
 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

## PLAN DE RECUPERACIÓN DE DESASTRES TECNOLOGICOS




**SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS**

**DICIEMBRE DE 2025**

	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLÓGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

## TABLA DE CONTENIDO

1.	INTRODUCCION	4
2.	OBJETIVO GENERAL	5
2.1.	Objetivos específicos	5
3.	ANTECEDENTES	5
3.1.	Condiciones normales de operación	6
3.2.	Escenarios de Desastre Identificados	7
3.3.	Estrategias DRP	10
3.4.	Arquitectura De TI	16
3.5.	Catálogo De Sistemas De Información	19
3.6.	Resultados De Análisis De Impacto Al Negocio	23
4.	ALCANCE DEL DRP	24
4.1.	Controles Seguridad Física Y Servicios De Soporte En Data Center	24
4.2.	Seguridad Informática	24
4.3.	Servicios De TI	25
4.4.	Sistemas De Información Y Aplicaciones	25
4.5.	PREMISAS Y LIMITACIONES	27
5.	GOBIERNO DEL PLAN DE RECUPERACIÓN DE DESASTRES	28
5.1.	Política	28
5.2.	Roles y Responsabilidades	29
5.2.1.	Líder DRP	30
5.2.2.	Equipo de recuperación de servicios tecnológicos base	30
5.2.3.	Equipo de recuperación de sistemas de información y aplicaciones	30
5.2.4.	Equipo de enlace con usuarios y proveedores	31
6.	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	32
6.1.	FASE PREVENTIVA	33
6.2.	FASE DE RESPUESTA	33
6.1.1.	Procedimiento de respuesta a emergencias	34
6.1.2.	Procedimiento de notificación	35
6.1.3.	Procedimiento de evaluación de daños	37
6.1.4.	Procedimiento de activación	38
6.1.5.	Procedimiento de recuperación de la infraestructura tecnológica	38

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


6.3.	FASE DE RESTAURACIÓN	40
6.3.1.	Procedimiento de alistamiento de instalaciones	40
6.3.2.	Procedimiento de retorno a la normalidad	42
7.	RIESGOS DE ACTIVAR EL DRP	44
8.	BIBLIOGRAFÍA	46
9.	HISTORIAL DE CAMBIOS	¡Error! Marcador no definido.
10.	GLOSARIO ISO 22301	46

## ÍNDICE DE TABLAS

Tabla 1.	Escenarios de Desastre	9
Tabla 2.	Estrategia de Continuidad	16
<b>Tabla 3.</b>	Catálogo de Sistemas de Información	22
Tabla 4.	Secuencia de recuperación calculada	24
Tabla 5	Secuencia de Recuperación Tecnológica	26
Tabla 6	Actividades de la fase preventiva	33
Tabla 7	Datos de contacto internos del DRP	35
Tabla 8	Datos de contacto externos del DRP	36
Tabla 9	Procedimiento de recuperación de la infraestructura tecnológica	40
Tabla 10	Procedimiento de alistamiento de instalaciones	41
Tabla 11	Procedimiento de retorno a la normalidad	43

## ÍNDICE DE ILUSTRACIONES

Ilustración 1	Arquitectura tecnológica de la Agencia Nacional de Tierras – ANT	17
Ilustración 2	Conexiones con Datacenter Principal HostDime Nebula	18
Ilustración 3	Equipos del DRP	29
Ilustración 4	Fases del DRP	32
Ilustración 5	Etapas de respuesta	34
Ilustración 6	Actividades en la respuesta a emergencias	34
Ilustración 7	Actividades de la evaluación de daños	37
Ilustración 8	Activación del BCP o DRP	38

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025


## 1. INTRODUCCION

La Agencia Nacional de Tierras (ANT), en cumplimiento de su misión institucional y de los lineamientos del Estado en materia de gestión del riesgo, continuidad del negocio y seguridad de la información, ha definido el presente Plan de Recuperación de Desastres Tecnológicos (DRP) como un instrumento fundamental para garantizar la restauración oportuna de los servicios tecnológicos que soportan sus procesos misionales, estratégicos y de apoyo, ante la ocurrencia de incidentes o eventos disruptivos de origen tecnológico.

Este plan se construye con base en los resultados del Análisis de Impacto al Negocio (BIA), el cual permitió identificar los procesos críticos de la entidad, los activos de información asociados, los servicios tecnológicos que los soportan, así como los niveles máximos de interrupción aceptables, los tiempos objetivos de recuperación (RTO) y los puntos objetivos de recuperación de la información (RPO). Dichos resultados constituyen el insumo principal para la definición de las estrategias, procedimientos y prioridades de recuperación tecnológica establecidas en este documento.

El DRP de la ANT establece los roles, responsabilidades, procedimientos técnicos y operativos, así como los mecanismos de coordinación necesarios para responder de manera estructurada y eficaz ante escenarios de indisponibilidad tecnológica, tales como fallas de infraestructura, incidentes de ciberseguridad, pérdida de información, interrupciones de conectividad o desastres que afecten los centros de procesamiento de datos y los servicios tecnológicos críticos.

La implementación y mantenimiento de este plan permite a la Agencia fortalecer su resiliencia tecnológica, minimizar los impactos operativos, legales y reputacionales derivados de interrupciones prolongadas, y asegurar la continuidad en la prestación de los servicios a la ciudadanía, en coherencia con el Plan de Continuidad de Negocio, el Modelo Integrado de Planeación y Gestión (MIPG) y las buenas prácticas internacionales en gestión de continuidad y recuperación ante desastres.

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

## 2. OBJETIVO GENERAL

Garantizar la recuperación oportuna y segura de los servicios tecnológicos, aplicaciones, infraestructura y activos de información que soportan los procesos de la Agencia Nacional de Tierras (ANT), con base en los resultados del Análisis de Impacto al Negocio (BIA), mediante la definición e implementación de estrategias, procedimientos, roles y recursos de recuperación ante desastres, que permitan restablecer la operación dentro de los tiempos y niveles de servicio aceptables (RTO y RPO), minimizando los impactos operativos, legales y reputacionales y asegurando la continuidad en la prestación de los servicios a la ciudadanía.

### 2.1. Objetivos específicos


- Identificar y priorizar los servicios tecnológicos, aplicaciones, infraestructuras y activos de información críticos de la Agencia Nacional de Tierras (ANT), con base en los resultados del Análisis de Impacto al Negocio (BIA), con el fin de orientar de manera efectiva las acciones de recuperación ante desastres tecnológicos.
- Definir los tiempos objetivos de recuperación (RTO) y los puntos objetivos de recuperación de la información (RPO) para los servicios tecnológicos críticos, conforme a los niveles de impacto y tolerancia al riesgo establecidos en el Análisis de Impacto al Negocio (BIA).
- Establecer las estrategias de recuperación tecnológica necesarias para asegurar la disponibilidad y restablecimiento de la infraestructura, las plataformas, los sistemas de información y los servicios de comunicaciones ante escenarios de desastre o interrupciones mayores.
- Definir de manera clara los roles y responsabilidades del personal interno y de los proveedores tecnológicos involucrados en la ejecución, coordinación y control del Plan de Recuperación de Desastres (DRP).
- Establecer mecanismos de coordinación, articulación y alineación del Plan de Recuperación de Desastres (DRP) con el Plan de Continuidad del Negocio (PCN), el Sistema de Gestión de Seguridad de la Información y los demás instrumentos de gestión institucional.
- Determinar los requerimientos de recursos tecnológicos, humanos y logísticos necesarios para la implementación, operación y mantenimiento efectivo del Plan de Recuperación de Desastres (DRP)
- Fortalecer la capacidad de respuesta y la resiliencia tecnológica de la Agencia Nacional de Tierras (ANT) frente a eventos disruptivos que puedan afectar la disponibilidad de los servicios tecnológicos y la continuidad de sus operaciones institucionales.

## 3. ANTECEDENTES

La Agencia Nacional de Tierras, como máxima autoridad de las tierras de la Nación, tiene por objeto ejecutar la política de ordenamiento social de la propiedad rural formulada por el Ministerio de Agricultura y Desarrollo Rural, para lo cual debe gestionar el acceso a la tierra como factor productivo, lograr la seguridad jurídica sobre ésta, promover su uso en cumplimiento de la función social de la propiedad y administrar y disponer de los predios rurales de propiedad de la Nación.

En términos generales, la Agencia Nacional de Tierras garantiza el acceso a la tierra para los campesinos que no la tienen o que tienen muy poca e insuficiente para su sustento.

También se pondrá en marcha la figura del Inspector de Tierras dotándola de todas las herramientas que permitan hacerles veeduría a los procesos de manera minuciosa. Sin embargo, y para cerrarles el paso a los corruptos,

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

implementará también una gestión abierta al público y participativa de modo que las comunidades en las regiones, y de manera organizada, puedan participar y vigilar las actuaciones de la Agencia y de sus funcionarios.

### **3.1. Condiciones normales de operación**

La Agencia Nacional de Tierras (ANT) desarrolla su operación a nivel nacional, a través de una estructura descentralizada conformada por una sede central y oficinas territoriales y regionales, desde las cuales se ejecutan los procesos misionales relacionados con la administración, ordenamiento y formalización de la propiedad rural, así como los procesos estratégicos y de apoyo institucional.

La sede central concentra la dirección estratégica, la toma de decisiones, la coordinación institucional y la administración de los principales procesos de apoyo, incluyendo direccionamiento estratégico, apoyo jurídica, gestión financiera, gestión de talento humano, gestión de la información y seguimiento, evaluación y mejora. Por su parte, las oficinas territoriales permiten la atención directa a la ciudadanía y la ejecución operativa de los procesos misionales en las distintas regiones del país, garantizando la cobertura territorial y la presencia institucional en zonas rurales.


Desde el punto de vista tecnológico, la operación de la ANT se soporta en una infraestructura tecnológica centralizada, que incluye plataformas de información, sistemas de gestión institucional, bases de datos, aplicaciones misionales y servicios de comunicación, alojados en un centro de datos propio y algunos servicios tecnológicos provistos por terceros, conforme a los esquemas de contratación vigentes del Estado. Esta infraestructura permite el acceso remoto y distribuido de los funcionarios desde las diferentes sedes, a través de redes seguras y mecanismos de autenticación institucional.

Los servicios tecnológicos críticos incluyen, entre otros, los sistemas de información misionales para la gestión de tierras, plataformas documentales, correo electrónico institucional, herramientas de colaboración, servicios de red y conectividad, así como los componentes de respaldo y seguridad de la información. La indisponibilidad de estos servicios impacta directamente la capacidad de la entidad para prestar servicios a la ciudadanía y cumplir sus funciones legales.

La operación diaria de la ANT depende de la disponibilidad de la infraestructura física (oficinas, puestos de trabajo y conectividad), del personal clave, y del funcionamiento continuo de la infraestructura tecnológica, lo que hace necesario contar con mecanismos formales de continuidad y recuperación que permitan mitigar los efectos de eventos disruptivos y garantizar la resiliencia institucional.

### **Estrategia De Recuperación Actual De La Agencia Nacional De Tierras - ANT**

- La Agencia Nacional de Tierras - ANT cuenta con la capacidad para implementar en la nube servicios de contingencia (Datacenter Alterno en Nube), disponibles en caso de que se presente una falla que afecte los sistemas de información y aplicaciones que se encuentran operando en Datacenter Principal o en Azure.
- La Agencia Nacional de Tierras - ANT cuenta con soluciones de virtualización que garantizan la alta disponibilidad de los servidores gestionados, así mismo en Azure se tienen servicios en alta disponibilidad según la criticidad del servicio desplegado.
- La Agencia Nacional de Tierras - ANT cuenta con soluciones de seguridad informática que previenen la materialización de ciberataques a la infraestructura.


