errores humanos en la operación o configuración de sistemas.

Principios de seguridad aplicados

- Disponibilidad alta: Se prioriza la restauración oportuna de servicios críticos.
- Integridad media: Se implementan controles para prevenir alteraciones no autorizadas en la información.

- Confidencialidad media: Se garantiza el acceso controlado a la información durante la recuperación.

11. Retorno a la normalidad

De acuerdo con el escenario de interrupción o afectación de la operación y las acciones de respuesta adelantadas se deberán ejecutar las siguientes acciones.

- Restablecimiento de sistemas y servicios afectados. El jefe de la Oficina de Informática debe restaurar la infraestructura tecnológica según el Plan de Recuperación de Desastres (DRP), incluyendo servidores, redes, aplicaciones y bases de datos.
- Las dependencias son responsables de validar la integridad y disponibilidad de la información restaurada e informar cualquier alteración de esta a través de la Mesa de Servicio.
- Reparación de estructuras físicas. El líder del Grupo de Servicios Administrativos y el líder de Talento Humano deben evaluar los daños en instalaciones, para ejecutar reparaciones necesarias para garantizar condiciones seguras de operación.
- Reincorporación del personal. El equipo de gestión de emergencias o crisis evaluará la determinación, en coordinación con los jefes y directivos de área, el retorno del personal a las instalaciones, asegurando las medidas de seguridad y salud en el trabajo (SST). Solicitará a la Secretaría General o coordinador de Gestión del Talento Humano, la expedición de la comunicación oficial para el retorno a normalidad de la operación presencial. Esta condición no deberá afectar los acuerdos de trabajo remoto o en casa autorizados y vigentes.
- Validación de procesos críticos. El equipo de gestión de emergencias o crisis reportará ante el Comité Institucional de Gestión y Desempeño la verificación del retorno de a niveles aceptables de operación.
- El jefe de la Oficina de informática debe realizar pruebas funcionales de los sistemas y servicios antes de la reactivación completa.

- Documentación y análisis post-incidente

  Cada una de las dependencias involucradas debe registrar todas las acciones ejecutadas, tiempos de recuperación y recursos utilizados, que permita formular lecciones aprendidas, para ajustar el plan con base en los resultados.
- Comunicación oficial. El Grupo de Comunicaciones debe emitir comunicados internos y/o externos sobre la normalización de operaciones, y restablecimiento de servicios, de acuerdo con los procedimientos definidos.

12. Competencia, pruebas y mejoras

- Inducción anual al PCN para todo el personal a través del Plan de Capacitación Institucional; formación específica para equipos críticos de acuerdo con las vulnerabilidades y mejoras identificadas.
- Las pruebas del DRP y simulacros de emergencias se deberán incorporar en la planeación institucional.
- El Plan de Continuidad de Negocio se revisará y actualizará al menos una vez al año y de acuerdo con la necesidad. Su actualización será liderada por la Oficina Asesora de Planeación en Coordinación con la Oficina de Tecnologías y la Secretaría General, así como de las dependencias que hacen parte de los procesos institucionales.
- En la siguiente actualización de plan de continuidad del negocio se tendrá en cuenta la gestión por procesos y se incluirá a toda la entidad.

13. Documentos relacionados en el SGI

- SGI-PN006 PLAN DE RECUPERACION DE DESASTRES
- GTI-P004 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES
- GTI-P007 PROCEDIMIENTO BACK UP
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

- SGI-PN001 PLAN PARA LA ATENCIÓN DE URGENCIAS EMERGENCIAS CONTINGENCIAS Y DESASTRES
- GD-I003 INSTRUCTIVO PARA LA PREVENCIÓN Y ATENCIÓN DE DESASTRES EN DEPOSITOS DE ARCHIVOS GENERAL DEL IDEAM.
- MATRIZ BIA – MATRIZ DE ANÁLISIS DE IMPACTO DEL NEGOCIO
- MAPA DE RIESGOS INSTITUCIONAL
- LISTADO MAESTRO DE DOCUMENTOS
- POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- POLÍTICA Y MANUAL DE ADMINISTRACIÓN DE RIESGOS

14. Bibliografía

NTC ISO -22301:2012 Continuidad del negocio. Sistema de continuidad del negocio.

NTC ISO -IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información requisitos

Guía para la preparación de las TIC para la continuidad del negocio, MINCTIC

Guía para realizar en análisis de impacto del negocio BIA, MINTIC

Guía: Controles de seguridad y privacidad de la información, MINTIC

15. Control de cambios

Versión	Fecha	Descripción
01	23/12/2025	Creación del Documento