	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 3.2. Escenarios de Desastre Identificados<sup>1</sup>

A continuación se presentan los escenarios de desastre identificados:


ESCENARIO DE DESASTRE	AMENAZAS / CAUSAS	VULNERABILIDADES	CONSECUENCIAS	BCP	DRP
<b>Escenario # 1</b> <b>Falla generalizada de los canales de comunicación en Centro de Datos Principal de la ANT</b>  <b>Categoría II</b>	<ul style="list-style-type: none"> <li>Fallas en los dispositivos de red internos (Firewall, switches, etc.)</li> <li>Fallas en los dispositivos de red proporcionados por el proveedor.</li> <li>Fallas en los canales de comunicación contratados en Centro de Datos Principal.</li> <li>Condiciones ambientales extremas.</li> <li>Amenazas naturales (sismos, inundaciones, incendios, entre otros).</li> <li>Fallas eléctricas, incendios, inundaciones, fallas de hardware, ataques físicos</li> </ul>	<ul style="list-style-type: none"> <li>Se tiene un único proveedor (EMTEL) para la prestación de servicios MPLS y acceso a Internet. Sin embargo, dichos servicios tienen HA.</li> <li>Se cuenta con un único Centro de Datos, no se tiene alterno.</li> <li>No se tiene Datacenter Alterno</li> </ul>	<ul style="list-style-type: none"> <li>Pérdida de comunicación con ciudadanos, y con servicios en la Nube.</li> <li>Pérdida en el acceso a internet.</li> <li>Fallas en los canales de replicación con servicios en la Nube.</li> <li>Imposibilidad para hacer reportes a entidades de vigilancia y control.</li> <li>Imposibilidad para acceder a servicios de TI internos, como: Office 365, carpetas compartidas, sistemas y aplicaciones que apoyan los diferentes procesos.</li> <li>Interrupción de procesos que dependen del acceso a internet.</li> </ul>		X

<sup>1</sup> Ver documento: Escenarios de Desastre

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

ESCENARIO DE DESASTRE	AMENAZAS / CAUSAS	VULNERABILIDADES	CONSECUENCIAS	BCP	DRP
<b>Escenario # 2</b>  <b>Interrupción total de servicios tecnológicos en Centro de Datos Principal de la ANT</b>  <b>Categoría I</b>	<ul style="list-style-type: none"> <li>• Ataque cibernético dirigido.</li> <li>• Contaminación por malware (Código malicioso, virus, troyanos, ransomware, entre otros).</li> <li>• Ausencia de mantenimiento a la infraestructura tecnológica.</li> <li>• Ausencia prolongada del servicio de energía eléctrica.</li> <li>• Falla en sistemas de soporte al Centro de Datos Principal (Aires acondicionados, UPS, plantas eléctricas u otros).</li> <li>• Errores en la administración de la plataforma tecnológica del Centro de Datos Principal.</li> <li>• Falla masiva de hardware crítico que soporta los servicios de TI.</li> <li>• Condiciones ambientales extremas.</li> </ul>	<ul style="list-style-type: none"> <li>• Se cuenta con un único Centro de Datos, no se tiene alterno.</li> <li>• Aunque se tiene infraestructura en sede CAN, es para pruebas y desarrollo y no tiene la capacidad para soportar el ambiente productivo que se tiene en Centro de Datos Principal en Hostdime.</li> </ul>	<ul style="list-style-type: none"> <li>• Interrupción de los procesos que dependen completamente de los servicios prestados por el Centro de Datos Principal.</li> <li>• Interrupción de procesos de apoyo que requieren servicios tecnológicos prestados por el Centro de Datos Principal para operar.</li> <li>• Interrupción de los servicios prestados a los ciudadanos.</li> <li>• No disponibilidad de la información almacenada en servidores OnPremise</li> <li>• Caída de los sistemas de información internos.</li> <li>• Interrupción de los servicios de TI críticos.</li> </ul>		X
<b>Escenario # 3</b>  <b>No disponibilidad de las oficinas principales de la ANT</b>  <b>Categoría I</b>	<ul style="list-style-type: none"> <li>• Amenazas naturales (sismos, inundaciones, incendios, entre otros).</li> <li>• Afectación del orden público (marchas, protestas).</li> <li>• Epidemia.</li> <li>• Cuarentenas o medidas decretadas por el Gobierno para contener las pandemias.</li> <li>• Ataque externo (ataque terrorista).</li> </ul>	<ul style="list-style-type: none"> <li>• Aunque se tiene definida una estrategia de teletrabajo, no se tiene definidas Oficinas Alternas</li> </ul>	<ul style="list-style-type: none"> <li>• Destrucción de información física de las diferentes áreas.</li> <li>• Parálisis de los procesos del negocio.</li> <li>• No disponibilidad del personal.</li> <li>• No disponibilidad de las instalaciones físicas necesarias para los procesos.</li> <li>• Heridos.</li> <li>• Pérdida de vidas humanas.</li> <li>• Interrupción de los servicios prestados a los ciudadanos.</li> </ul>	X	




	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLÓGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

ESCENARIO DE DESASTRE	AMENAZAS / CAUSAS	VULNERABILIDADES	CONSECUENCIAS	BCP	DRP
<b>Escenario # 4</b>  <b>Ausencia de personal crítico</b>  <b>Categoría II</b>	<ul style="list-style-type: none"> <li>No renovación oportuna de contratos de personal contratista</li> <li>No disponer del personal técnico que mantiene o administra la plataforma o infraestructura tecnológica</li> </ul>	<ul style="list-style-type: none"> <li>Se tiene un único proveedor por servicio tecnológico.</li> <li>Ausencia de documentación de actividades críticas.</li> <li>Alta dependencia de personal contratista.</li> <li>Incapacidad de ejecutar procesos críticos sin personal capacitado.</li> </ul>	<ul style="list-style-type: none"> <li>Interrupción de procesos por la ausencia de personal contratista,</li> <li>Interrupción de los servicios prestados a los ciudadanos.</li> </ul>	X	
<b>Escenario # 5</b>  <b>Interrupción de proveedores de servicios críticos que impactan la continuidad de los procesos de la ANT</b>  <b>Categoría II</b>	<ul style="list-style-type: none"> <li>Interrupción del proveedor de servicios de conectividad EMTel: MPLS y acceso a internet.</li> <li>Interrupción de servicios prestados por Microsoft: Azure y Office 365.</li> <li>Interrupción de servicios prestados por el proveedor Datasec: Seguridad perimetral.</li> </ul>	<ul style="list-style-type: none"> <li>Se tiene un único proveedor por servicio tecnológico.</li> <li>Ausencia de procesos de evaluación de proveedores en cuanto al BCP y DRP.</li> </ul>	<ul style="list-style-type: none"> <li>No disponibilidad de canales de comunicación.</li> <li>No disponibilidad del servicio de Office 365.</li> <li>Interrupción total de servicios tecnológicos en Centro de Datos Principal.</li> <li>Interrupción de los servicios prestados a los ciudadanos.</li> </ul>	X	
<b>Escenario # 6</b>  <b>Estado de emergencia a nivel nacional</b>  <b>Categoría III</b>	<ul style="list-style-type: none"> <li>Amenaza natural.</li> <li>Pandemia.</li> <li>Cuarentenas o medidas decretadas por el Gobierno para contener las pandemias.</li> <li>Ataque terrorista.</li> <li>Conflicto armado internacional.</li> </ul>	<ul style="list-style-type: none"> <li>No se identifican vulnerabilidades ya que en pandemia se dio continuidad a los servicios de la ANT, mediante la estrategia de trabajo en casa.</li> </ul>	<ul style="list-style-type: none"> <li>No disponibilidad de la información.</li> <li>Parálisis de los procesos del negocio.</li> <li>Destrucción de información lógica y física.</li> <li>No disponibilidad de personal.</li> <li>Heridos.</li> <li>Pérdida de vidas humanas.</li> <li>Interrupción de los servicios prestados a los ciudadanos.</li> </ul>	X	X

Tabla 1. Escenarios de Desastre

Vale la pena hacer la siguiente aclaración: Como parte del desarrollo de las funciones en la ANT, se pueden presentar situaciones puntuales que afectan o interrumpen parcialmente la ejecución de actividades o tareas particulares. Estos casos no se catalogan como situaciones de desastres o incidentes mayores, razón por la cual no se abordan como parte de este plan.


	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 3.3. Estrategias DRP<sup>2</sup>


A continuación, se extrae un resumen de las estrategias contempladas en el documento Estrategias de continuidad que aplican al DRP, y en color verde se seleccionan las más opcionadas:

TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
2. Instalaciones físicas.	<b>2.1. Data Center Principal</b>			
	2.1.1. Data Center Principal en sede central de la ANT. Propio	Garantizar continuidad a todos los sistemas de información y servicios tecnológicos que operan actualmente en el Data Center ubicado en la sede central de la ANT.	<ul style="list-style-type: none"> <li>• Dar continuidad a los sistemas de información y servicios tecnológicos que operan actualmente en el Data Center principal, ubicado en la sede central de la ANT.</li> <li>• Gestionar y verificar el mantenimiento preventivo y correctivo de la infraestructura presente en dicho Data Center.</li> <li>• Evitar la obsolescencia tecnológica de la infraestructura presente en el Data Center.</li> <li>• Garantizar la dotación acorde a estándares y normas internacionales para Data Center.</li> </ul>	Implementada
	<b>2.2. Data Center Alterno</b>			
	2.2.1. DRP en nube pública con el mismo proveedor, en otra zona	Establecer con el proveedor que presta el servicio de nube pública principal (Microsoft Azure), un servicio complementario que haga las veces de esquema de DRP en una zona diferente a la zona utilizada para los servicios dispuestos en Datacenter Principal y los servicios productivos en Microsoft Azure	<ul style="list-style-type: none"> <li>• Puede definirse un alcance particular para el servicio de DRP que tan solo contemple el subconjunto de capacidades tecnológicas identificadas como críticas para la ANT, o que tengan un RTO cercano a cero (0), dispuestos en Datacenter Principal y en el ambiente productivo de Microsoft Azure.</li> <li>• Pueden establecerse esquemas de sincronización con diferente periodicidad, dependiendo de los RPO identificados en el BIA.</li> <li>• El redireccionamiento del tráfico hacia las capacidades tecnológicas establecidas en la nueva zona debe ser definido conjuntamente entre la ANT, los proveedores de telecomunicaciones y otros proveedores críticos,</li> </ul>	Pendiente de aprobación


<sup>2</sup> Ver documento: Estrategias de continuidad

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
			<p>con el fin de planear y contemplar la ejecución oportuna de todos los cambios requeridos cuando se active el DRP.</p> <ul style="list-style-type: none"> <li>Los esquemas de seguridad perimetral también deben cubrir la operación desde la nueva zona de nube pública cuando se active el DRP.</li> </ul>	
	2.2.2. DRP en una nube pública con proveedor diferente.	Establecer con otro proveedor diferente al que presta el servicio de nube pública principal (Microsoft Azure), un servicio que haga las veces de un esquema de DRP, para los servicios dispuestos en Datacenter Principal y los servicios productivos en Microsoft Azure.	<ul style="list-style-type: none"> <li>Puede definirse un alcance particular para el servicio de DRP que tan solo contemple el subconjunto de capacidades tecnológicas identificadas como críticas para la ANT, o que tengan un RTO cercano a cero (0), dispuestos en Datacenter Principal y en el ambiente productivo de Microsoft Azure.</li> <li>Pueden establecerse esquemas de sincronización con diferente periodicidad, dependiendo de los RPO identificados en el BIA.</li> <li>El redireccionamiento del tráfico hacia las capacidades tecnológicas establecidas en la nueva zona debe ser definido conjuntamente entre la ANT, los proveedores de telecomunicaciones y otros proveedores críticos, con el fin de planear y contemplar la ejecución oportuna de todos los cambios requeridos cuando se active el DRP.</li> <li>Los esquemas de seguridad perimetral también deben cubrir la operación desde la nueva zona de nube pública cuando se active el DRP.</li> </ul>	Pendiente de aprobación
	2.2.3. DRP en nube privada.	Implementar un esquema de DRP a través de un servicio de nube privada, para los servicios dispuestos en Datacenter Principal y los servicios productivos en Microsoft Azure.	<ul style="list-style-type: none"> <li>Puede definirse un alcance particular para el servicio de DRP que tan solo contemple el subconjunto de capacidades tecnológicas identificadas como críticas para la ANT, o que tengan un RTO cercano a cero (0), dispuestos en Datacenter Principal y en el ambiente productivo de Microsoft Azure.</li> <li>Pueden establecerse esquemas de sincronización con diferente periodicidad, dependiendo de los RPO identificados en el BIA.</li> <li>El redireccionamiento del tráfico hacia las capacidades tecnológicas establecidas en la nueva zona debe ser definido conjuntamente entre la ANT, los proveedores de telecomunicaciones y otros proveedores críticos, con el fin de planear y contemplar la ejecución oportuna de todos los cambios requeridos cuando se active el DRP.</li> </ul>	Pendiente de aprobación

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
			<ul style="list-style-type: none"> <li>La ANT deberá establecer y gestionar los esquemas de seguridad de la información y ciberseguridad para cubrir la operación del DRP en la nube privada.</li> <li>Para mantener o mejorar la eficiencia y escalabilidad de las capacidades del DRP se requerirá de varios análisis minuciosos y proyectos que estarán directamente a cargo de la ANT.</li> </ul>	
	2.2.4. DRP en infraestructura propia.	Implementar un esquema de DRP en una infraestructura propia On-Premise.	<ul style="list-style-type: none"> <li>Puede definirse un alcance particular para el servicio de DRP que tan solo contemple el subconjunto de capacidades tecnológicas identificadas como críticas para la ANT, o que tengan un RTO cercano a cero (0), dispuestos en Datacenter Principal y en el ambiente productivo de Microsoft Azure.</li> <li>Pueden establecerse esquemas de sincronización con diferente periodicidad, dependiendo de los RPO identificados en el BIA.</li> <li>El redireccionamiento del tráfico hacia las capacidades tecnológicas establecidas en la nueva zona debe ser definido conjuntamente entre la ANT, los proveedores de telecomunicaciones y otros proveedores críticos, con el fin de planear y contemplar la ejecución oportuna de todos los cambios requeridos cuando se active el DRP.</li> <li>La ANT deberá establecer y gestionar los esquemas de seguridad de la información y ciberseguridad para cubrir la operación del DRP en la nube privada.</li> <li>Para mantener o mejorar la eficiencia y escalabilidad de las capacidades del DRP se requerirá de varios análisis minuciosos y proyectos que estarán directamente a cargo de la ANT.</li> </ul>	Pendiente de aprobación
<b>2.4. Centro Alterno de Operaciones (Oficinas alternas)</b>				
	2.4.1. Acordar con una Entidad del sector la adecuación de un espacio como el Centro Alterno de Operaciones de la ANT.	Garantizar unas instalaciones físicas de forma rápida y económica para que los colaboradores de la ANT puedan desarrollar sus actividades en caso de presentarse un desastre o emergencia en las oficinas de la Entidad.	<ul style="list-style-type: none"> <li>Informe BIA actualizado (Análisis de puestos de trabajo)</li> <li>Escenarios de desastre identificados.</li> <li>Definir un acuerdo con una entidad del sector para adecuar un espacio como Centro Alterno de Operaciones de la ANT, con el fin de operar los procesos de negocio en caso de una contingencia en las oficinas administrativas de la entidad.</li> </ul>	Pendiente de aprobación

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
			<ul style="list-style-type: none"> <li>Definir las condiciones de entrega del espacio (puestos de trabajo, puntos de redes, entre otros)</li> </ul>	
	2.4.2. Establecer un contrato de arrendamiento de oficinas en las que se pueda poner en funcionamiento el Centro Alterno de Operaciones de la ANT.	Garantizar unas instalaciones físicas con un costo previamente acordado, para que los colaboradores de la ANT puedan desarrollar sus actividades en caso de presentarse un desastre o emergencia en las oficinas de la Entidad.	<ul style="list-style-type: none"> <li>Informe BIA actualizado (análisis de puestos de trabajo)</li> <li>Escenarios de desastre identificados.</li> <li>Identificar los posibles contratistas que permitan generar un contrato de arrendamiento que entre en vigencia únicamente cuando se presente un desastre o emergencia en la ANT.</li> <li>Evaluar las diferentes propuestas.</li> <li>Seleccionar las oficinas desde las que funcionara el Centro Alterno de Operaciones.</li> </ul>	Pendiente de aprobación
	2.4.3. Realización de actividades mediante acceso remoto (trabajo en casa).	Permitir la continuidad de los procesos de negocio mediante el uso de las TICs como el acceso remoto.	<ul style="list-style-type: none"> <li>Informe BIA actualizado (análisis de puestos de trabajo)</li> <li>Escenarios de desastre identificados.</li> <li>Identificar personal que pueda desarrollar sus funciones en modo teletrabajo.</li> <li>Definir políticas de acceso remoto en caso de emergencias.</li> <li>Establecer auxilios económicos para los colaboradores que desarrollan sus labores desde la casa, debido al uso de recursos del hogar para desempeñar sus actividades laborales.</li> <li>Realizar pruebas de conectividad de los teletrabajadores a los servicios de TI requeridos por los colaboradores, para desarrollar sus funciones.</li> </ul>	Implementada
3. Aprovisionamiento de infraestructura en Data Center Alterno y Centro de Monitoreo Alterno.	<b>3.1. Infraestructura en Data Center Alterno</b>  3.1.1. Plataforma de replicación.	Contar con la tecnología necesaria para garantizar la replicación de la información entre el Data Center Principal y el Data Center Alterno. Incluye la replicación de Backups y Máquinas Virtuales.	<ul style="list-style-type: none"> <li>Actualmente se tiene un servicio de replicación entre el Data Center principal y el Data Center Alterno, que incluye la replicación de Backups y Máquinas Virtuales de los servicios tecnológicos identificados en el BIA como críticos.</li> <li>Poner en funcionamiento el servicio de replicación.</li> </ul>	Pendiente de aprobación


	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
	3.1.2. Puesta en funcionamiento de infraestructura tecnológica en Data Center Alterno.	Garantizar que la ANT cuente con un Data Center Alterno desde el que operen los servicios tecnológicos identificados en el BIA como críticos.	<ul style="list-style-type: none"> <li>• Aprovisionamiento de la infraestructura tecnológica necesaria en el Data Center Alterno para poner en operación los servicios tecnológicos críticos identificados en el BIA.</li> <li>• Realizar la configuración de los servicios de red, solución de hiperconvergencia, servidores de bases de datos, servidores de almacenamiento y soluciones de seguridad informática.</li> <li>• Mantener actualizados los procedimientos de recuperación tecnológica para los servicios críticos de TI</li> </ul>	Pendiente de aprobación
	3.1.3. Soluciones de seguridad informática.	Garantizar que el Data Center Alterno cuente con las soluciones de seguridad informática mínimas para proteger las plataformas y la operación desde dicho lugar.	<ul style="list-style-type: none"> <li>• Adquirir y poner en funcionamiento las siguientes soluciones de seguridad informática, según lo identificado en el BIA: <ul style="list-style-type: none"> <li>○ Firewall de aplicaciones web WAF</li> <li>○ Firewall perimetral – VPN.</li> <li>○ Sistema de prevención de intrusos IPS</li> <li>○ Antivirus EndPoint</li> <li>○ Correlación de eventos SIEM</li> </ul> </li> </ul>	Pendiente de aprobación
4. Información y Datos	4.1. Implementar un esquema para la gestión de las copias de respaldo de la información y datos clave para la prestación de los servicios críticos que garantice su oportuna transferencia y/o restauración, en caso de requerirse.	Garantizar que se disponga de las copias de respaldo de la información y de los datos requeridos para continuar prestando los servicios críticos en infraestructuras o instalaciones contingentes (diferentes a las principales). En el alcance del esquema se deben validar los requerimientos de información digital y de documentación física, así como los índices RTO y RPO definidos para los servicios críticos.	<ul style="list-style-type: none"> <li>• Identificar aquellos requerimientos de información y/o datos para la prestación de los servicios críticos que aún no disponen de un esquema de gestión de copias de respaldo que esté acorde con los umbrales de plazos establecidos.</li> <li>• Planificar y desarrollar el proyecto de gestión de las copias de respaldo identificadas en la actividad anterior, el cual debe considerar la correcta obtención, la custodia segura, la debida indexación, la oportuna transferencia y la efectiva restauración en infraestructura/instalaciones contingentes.</li> <li>• Continuar, diseñar e iniciar el plan de pruebas periódicas de restauración de las copias de respaldo que permitan verificar su calidad y usabilidad.</li> <li>• Continuar, planear y ejecutar simulacros periódicos que incluyan la transferencia y/o restauración de las copias de respaldo a infraestructura/instalaciones alternas a fin de comprobar que el esquema</li> </ul>	Implementada

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
			atiende los requisitos de oportunidad pactados con los usuarios y entidades.	
	4.2. Proceso de digitalización de documentos físicos.	Tener una copia digital de toda la documentación en medio físico que es crítica para la operación de los procesos de negocio de la ANT.	<ul style="list-style-type: none"> <li>● Inventario detallado de la información física en cada sede que sea de vital importancia para los procesos de negocio.</li> <li>● Implementar un proceso de digitalización de la documentación física crítica para la operación de la ANT.</li> <li>● Garantizar el acceso a la información digitalizada desde el Data Center Alterno.</li> </ul>	Pendiente de aprobación
	4.3. Mantener y fortalecer las soluciones tecnológicas que permitan intensificar la digitalidad y reducir procesos, procedimientos y gestión de documentos y objetos físicos.	Esta alternativa permite la automatización progresiva de tareas manuales y físicas que conllevan inconvenientes de dependencia de personal, instalaciones y generación y manipulación de documentos y objetos físicos, los cuales conllevan riesgos relacionados con la destrucción de activos.	<ul style="list-style-type: none"> <li>● Evaluar periódicamente las estrategias de digitalidad para mejorar continuamente la eficiencia en la gestión documental y mitigar el riesgo de destrucción de archivos y repositorios físicos de información.</li> <li>● Hay que asegurar que toda la documentación formal nueva producida por la ANT y recibida por esta, sea digitalizada e indexada desde el principio y de esta manera reducir al mínimo la acumulación de documentos físicos.</li> </ul>	Pendiente de aprobación
6. Tecnologías de la Información y Comunicaciones	<b>6.1. Data Center Principal</b>			
	6.1.1. Implementar los servicios/canales alternos de telecomunicaciones con proveedores distintos para mejorar la probabilidad de continuar operando en caso de caídas de los enlaces principales.	Asegurar que los servicios y/o canales de telecomunicaciones (acceso a Internet, enlaces de telecomunicaciones) dispongan de respaldos completamente independientes de los principales. Nota: Se recomienda que los canales alternos sean proporcionados por un ISP diferente al proveedor principal. Esto con el fin de garantizar la continuidad del servicio en caso de presentarse una falla en dicho proveedor.	<ul style="list-style-type: none"> <li>● Adquirir e implementar los canales alternos en las sedes principales.</li> <li>● Realizar pruebas de los canales alternos.</li> </ul>	Implementada
	<b>6.2. Data Center Alterno</b>			



	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


TIPO	ALTERNATIVAS DE RECUPERACIÓN	OBJETIVO	RETOS PARA LA ANT	ESTADO
	6.2.1. Canales de replicación entre el Data Center Principal y el Data Center Alterno.	Contar con un canal dedicado para garantizar la replicación de Backups y máquinas virtuales entre el Data Center Principal y el Data Center Alterno.	<ul style="list-style-type: none"> <li>Identificar y seleccionar el ISP que puede proveer dicho servicio.</li> <li>Adquirir e implementar el canal.</li> <li>Realizar pruebas del canal de replicación.</li> </ul>	Pendiente de aprobación
	<b>6.5. Centro Alterno de Operaciones (Oficinas alternas)</b>			
	6.5.1. Canal para el acceso a Internet desde el Centro Alterno de Operaciones.	Contar con acceso a Internet desde el Centro Alterno de Operaciones.	<ul style="list-style-type: none"> <li>Identificar y seleccionar el ISP.</li> <li>Adquirir e implementar un canal alternativo.</li> <li>Realizar pruebas de conexión.</li> </ul>	Pendiente de aprobación
	6.5.2. Canales de comunicación desde el Centro Alterno de Operaciones al Data Center Principal, Data Center Alterno	Contar con canales de comunicación desde el Centro Alterno de Operaciones al Data Center Principal, al Data Center Alterno con el fin de asegurar que los equipos de cómputo ubicados en el Centro Alterno de Operaciones cuenten con los accesos necesarios a los servicios de TI críticos.	<ul style="list-style-type: none"> <li>Identificar y seleccionar el ISP.</li> <li>Adquirir e implementar los canales.</li> <li>Realizar pruebas de conectividad desde el Centro Alterno de Operaciones hacia el Data Center Principal y al Data Center Alterno</li> </ul>	Pendiente de aprobación

Tabla 2. Estrategia de Continuidad

### 3.4. Arquitectura De TI

La Agencia Nacional de Tierras - ANT cuenta con una infraestructura propia en Datacenter Principal de la ANT, así mismo cuenta con servicios tecnológicos desplegados en Azure, a los que se accede mediante una VPN site to site con el Datacenter Principal. Por otra parte, se cuenta con una MPLS que permite la



	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

conexión entre las Sedes Chapinero y Américas ubicadas en Bogotá y las 32 Unidades de Gestión Territorial - UGT con el Datacenter Principal, como se observa a continuación:

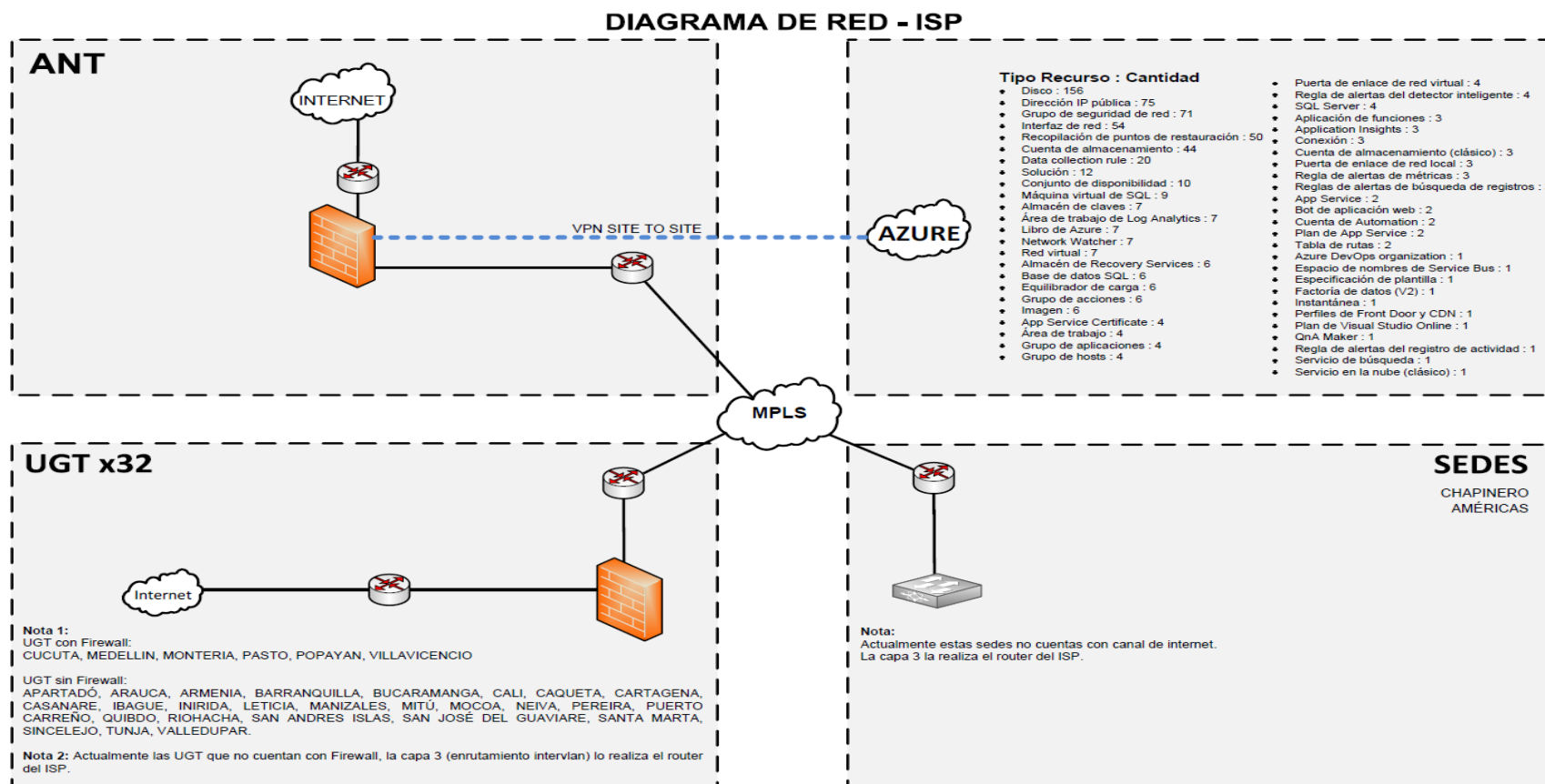



Ilustración 1 Arquitectura tecnológica de la Agencia Nacional de Tierras – ANT3

<sup>3</sup> El diagrama fue facilitado por la ANT donde no se incluye la sede Centro en Bogotá. Para efectos del análisis del DRP / BCP en Bogotá se contemplan las sedes Américas, Chapinero y Centro

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Actualmente en el Datacenter Principal se encuentra ubicado en el Centro de datos HostDime Nebula certificado ICREA V, el cual está ubicado en la Zona Franca de Tocancipá Int 9, Km 1.5 vía Briceño-Zipacquirá, Tocancipá, Cundinamarca.

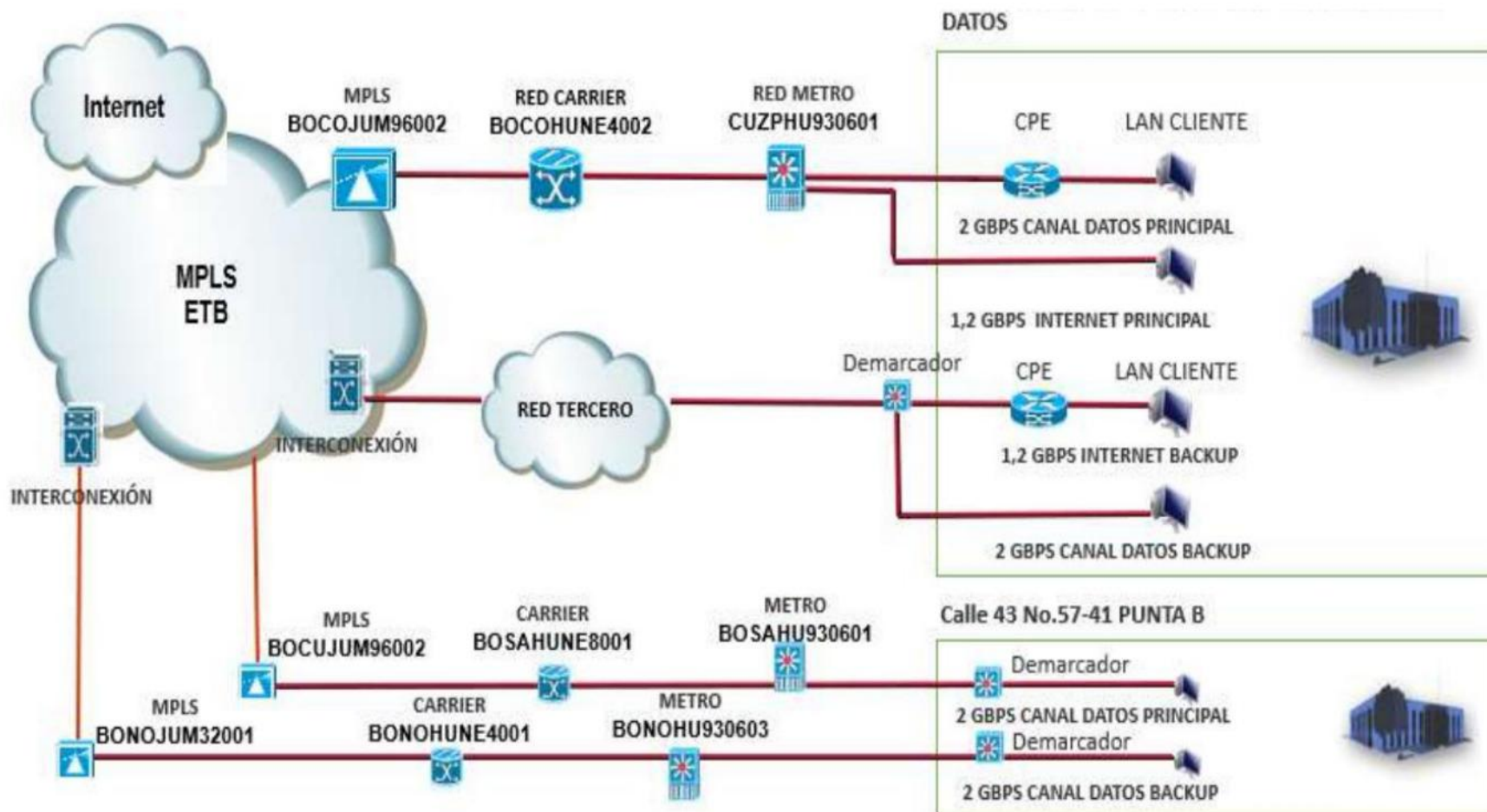




Ilustración 2 Conexiones con Datacenter Principal HostDime Nebula

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


### 3.5. Catálogo De Sistemas De Información

A continuación, se presenta el Catálogo de Sistemas de Información que tiene actualmente el Equipo de Infraestructura y Soporte Tecnológico:


ÍTEM	NOMBRE DE SOLUCIÓN TECNOLÓGICA	DESCRIPCIÓN	MISIONALIDAD	AREA RESPONSABLE	TIPO	TIPO DE DESARROLLO	LICENCIAMIENTO	LENGUAJE
S.1	ORFEO	Aplicativo de gestión documental que permite gestionar la correspondencia interna, entrante y saliente según la TRD definida. Adicionalmente permite gestionar de los expedientes creados desde el SIT.	Apoyo	Proceso de gestión documental de la ANT	Web	Adquirido con modificaciones	Activo	PHP
S.2	KLIC	Aplicativo que permite el registro y cargue de los soportes de las actividades gestionadas mensualmente por cada uno de los contratistas, así mismo permite el seguimiento y VoBo de los supervisores de los contratos.	Apoyo	Radicación de cuentas	Web	Desarrollo interno	Activo	PHP
S.3	MOODLE	Plataforma que permite realizar capacitaciones virtuales de la Agencia	Apoyo	Gestión del conocimiento.	Web	Adquirido con modificaciones	Activo	PHP
S.4	SISTEMA INTEGRADO DE TIERRAS - SIT	Sistema de información, que permite gestionar y procesar de manera articulada y centralizada la información que se genera en la Agencia. Está compuesto por una serie de módulos que soportan aquellos procesos misionales de la ANT, como así mismo aquellos que son transversales.	Misional	Adjudicación de baldíos (Persona Natural, Restitución). Formalización de la propiedad. Proceso RESO. Procesos de asuntos Étnicos (Decretos 1066, 1071 y 2333). Procesos Agrarios.	Web	Desarrollo interno	Activo	.net
S.5	Herramientas para Barrido Predial Masivo - BPM	Sistema que permite recopilar, organizar, administrar, analizar, compartir y distribuir la información alfanumérica y geográfica generada desde la Agencia y sus aliados estratégicos en la oferta de servicios.	Misional	Proceso barrido predial masivo	Aplicación Móvil	Desarrollo interno	Activo	

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

ÍTEM	NOMBRE DE SOLUCIÓN TECNOLÓGICA	DESCRIPCIÓN	MISIONALIDAD	AREA RESPONSABLE	TIPO	TIPO DE DESARROLLO	LICENCIAMIENTO	LENGUAJE
S.6	Sistema Integral Directo de Reforma Agraria - SIDRA	Sistema que permite documentar y validar las actividades para el otorgamiento del subsidio a los potenciales beneficiarios priorizados en el marco de lo establecido en el acuerdo 310 del 2013.	Misional	Subsidio de reforma agraria	Web	Desarrollo Interno	Activo	.net
S.7	BALDÍOS EDP	"Sistema legado del INCODER que permite la consulta de los procesos de adjudicación para (personas naturales y restitución). Para los procesos de EDP el sistema permite la consulta y gestión de los procesos de adjudicación."	Misional	Adjudicación de baldíos:- Persona Natural.- Restitución - EDP	Escritorio	Desarrollo Interno	Activo	
S.8	SIG-Formalización	Herramienta legado del MADR, que apoya el proceso de Formalización de predios del Estado.	Misional	Proceso de formalización	web	Desarrollo externo	Activo	
S.9	Heródoto	Sistema que permite el registro del seguimiento realizados a los expedientes de los procesos que se gestionan en la Dirección de Asuntos Étnicos.	Misional	Proceso de comunidades Indígenas Proceso de comunidades negras. Informe de tierras. Órdenes judiciales	web	Desarrollo interno	Activo	
S.10	Bodega de Datos - DW	Llamada DATA WAREHOUSE, es un conjunto de datos organizados e integrados que sufrieron procesos de Extracción Transformación y Carga (ETL) para su posterior uso, los cuales soportan el proceso de toma de decisiones, está orientada al manejo de grandes volúmenes de información provenientes de diversas fuentes, esto incluye además de la base de datos los cubos de información.	Misional	Procesos misionales de la ANT.	web	Desarrollo interno	Activo	
S.11	SICAZ	Herramienta que permite el registro del análisis realizado a las solicitudes de adjudicación asignadas a la subdirección de acceso a tierras por zonas focalizadas.	Misional	Procesos misionales de la ANT.		Desarrollo interno	Activo	


	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

ÍTEM	NOMBRE DE SOLUCIÓN TECNOLÓGICA	DESCRIPCIÓN	MISIONALIDAD	AREA RESPONSABLE	TIPO	TIPO DE DESARROLLO	LICENCIAMIENTO	LENGUAJE
S.12	Sistema de Alertas y Respuestas Tempranas - SART	Funcionalidad integrada al SIT que permitirá el registro y seguimiento a los conflictos identificados por el equipo de dialogo social.		Procesos misionales de la ANT.				.net
S.13	Centro de Atención y Servicios - CAS	Aplicativo de mesa de servicios que permite gestionar las solicitudes y requerimientos tecnológicos.	Apoyo	Mesa de servicios TI	web	Desarrollo externo	Activo	
S.14	Intranet	Portal interno para colaboradores en plataforma SharePoint	Misional	Gestión de la comunicación	web	Desarrollo interno	Activo	
S.15	PORTAL WEB	Gestor de contenidos para el portal web	Misional	Comunicaciones	web	Adquirido con modificaciones	Activo	
S.16	Heinsohn Nomina Gobierno - HNG	Software para la gestión y liquidación de la nómina de funcionarios	Administrativo, Financiero y de Apoyo	Talento Humano	web	Adquirido con modificaciones	Activo	
S.17	Orquestador	Permite validar, incluir y Calificar de manera automatizada a los sujetos de ordenamiento territorial	Misional	Gestión de tierras	Web	Desarrollo interno	Activo	
S.18	Módulo de Información Geográfica para el Ordenamiento - MIGO	Aplicativo que permite la gestión de información geográfica de la ANT	Misional	Procesos misionales de la ANT.	Web	Desarrollo interno	Activo	
S.19	Instrumentos para el Ordenamiento Social de la Propiedad Rural	Conjunto de herramientas (Toolbox) de ArcGIS Pro, para la elaboración, levantamiento, análisis y procesamiento de información geográfica, entre otros, que son utilizadas en los sistemas de información existentes o como enlaces independientes para la elaboración de encuestas, tableros de control, visores geográficos, entre otros.	Misional	Procesos misionales de la ANT.	Escritorio	Desarrollo interno	Activo	
S.20	Banco de Imágenes	Herramienta de apoyo para los profesionales de la entidad que requieran visualizar las imágenes disponibles para el cumplimiento de las	Misional	Procesos misionales de la ANT.	Web	Desarrollo interno	Activo	

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

ÍTEM	NOMBRE DE SOLUCIÓN TECNOLÓGICA	DESCRIPCIÓN	MISIONALIDA D	AREA RESPONSABLE	TIPO	TIPO DE DESARROLLO	LICENCI AMIENT O	LENGUAJE
		misionalidades y las metas establecidas en las diversas áreas.						


*Tabla 3. Catálogo de Sistemas de Información*

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 3.6. Resultados De Análisis De Impacto Al Negocio

A continuación se presenta la secuencia de recuperación por dependencias, resultado del Análisis de Impacto al Negocio en la ANT:

Nombre de la dependencia:	RTO (Horas)	RPO (Días)	MTPD (Días)	Impacto Financiero	Impacto Operacional / Misional	Impacto a Beneficiarios	Impacto Cumplimiento	Impacto Reputacional	Impacto Información / Datos
410 - Subdirección de Acceso a Tierras en Zonas Focalizadas	4	7	1	4,05	4,05	4,65	4,65	4,65	4,3
600 - Secretaría general - Equipo de Infraestructura y Soporte Tecnológico	4	1	2	1,9	5	5	3,6	5	3,45
103 - Oficina Jurídica	4	30	2	3,65	3,65	3,65	3,65	3,65	3,65
220 - Subdirección de Sistemas de Información de Tierras	4	0,25	2	1,9	2,9	2,65	2,65	2,3	2,45
620 - Subdirección Administrativa y Financiera	6	1	1	4,55	4,3	4,3	4,3	4,3	4,55
420 - Subdirección de Acceso a Tierras por Demanda y Descongestión	6	1	1	3	4,05	4,05	4,05	4,05	4,05
101 - Oficina de Planeación	6	7	2	1,85	3,6	3,6	3,6	3,6	3,6
600 - Secretaría general	6	0,5	2	3,25	3,25	3,25	3,25	3,25	3,25
104 - Oficina del Inspector de la Gestión de Tierras	6	7	2	2,05	2,9	2,9	2,9	2,9	2,9
620 - Subdirección Administrativa y Financiera – Tesorería	6	0,5	2	3,1	1,05	2,65	2,65	2,65	1,9
400 - Dirección de Acceso a Tierras	6	7	2	2,65	3,6	3,55	3,6	2,2	2,4
610 - Subdirección de Talento Humano	6	1	3	3,45	3,45	3,45	3,45	3,45	3,45
320 - Subdirección de Procesos Agrarios y Gestión Jurídica - SPA	6	1	3	1,1	2,7	2,25	2,45	2,45	2,7
601 - Coordinación para la Gestión Contractual	6	1	3	2,3	3,25	2,3	3,25	2,3	5
300 - Dirección de Gestión Jurídica de Tierras - DGJT	6	1	3	4,4	3,45	1,65	2,45	1,45	3,45

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS					CÓDIGO	INTI-Plan-006	
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO					VERSIÓN	1	
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN					FECHA	31/12/2025	

620 - Subdirección Administrativa y Financiera – Gestión Documental	8	1	3	2,25	2,25	2,25	2,65	2,65	2,1
210 - Subdirección de Planeación Operativa	8	1	3	1,65	3,1	3,1	3,1	2,25	1,9
430 - Subdirección de Administración de Tierras de la Nación	8	15	3	2,25	2,25	2,25	2,25	2,25	2,25
102 - Oficina de Control Interno	24	1	3	4,05	4,05	4,05	4,05	4,05	4,05
200 - Dirección de Gestión del Ordenamiento Social de la Propiedad - DOSPR	48	0,25	3	1,45	1,45	1,25	1,25	1,25	1,25

*Tabla 4. Secuencia de recuperación calculada*

#### 4. ALCANCE DEL DRP

A continuación, se relacionan los sistemas de información y servicios de TI incluidos en este plan de recuperación de desastres tecnológicos, según el análisis de impacto al negocio realizado:


##### 4.1. Controles Seguridad Física Y Servicios De Soporte En Data Center

- Controles de acceso.
- CCTV.
- Sistema de aire acondicionado.
- Sistema contra incendios.
- UPS y plantas eléctricas.
- Red eléctrica regulada.

##### 4.2. Seguridad Informática

- Balanceador de aplicaciones.
- Firewall perimetrales en sedes: Montería, Cúcuta, Medellín, Pasto, Popayán, Villavicencio.
- Firewall perimetral en Datacenter Principal de la ANT.
- Concentrador de VPNs.
- Firewall de Aplicaciones.
- Solución de Control de Acceso a la Red.
- Protección contra ataques de Denegación de Servicio Distribuido.
- Solución para el análisis de tráfico, inteligencia de amenazas y evaluación de la postura de seguridad.
- Solución para la protección proactiva avanzada frente amenazas.
- Solución Antivirus.



	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

- Solución de correlación de eventos integrada con las soluciones de seguridad existentes.

#### 4.3. Servicios De TI


- Conectividad y canales de comunicación.
- Soluciones de seguridad informática.
- Acceso a internet.
- Carpetas compartidas y repositorios locales de la Entidad.
- Correo - Office 365
- One Drive - Office 365
- SharePoint - Office 365
- Teams - Office 365
- Sharepoint
- Ofimática – paquete de Microsoft Office
- VPNs – client to site y site to site.
- Portal web de la Agencia Nacional de Tierras - ANT.
- Infraestructura (hardware): soluciones de almacenamiento, Hypervisores, dispositivos de red, etc.
- Plataforma de virtualización. VMware.
- Motores de base de datos - Azure database, SQL Server, Postgress, Oracle
- Veeambackup - backup de servidores onpremise
- Aruba central - administrador de switches a nivel nacional wlan lesslan
- Sabbix - monitoreo de infraestructura - Moderado
- Redes Wifi
- Intranet

#### 4.4. Sistemas De Información Y Aplicaciones

A continuación, se relacionan los sistemas de información y aplicaciones en los que debe enfocarse el esfuerzo, en caso de la materialización de un escenario de interrupción total, por su apoyo a procesos críticos que fueron priorizados según el análisis de impacto al negocio BIA4.


Nombre de la dependencia:	RTO (Horas)	RPO (Días)	MTPD (Días)	Sistemas de Información / Aplicaciones
410 - Subdirección de Acceso a Tierras en Zonas Focalizadas	4	7	1	<ul style="list-style-type: none"> <li>• Módulo de Información Geográfica para el Ordenamiento - MIGO</li> <li>• Herramientas para Barrido Predial Masivo - BPM - SIP</li> <li>• Sistema Integrado De Tierras - SIT</li> <li>• ORFEO</li> <li>• KLIC</li> <li>• BALDÍOS EDP</li> <li>• Orquestador - Registro de Sujetos de Ordenamiento - RESO</li> <li>• Instrumentos para el Ordenamiento Social de la Propiedad Rural</li> <li>• Sistema de Alertas y Respuestas Tempranas - SART</li> </ul>

<sup>4</sup> Ver Informe de Análisis de Impacto al Negocio

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLÓGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

Nombre de la dependencia:	RTO (Horas)	RPO (Días)	MTPD (Días)	Sistemas de Información / Aplicaciones
600 - Secretaría general - Equipo de Infraestructura y Soporte Tecnológico	4	1	2	Power BI y Reporting Services
103 - Oficina Jurídica	4	30	2	Contempladas anteriormente
220 - Subdirección de Sistemas de Información de Tierras	4	0,25	2	Contempladas anteriormente
620 - Subdirección Administrativa y Financiera	6	1	1	Centro de Atención y Servicios – CAS. Acceso a Internet.
420 - Subdirección de Acceso a Tierras por Demanda y Descongestión	6	1	1	Contempladas anteriormente
101 - Oficina de Planeación	6	7	2	Contempladas anteriormente
600 - Secretaría general	6	0,5	2	<ul style="list-style-type: none"> <li>• CRM</li> <li>• PIIP</li> <li>• Acceso a Internet.</li> </ul>
104 - Oficina del Inspector de la Gestión de Tierras	6	7	2	Contempladas anteriormente
620 - Subdirección Administrativa y Financiera – Tesorería	6	0,5	2	Contempladas anteriormente. Acceso a Internet.
400 - Dirección de Acceso a Tierras	6	7	2	Contempladas anteriormente. Acceso a Internet.
610 - Subdirección de Talento Humano	6	1	3	Heinsohn Nomina Gobierno - HNG
320 - Subdirección de Procesos Agrarios y Gestión Jurídica - SPA	6	1	3	Base de datos procesos agrarios (MATRIZ INTERNA EXCEL) Base de datos SU-288 (MATRIZ INTERNA EXCEL)
601 - Coordinación para la Gestión Contractual	6	1	3	Contempladas anteriormente. Acceso a Internet.
300 - Dirección de Gestión Jurídica de Tierras - DGJT	6	1	3	ArcGIS
620 - Subdirección Administrativa y Financiera – Gestión Documental	8	1	3	Contempladas anteriormente.
210 - Subdirección de Planeación Operativa	8	1	3	Aplicativo FILI Power BI
430 - Subdirección de Administración de Tierras de la Nación	8	15	3	ArcGIS Online
102 - Oficina de Control Interno	24	1	3	Contempladas anteriormente
200 - Dirección de Gestión del Ordenamiento Social de la Propiedad - DOSPR	48	0,25	3	Contempladas anteriormente

Tabla 5 Secuencia de Recuperación Tecnológica

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

#### **4.5. PREMISAS Y LIMITACIONES**


Para que este plan funcione, se deben cumplir las siguientes condiciones:

- Se debe contar con los recursos mínimos necesarios para el desarrollo de las funciones del Equipo de Infraestructura y Soporte Tecnológico de acuerdo con el alcance relacionado en el numeral 4 de este documento, entre los que se destacan: Hardware, software, personal mínimo, proveedores, suministros e información.
- Los funcionarios del Equipo de Infraestructura y Soporte Tecnológico de la Agencia Nacional de Tierras - ANT deben tener acceso a internet y las plataformas tecnológicas para dar inicio al Plan de Recuperación de Desastres Tecnológicos, bien sea que hayan sido trasladados a un sitio alternativo o estén conectados de forma remota.
- En caso de que se genere una contingencia, se debe contar con la disponibilidad de al menos un profesional por cada función del Equipo de Infraestructura y Soporte Tecnológico.
- Se cuenta con respaldo de datos localizados en una instalación diferente al Datacenter Principal y se encuentran actualizados.
- Los servicios de TI críticos a recuperar son los relacionados en el numeral 4 de este documento.
- El Datacenter Alternativo se encuentra disponible para dar inicio al Plan de Recuperación de Desastres Tecnológicos.
- Se cuenta con canales de comunicación entre el Datacenter Alternativo, y los usuarios ubicados en las Sedes Chapinero y Américas ubicadas en Bogotá y las 32 Unidades de Gestión Territorial – UGT.

#### **Exclusiones**

Este plan excluye lo siguiente:

- La pérdida de datos en computadores de usuario final, no almacenados en los servicios de Office 365.
- La recuperación de servicios de TI en el Datacenter Alternativo, diferentes a los definidos en el numeral 4 de este documento.
- Garantizar la continuidad de los servicios tecnológicos en escenarios de desastre diferentes a los analizados en el numeral 3.2 de este documento.


 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

## 5. GOBIERNO DEL PLAN DE RECUPERACIÓN DE DESASTRES

### 5.1. Política

A continuación, se presenta la política que deberá cumplirse para garantizar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Plan de Recuperación de Desastres Tecnológicos – DRP en la Agencia Nacional de Tierras - ANT:

- La Subdirección De Sistemas De Información De Tierras reconoce que el DRP le ayuda a recuperarse de desastres que interrumpan los servicios de TI misionales, por tanto, velará por los recursos necesarios para garantizar la sostenibilidad de dicho plan.
- Las tareas definidas en las fases preventiva, respuesta y restauración definidas en el DRP, deben hacer parte del manual de funciones de los responsables.
- Todo el personal del Equipo de Infraestructura y Soporte Tecnológico que tenga responsabilidades en el Plan de Recuperación de Desastres Tecnológicos – DRP en la Agencia Nacional de Tierras – ANT, deberá estar entrenado y capacitado en los procedimientos que lo conforman, así como conocer claramente sus roles y responsabilidades durante las fases del plan.
- El DRP deberá ser revisado y probado anualmente para garantizar su efectividad en la mitigación de los escenarios de desastre planteados en el numeral 2.4.
- Las pruebas al DRP deben ser acordadas con las áreas y terceros requeridos para las mismas.
- El Líder del DRP es responsable por la actualización constante de este documento y sus anexos.
- El DRP, así como los planes y procedimientos que hacen parte de él, deberán ser revisados anualmente o cuando se presenten cambios importantes en los procesos misionales.
- Se debe contar con una copia del Plan de Recuperación de Desastres Tecnológicos – DRP y sus correspondientes anexos en una ubicación diferente al Datacenter Principal y a los servicios de Azure que hacen parte de la operación normal.

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

## 5.2. Roles y Responsabilidades

A continuación, se presentan los equipos que hacen parte del Plan de Recuperación de Desastres Tecnológicos, los cuales están conformados por el personal clave necesario para la activación, recuperación y retorno a la normalidad de los sistemas de información, aplicaciones y servicios de TI de la Agencia Nacional de Tierras - ANT. Cada equipo tiene asignadas funciones y procedimientos a desarrollar en distintas fases del DRP.

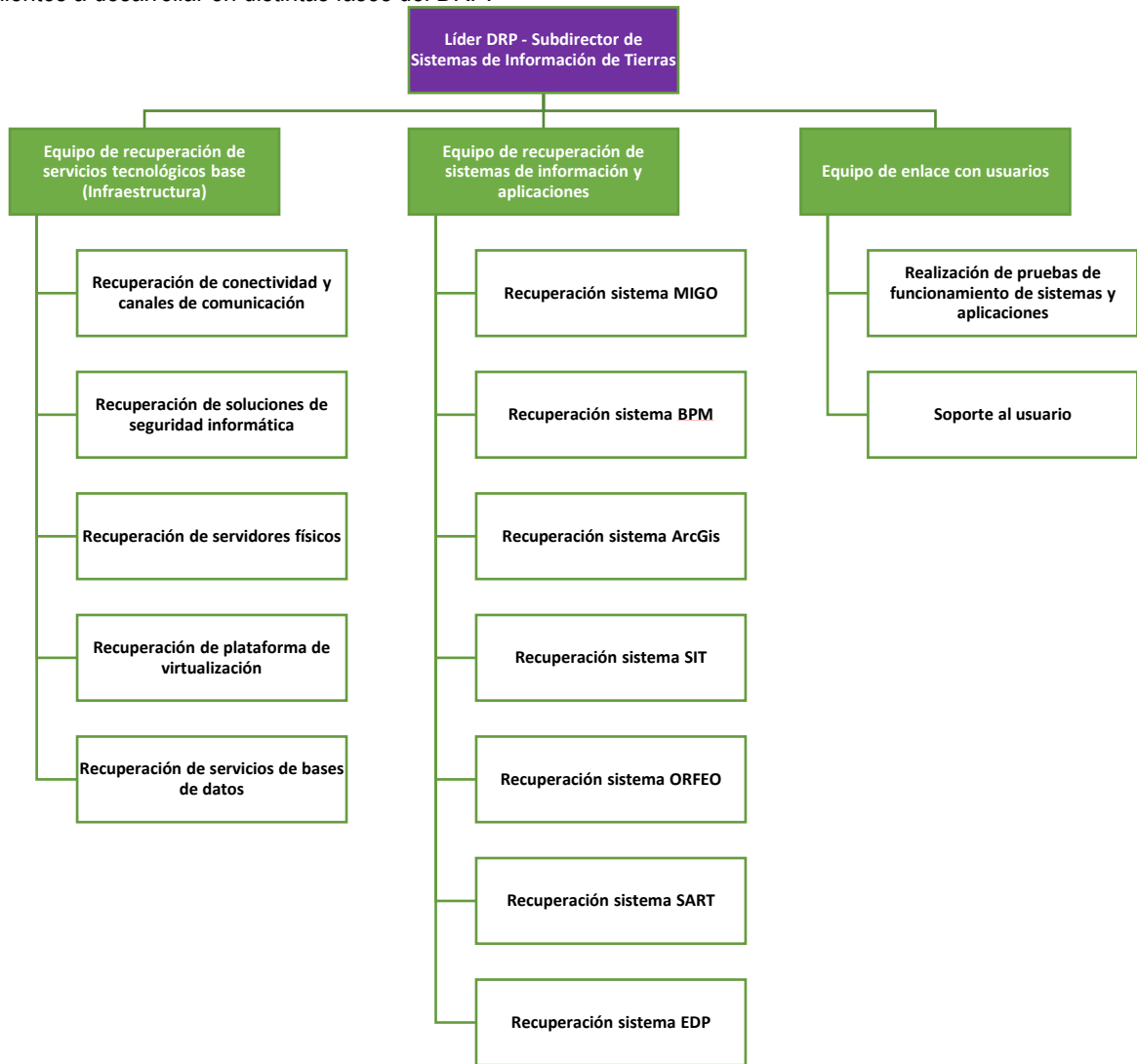



Ilustración 3 Equipos del DRP

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

### 5.2.1. Líder DRP

El líder del DRP es el Subdirector de Sistemas de Información de Tierras. Las responsabilidades del Líder del DRP son:

- Declarar la activación del Plan de Recuperación de Desastres Tecnológicos.
- Declarar la puesta en funcionamiento de los sistemas de información y aplicaciones que hacen parte del alcance del DRP.
- Declarar el fin de las operaciones en contingencia.
- Coordinar el retorno a la normalidad.

### 5.2.2. Equipo de recuperación de servicios tecnológicos base


Las responsabilidades de este equipo son:

- Recuperar la conectividad y la operación de los canales de comunicación.
- Recuperar las soluciones de seguridad informática.
- Recuperar el funcionamiento de los servidores físicos (Nodos de virtualización).
- Recuperar el funcionamiento de las bases de datos.
- Recuperar el funcionamiento de la plataforma de virtualización.
- Recuperar el funcionamiento de las máquinas virtuales que soportan los sistemas de información y las aplicaciones críticas.
- Informar los eventos importantes al Líder de DRP.

### 5.2.3. Equipo de recuperación de sistemas de información y aplicaciones

Las responsabilidades de este equipo son:

- Recuperación de sistemas de información y aplicaciones críticas:
  - Módulo de Información Geográfica para el Ordenamiento - MIGO
  - Herramientas para Barrido Predial Masivo - BPM - SIP
  - Sistema Integrado De Tierras - SIT
  - ORFEO
  - KLIC
  - BALDÍOS EDP
  - Orquestador - Registro de Sujetos de Ordenamiento - RESO
  - Instrumentos para el Ordenamiento Social de la Propiedad Rural
  - Sistema de Alertas y Respuestas Tempranas – SART
  - Power BI y Reporting Services
  - Centro de Atención y Servicios – CAS. Acceso a Internet.
  - CRM
  - PIIP
  - Heinsohn Nomina Gobierno – HNG
  - ArcGIS


 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

- Aplicativo FILI
- b. Comunicar cualquier incidente con los sistemas de información y aplicaciones.
- c. Dar solución a incidentes en los sistemas.
- d. Visto bueno para realización de pruebas.
- e. Informar los eventos importantes al Líder de DRP.

#### **5.2.4. Equipo de enlace con usuarios y proveedores**

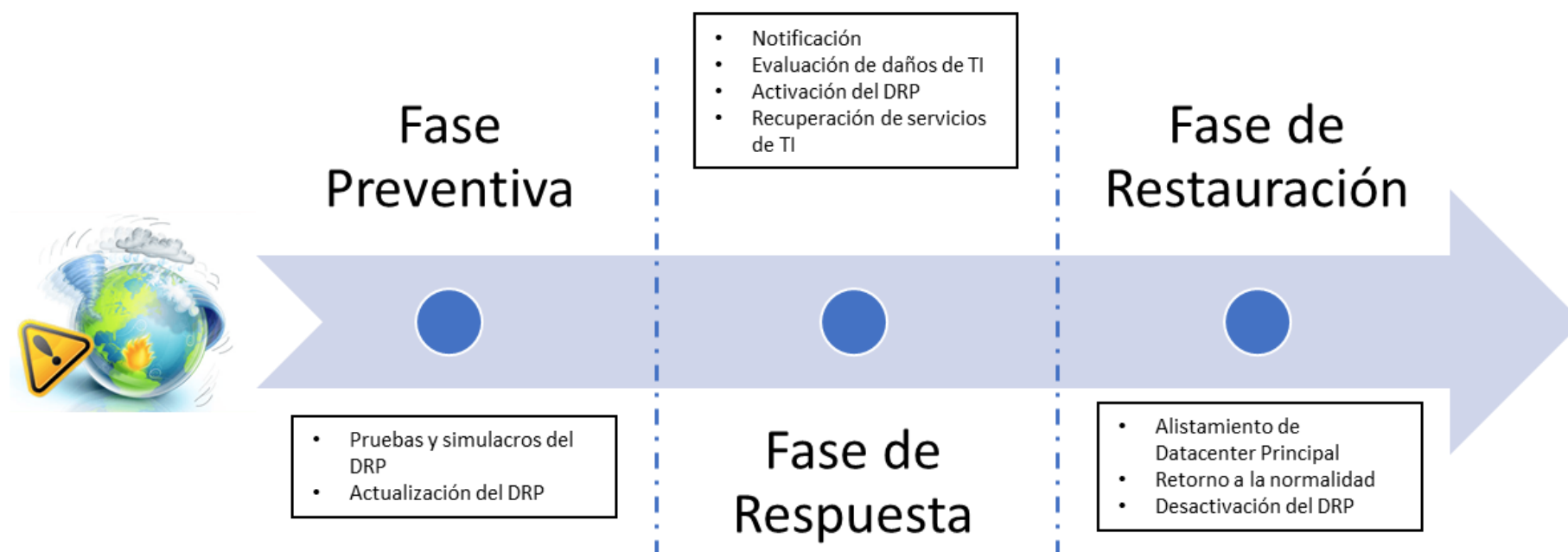
Las responsabilidades de este equipo son:

- a. Hacer el acompañamiento a los usuarios durante las pruebas de funcionamiento de sistemas y aplicaciones.
- b. Notificar cualquier falla al equipo de recuperación de servicios tecnológicos base y al equipo de recuperación de sistemas de información y aplicaciones.
- c. Coordinar el soporte a usuarios durante la recuperación.
- d. Informar los eventos importantes al Líder de DRP.

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025


## 6. PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS

El Plan de Recuperación de Desastres Tecnológicos se desarrolló para recuperar y restaurar los sistemas de información y servicios tecnológicos críticos de la Agencia Nacional de Tierras - ANT, usando un enfoque de tres fases: fase preventiva, fase de respuesta y fase de restauración, los cuales se desarrollan en los siguientes numerales.



*Ilustración 4 Fases del DRP*



	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 6.1. FASE PREVENTIVA


Son todas las tareas diarias que se realizan para prevenir la pérdida de información, y fallas relacionadas con los sistemas de información, aplicaciones o servicios de TI críticos, de la Agencia Nacional de Tierras - ANT:

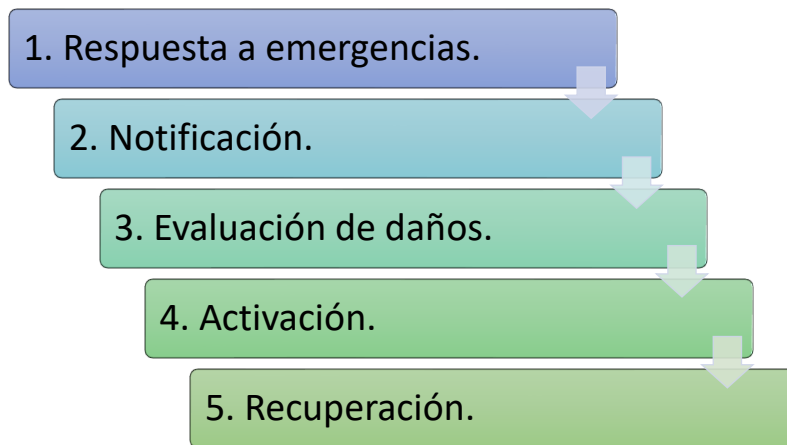
Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Realizar pruebas y simulacros del DRP	Planear y realizar pruebas y simulacros de funcionamiento del Datacenter Alterno en Nube	<ul style="list-style-type: none"> <li>Diseño de pruebas</li> <li>Informe de pruebas realizadas</li> </ul>	Líder del DRP
2.	Actualizar información de contacto de los funcionarios y terceros con responsabilidad en el DRP.	Con motivo de las pruebas y auditorías del DRP se debe verificar la actualización de los datos de contacto del personal y terceros con responsabilidad en el DRP.	Hoja Excel con información de contacto de los miembros de los equipos de recuperación.	Líder del DRP
3.	Actualizar los planes y procedimientos del DRP	Con base en los resultados de las pruebas y ejercicios, el control de cambios y los informes de auditoría, se deben actualizar los planes y procedimientos del DRP: Cambios en servicios, tecnología, proveedores, entre otros.	Planes y procedimientos de recuperación documentados	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
4.	Actualizar el inventario de activos	Mantener un inventario actualizado de la infraestructura tecnológica tanto en los Datacenters, como de las contingencias definidas y verificar la actualización de cambios que se presenten: Nuevos dispositivos, dispositivos retirados, ampliación de canales, almacenamiento, entre otros.	Archivo Excel con el inventario de activos en los Datacenters	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
5.	Revisar informes de monitoreo de la plataforma en los Datacenters	Revisar los informes diario, semanal y mensual de monitoreo de disponibilidad de los servicios de la infraestructura en los Datacenters.	Reportes de Monitoreo de los Datacenters	Líder del DRP
6.	Ejecutar auditorías internas al DRP	Coordinar la ejecución de auditorías periódicas al DRP.	Procedimiento de Auditoría al DRP	Líder del DRP

*Tabla 6 Actividades de la fase preventiva*

### 6.2. FASE DE RESPUESTA

Involucra las tareas que se deben llevar a cabo una vez se ha materializado un desastre, el cual comprende las siguientes etapas:

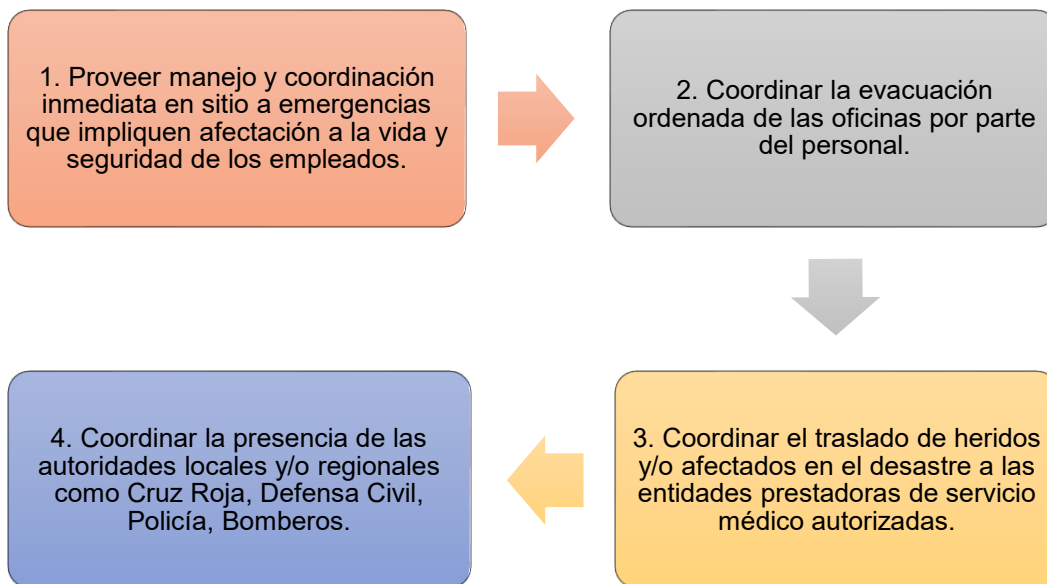
	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025




*Ilustración 5 Etapas de respuesta*

#### 6.1.1. Procedimiento de respuesta a emergencias

Una vez se ha materializado un desastre, se deberá proteger en su orden: la vida humana, la información, la infraestructura tecnológica y las instalaciones físicas de la Entidad. A continuación, el procedimiento general que debe seguir la Brigada de Emergencias:



*Ilustración 6 Actividades en la respuesta a emergencias*

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 6.1.2. Procedimiento de notificación

El proceso de notificación se debe llevar a cabo, una vez se ha presentado un evento que amenaza con producir una interrupción prolongada de los procesos y/o servicios de tecnología en la Agencia Nacional de Tierras – ANT, esto con el fin de notificar la situación presentada y controlar su avance de tal manera que una persona realice y controle máximo tres contactos y reporte al Comité de Crisis. Esto permitirá que en poco tiempo las partes interesadas estén al tanto de la situación presentada.

A continuación, se presentan los datos de contacto para llevar a cabo el proceso de notificación en caso de un desastre que afecte la operación de la infraestructura, sistemas de información, aplicaciones y servicios de TI críticos de la entidad.


#### Contactos Internos

No.	Rol	Nombre	Contacto
1.	Responsable de Servidores	Jhon Camacho	3102909862
2.	Responsable de Bases de Datos	Jhovanny Sierra	3157810730
3.	Responsable de Redes	Juan Espinosa	3008905111
4.	Responsable de Aplicaciones	Samara Castiblanco	3187171896
5.	Responsable de Mesa de Ayuda	Irma Cuello	3108063507
6.	Líder de Infraestructura	Roberto Zabala	3012716213

Tabla 7 Datos de contacto internos del DRP

#### Contactos de Terceros o Proveedores


Producto / Servicio	Proveedor / Empresa	Nombre de Contacto	Correo Contacto	Estado del contrato	Observaciones
Adobe Acrobat Pro Y Creative Cloud	Megacad Ingeniería Y Sistemas S.A.S	Megacad	<a href="mailto:megacad@megacad.com.co">megacad@megacad.com.co</a>	Vigente	La administración y asignación de licencias se realiza desde la plataforma Admin Console de Adobe.
Antivirus Bitdefender	Star Solutions Ti	Star Solutions TI	<a href="mailto:daniloborges@star-ti.com">daniloborges@star-ti.com</a> <a href="mailto:diegovasquez@star-ti.com">diegovasquez@star-ti.com</a>	Vigente	Contrato hasta el 17 Diciembre 2026
Aranda					N/A
Microsoft Azure	Controles Empresariales	Lina Perdomo	<a href="mailto:lperdomo@coem.co">lperdomo@coem.co</a>		Suscripción activa - Todos los casos relacionados con soporte de MS se gestionan desde la plataforma
Conectividad - Mpls, Internet, Internet Móvil	ETB	Helpdesk ETB	<a href="mailto:helpdesketb@etb.com.co">helpdesketb@etb.com.co</a>	Vigente	N/A
Desktop Escritorio Y Monitores	Tecnophone Colombia S.A. - Portátiles				N/A

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Producto / Servicio	Proveedor / Empresa	Nombre de Contacto	Correo Contacto	Estado del contrato	Observaciones
	Nueva Era Soluciones S.A.S - Monitores Y Desktop Escritorio				N/A
Fortinet - Equipos De Seguridad	Unión Temporal Seguridad ANT Datasec Wexler 2024	HelpDesk - DATASEC	<a href="mailto:soporte@datasec.com.co">soporte@datasec.com.co</a>	Vigente	Vigente hasta el 2027
Impresoras Y Escáneres	Gran Imagen	Geydis Vargas	<a href="mailto:comercialcorp@granimagen.com">comercialcorp@granimagen.com</a>	Vigente	N/A
Microsoft - Suite De Productividad, Licenciamientos De Servidores	Software One	Claudia Martínez	<a href="mailto:claudia.martinez@softwareone.com">claudia.martinez@softwareone.com</a>		Vigencia Licencias 28 de feb. 2025 - Todos los casos relacionados con soporte de MS se gestionan desde la plataforma
Aires Acondicionados	Apicom	Carolina Echeverria	<a href="mailto:carolina.echeverria@apicom.com.co">carolina.echeverria@apicom.com.co</a>	Vigente	Contrato de mantenimiento vigente hasta el 31 de Diciembre
UPS	N/A	N/A	N/A	N/A	Actualmente las UPS son de responsabilidad de la ADR.
Switches Y Access Point	Sanolivar	Gina Olivares	<a href="mailto:gina.olivares@sanolivar.co">gina.olivares@sanolivar.co</a>	Vigente	N/A
Certicámara - Certificados Digitales	Sociedad Cameral De Certificacion Digital Certicamara S.A.	Carolina Giraldo Bustamante	<a href="mailto:carolina.giraldo@certicamara.com">carolina.giraldo@certicamara.com</a>	No vigente	Actualmente no se tiene contrato con CERTICAMARA pero los certificados aún están vigentes.
Hiperconvergencia	Colsof S.A.S	Jhony Guerrero	<a href="mailto:jguerrero@colsof.com.co">jguerrero@colsof.com.co</a>	Vigente	N/A
Almacenamiento Dell San	Redcomputo	Jairo Landazábal	<a href="mailto:jlandazabal@redcomputo.com.co">jlandazabal@redcomputo.com.co</a>	Vigente	N/A
Almacenamiento NAS	Redcomputo	Jairo Landazábal	<a href="mailto:jlandazabal@redcomputo.com.co">jlandazabal@redcomputo.com.co</a>	Vigente	N/A
Pantallas Interactivas	Claryicon S.A.S	Fredy Orjuela	<a href="mailto:fredy.orjuela@claryicon.com">fredy.orjuela@claryicon.com</a>	Vigente	N/A
Video Proyector	Claryicon S.A.S	Fredy Orjuela	<a href="mailto:fredy.orjuela@claryicon.com">fredy.orjuela@claryicon.com</a>	Vigente	N/A

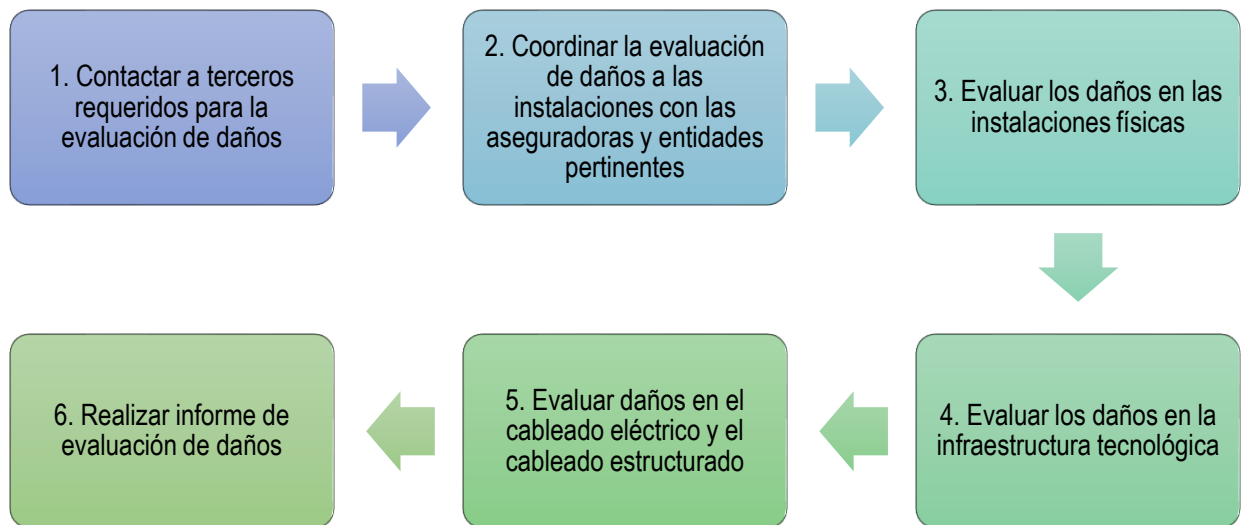
Tabla 8 Datos de contacto externos del DRP

Sin embargo, en esta etapa también se debe notificar el estado de las actividades de recuperación a los miembros del Comité de Crisis (Comité Institucional de Gestión y Desempeño).


 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

### 6.1.3. Procedimiento de evaluación de daños

El equipo de evaluación de daños y recuperación de instalaciones deberá realizar la valoración de los daños con base en el formato de reporte de daños y presentarlo al Comité de Crisis, quienes con base en esta información determinarán si se hace necesario activar el Plan de Continuidad del Negocio y/o el Plan de Recuperación de Desastres.

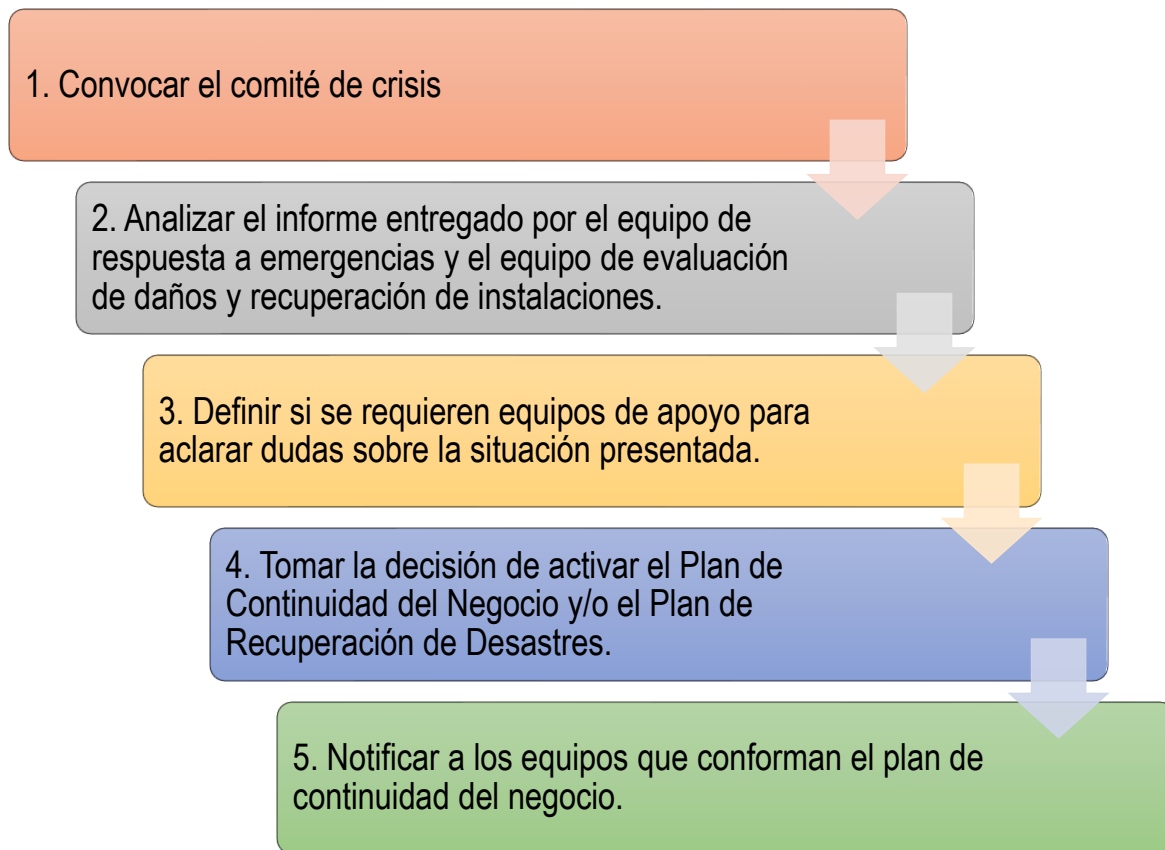


*Ilustración 7 Actividades de la evaluación de daños*

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

#### 6.1.4. Procedimiento de activación

La activación del Plan de Continuidad del Negocio y/o el Plan de Recuperación de Desastres, es una decisión que toma el Comité de Crisis a partir de los informes entregados por el equipo de respuesta a emergencias y el equipo de evaluación de daños y recuperación de instalaciones.




*Ilustración 8 Activación del BCP o DRP*


#### 6.1.5. Procedimiento de recuperación de la infraestructura tecnológica

Una vez cumplidas las etapas de notificación, evaluación de daños y activación se deberán ejecutar, los procedimientos establecidos para la recuperación de la plataforma tecnológica más crítica contemplada en el alcance de este documento:

Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Activar el Datacenter Alterno en Nube	Notificar a los responsables de las contingencias la decisión de activar el DRP.	Datos de contacto, teléfonos fijos y celulares.	Líder del DRP.

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
2.	Activar el Centro Alterno de Operaciones o la estrategia de trabajo remoto.	Notificar la decisión de activar el Centro Alterno de Operaciones o la estrategia de trabajo remoto.	Árbol de llamadas, teléfonos fijos y celulares.	Líder del DRP
3.	Trasladar al personal al Centro Alterno de Operaciones o desplazarse a los sitios autorizados para trabajo remoto.	Coordinar el traslado de los equipos del DRP al Centro Alterno de Operaciones.	Lista de personal de los equipos del DRP	Líder del DRP
4.	Iniciar la ejecución de los procedimientos de recuperación de los servicios de TI base	<ul style="list-style-type: none"> <li>Recuperación de conectividad y canales de comunicación.</li> <li>Recuperación de soluciones de seguridad informática.</li> <li>Recuperación de servidores físicos.</li> <li>Recuperación de plataforma de virtualización.</li> <li>Recuperación de máquinas virtuales.</li> </ul>	Procedimientos de recuperación de los servicios de TI base	Equipo de recuperación de servicios tecnológicos base (Infraestructura)
5.	Iniciar la ejecución de los procedimientos de recuperación de los sistemas de información y las aplicaciones críticas	<p>Recuperación de bases de datos y sistemas de información contempladas en el alcance del DRP.</p> <ul style="list-style-type: none"> <li>Módulo de Información Geográfica para el Ordenamiento - MIGO</li> <li>Herramientas para Barrido Predial Masivo - BPM - SIP</li> <li>Sistema Integrado De Tierras - SIT</li> <li>ORFEO</li> <li>KLIC</li> <li>BALDÍOS EDP</li> <li>Orquestador - Registro de Sujetos de Ordenamiento - RESO</li> <li>Instrumentos para el Ordenamiento Social de la Propiedad Rural</li> <li>Sistema de Alertas y Respuestas Tempranas – SART</li> <li>Power BI y Reporting Services</li> <li>Centro de Atención y Servicios – CAS. Acceso a Internet.</li> <li>CRM</li> <li>PIIP</li> <li>Heinsohn Nomina Gobierno – HNG</li> <li>ArcGIS</li> <li>Aplicativo FILI</li> <li></li> </ul>	<ul style="list-style-type: none"> <li>Procedimientos de recuperación de los sistemas de información y las aplicaciones.</li> <li>Secuencia de recuperación tecnológica.</li> </ul>	Equipo de recuperación de sistemas de información y aplicaciones
6.	Hacer seguimiento a la recuperación de los servicios de TI	Hacer seguimiento a la recuperación de los servicios de TI según la secuencia definida y reportar el estado al Líder del DRP	Árbol de llamadas, teléfonos fijos y celulares.	Líder del DRP

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
7.	Hacer pruebas básicas de los servicios de TI	Hacer pruebas de los servicios de TI a medida que se van recuperando.	Usuarios de prueba	Equipo de enlace con usuarios y proveedores (Infraestructura, seguridad, redes y sistemas de información)
8.	Notificación de recuperación de servicios de TI	Notificar a los funcionarios la puesta en funcionamiento de los servicios de TI.	Usuarios de producción	Equipo de enlace con usuarios y proveedores (Infraestructura, seguridad, redes y sistemas de información)
9.	Garantizar el acceso a los usuarios autorizados	Garantizar que los usuarios autorizados tengan acceso a los servicios TI recuperados.	<ul style="list-style-type: none"> <li>• VPNs</li> <li>• Recursos compartidos</li> <li>• Acceso remoto.</li> <li>• Usuarios de producción</li> </ul>	Equipo de enlace con usuarios y proveedores (Infraestructura, seguridad, redes y sistemas de información)
10.	Monitorear los servicios de TI	Monitorear el desempeño de los servicios de TI recuperados.	<ul style="list-style-type: none"> <li>• Software de monitoreo de redes</li> <li>• Usuarios de producción</li> </ul>	<ul style="list-style-type: none"> <li>• Equipo de recuperación de servicios tecnológicos base (Infraestructura)</li> <li>• Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>

*Tabla 9 Procedimiento de recuperación de la infraestructura tecnológica*

### 6.3. FASE DE RESTAURACIÓN


En paralelo a la fase de recuperación se deberá considerar la reparación o sustitución del Datacenter Principal, con el fin de que una vez hayan sido restauradas las instalaciones físicas, se adelanten las actividades requeridas para el retorno a las operaciones desde el sitio principal.

#### 6.3.1. Procedimiento de alistamiento de instalaciones

A continuación, el proceso para realizar la adecuación de las instalaciones físicas:


Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Dotación del Datacenter Principal	Con base en el reporte de evaluación de daños el proveedor debe tomar la decisión de compra o arriendo de servidores, dispositivos de almacenamiento, comunicaciones, seguridad.	Reporte de evaluación de daños, cotizaciones de terceros.	<ul style="list-style-type: none"> <li>• Líder del DRP</li> <li>• Equipo de recuperación de servicios tecnológicos base</li> <li>• Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>



	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
2.	Inspección de la infraestructura física	Se realiza la revisión de las obras físicas y se firma la aceptación de estas. Se deben revisar: Muros, bajantes, acometidas eléctricas, ductos de aire y otros elementos físicos del Datacenter Principal	<ul style="list-style-type: none"> <li>Norma ANSI/TIA-942</li> <li>Archivo de Excel con la lista de chequeo de evaluación.</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> </ul>
3.	Evaluación del cableado estructurado	Se determina la funcionalidad de: <ul style="list-style-type: none"> <li>Red local.</li> <li>Canales de internet del Datacenter Principal.</li> <li>Canales WAN.</li> <li>Canales de replicación hacia el Datacenter Alternativo en Nube.</li> <li>Soluciones de seguridad informática (Firewalls, VLANs)</li> <li>Sistema de telefonía.</li> </ul>	ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el Cableado: TIA/EIA 568-B1 Requerimientos generales; TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado; TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> </ul>
4.	Evaluación de la infraestructura de cómputo	Se realiza la revisión de las implementaciones de servidores, máquinas virtuales y sistemas de almacenamiento (SAN).	Los profesionales de servidores y base de datos en conjunto con el contratista revisan la funcionalidad de la infraestructura de cómputo.	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> </ul>
5.	Alistamiento de la infraestructura de cómputo	Se implementa y determina la funcionalidad de: <ul style="list-style-type: none"> <li>Servidores físicos.</li> <li>Plataforma de Virtualización.</li> <li>Servidores virtuales.</li> <li>Sistemas de almacenamiento.</li> <li>Servicios de tecnología críticos.</li> </ul>	<ul style="list-style-type: none"> <li>Guion de pruebas</li> <li>Informe de pruebas a los servicios críticos TIC.</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> </ul>
6.	Informe de alistamiento del Datacenter Principal	Emitir el reporte de alistamiento y recomendación del traslado de las operaciones al Datacenter Principal.	Software de ofimática	Líder del DRP


Tabla 10 Procedimiento de alistamiento de instalaciones

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

### 6.3.2. Procedimiento de retorno a la normalidad

A continuación, el proceso para realizar el retorno a la normalidad:


Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Definir fecha, hora y duración estimada para el traslado de operaciones al Datacenter Principal	<ul style="list-style-type: none"> <li>Revisión del informe con las duraciones estimadas por actividad.</li> <li>Evaluación de fecha y hora más conveniente.</li> <li>Notificación a las áreas usuarias de la suspensión del servicio.</li> <li>Notificación a terceros de la maniobra de traslado de operaciones.</li> </ul>	<ul style="list-style-type: none"> <li>Plan de traslado</li> <li>Árbol de llamadas</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
2.	Generar backups del Datacenter Alterno en Nube	Se toman los respaldos totales de la información procesada en los sistemas de información y las aplicaciones durante la activación del Datacenter Alterno en Nube.	<ul style="list-style-type: none"> <li>Solución de respaldo</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> <li>Proveedor de Datacenter principal</li> </ul>
3.	Restaurar información	La información procesada en el Datacenter Alterno en Nube se restaura en el Datacenter Principal mediante backups.	<ul style="list-style-type: none"> <li>Solución de respaldo</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> <li>Proveedor de Datacenter principal</li> </ul>
4.	Pruebas de funcionalidad de los sistemas de información y de las aplicaciones	Solicitar a funcionarios la verificación del funcionamiento de los sistemas de información y de las aplicaciones	Diseño de pruebas de funcionalidad de los sistemas de información y de las aplicaciones	<ul style="list-style-type: none"> <li>Equipo de enlace con usuarios y proveedores</li> <li>Usuarios</li> </ul>
5.	Notificar la funcionalidad del Datacenter Principal	Informar a los funcionarios y terceros la disponibilidad y funcionalidad del Datacenter Principal.	Árbol de llamadas, teléfonos fijos, celulares	<ul style="list-style-type: none"> <li>Líder del DRP</li> </ul>
6.	Suspender el servicio del Datacenter Alterno en Nube	En la fecha y hora establecida se suspende el procesamiento en el Datacenter Alterno en Nube	Software de monitoreo de redes	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Nro.	Actividad	Detalles de Implementación	Recursos	Responsable
7.	Configurar Datacenter Alternativo en Nube como pasivo	El Datacenter Alternativo en Nube se configura nuevamente para que se encuentre activo para replicación, pasivo para procesamiento	<ul style="list-style-type: none"> <li>Configuraciones de telecomunicaciones y seguridad originales</li> <li>Configuraciones de replicación originales</li> </ul>	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
8.	Iniciar operaciones en el Datacenter Principal	Iniciar operaciones desde el Datacenter Principal	Informe de avance del plan de retorno a la normalidad	<ul style="list-style-type: none"> <li>Líderes de proceso</li> </ul>
9.	Monitorear el desempeño del Datacenter Principal	Verificar el nivel de operación y calidad del servicio del Datacenter Principal en todos sus aspectos: Volumen de trabajo, comunicaciones, almacenamiento, conectividad con terceros y proveedores, servicio a usuarios remotos.	Servicio de Monitoreo de red	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
10.	Normalización en el respaldo de datos	Aplicar la política de replicación y toma de backups en el Datacenter Principal.	<ul style="list-style-type: none"> <li>Solución de respaldo</li> <li>Discos duros externos</li> </ul>	<ul style="list-style-type: none"> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> </ul>
11.	Declarar el fin de la contingencia	<ul style="list-style-type: none"> <li>Revisar informes de monitoreo del Datacenter Principal.</li> <li>Notificar a los funcionarios, terceros la finalización de la contingencia y declarar el retorno a la normalidad.</li> </ul>	Árbol de llamadas, teléfonos fijos, celulares	<ul style="list-style-type: none"> <li>Líder del DRP</li> </ul>
12.	Lecciones aprendidas	<ul style="list-style-type: none"> <li>Solicitar reunión con los participantes en la ejecución del DRP.</li> <li>Solicitar a los asistentes los puntos de mejora del DRP.</li> <li>Definir acciones correctivas.</li> <li>Solicitar el ajuste a los procedimientos de recuperación.</li> </ul>	<ul style="list-style-type: none"> <li>Sala de reuniones</li> <li>Anotaciones hechas durante la ejecución del DRP</li> </ul>	<ul style="list-style-type: none"> <li>Líder del DRP</li> <li>Equipo de recuperación de servicios tecnológicos base</li> <li>Equipo de recuperación de sistemas de información y aplicaciones</li> <li>Equipo de enlace con usuarios y proveedores</li> </ul>

Tabla 11 Procedimiento de retorno a la normalidad


Es bueno aclarar que, en esta etapa también se debe notificar la desactivación del DRP a los miembros del Comité de Crisis (Comité Institucional de Gestión y Desempeño).

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025


## 7. RIESGOS DE ACTIVAR EL DRP

A continuación, se presentan los riesgos que se deben gestionar durante la activación y operación del DRP:

Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Plan de Acción
R1	Problemas de Conectividad.	Falla de conectividad con Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.	Ausencia de pruebas y/o planes de mejoramiento ineficientes.	2	5	Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.
R2	Máquinas virtuales no disponibles.	Imposibilidad de conexión a la consola de administración de la plataforma de virtualización.	Ausencia de pruebas y/o planes de mejoramiento ineficientes.	2	5	Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.
R3	Personal no capacitado.	Personal no capacitado para recuperar los servicios de TI.	Ausencia o ineficiencia de programas de entrenamiento y capacitación a los colaboradores de tecnología.	3	5	Documentar procedimientos de recuperación de sistemas de información y servicios base de TI.
		Personal sin conocimiento del Plan de Recuperación de Desastres.				Divulgación del DRP.
R4	Datos incorrectos.	Archivos corruptos o mal copiados en la réplica del servidor BD.	Estrategia y procedimiento de backup ineficientes.	2	5	Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.
R5	Backups desactualizados.	Discos duros con datos antiguos.	Estrategia y procedimientos de backup ineficientes.	2	5	Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.
R6	El Datacenter Alternativo queda como Datacenter Principal.	El desastre deja totalmente destruido el Datacenter Principal y su reconstrucción toma más tiempo de lo estimado.	Ubicación geográfica.	2	5	<ul style="list-style-type: none"> <li>Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.</li> <li>Negociación con proveedores para adecuación del Datacenter Principal.</li> <li>Aprovisionamiento de infraestructura en Datacenter Alternativo para brindar servicios no cubiertos por el DRP.</li> </ul>

	PLAN	RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	CÓDIGO	INTI-Plan-006
	ACTIVIDAD	GESTIÓN DE CONTINUIDAD DE NEGOCIO	VERSIÓN	1
	PROCESO	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	FECHA	31/12/2025

Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Plan de Acción
R7	El Datacenter Alternativo en Nube falla o su capacidad de procesamiento es muy inferior a la demanda de servicios	En medio de la operación en el Datacenter Alternativo este falla o su capacidad de procesamiento es superada por la demanda de transacciones de los procesos	Capacidad instalada en el Datacenter Alternativo	2	5	<ul style="list-style-type: none"> <li>● Hacer pruebas de activación del Datacenter Alternativo o donde se encuentren las contingencias tecnológicas.</li> <li>● Negociación con proveedores para adecuación del Datacenter Principal.</li> <li>● Aprovechamiento de infraestructura en Datacenter Alternativo para brindar servicios no cubiertos por el DRP.</li> <li>● Activar planes de continuidad de negocio y contingencia operativas partiendo del escenario "Ausencia total de servicios de tecnología"</li> <li>● Activar sólo servicios TIC para procesos críticos del negocio</li> </ul>
R8	Interrupción de los servicios de negocio en la fase de retorno al Datacenter Principal.	Personal no capacitado para llevar a cabo el retorno de los sistemas de información y servicios de TI.	Ausencia o ineficiencia de programas de entrenamiento y capacitación a los colaboradores de tecnología.	3	5	Hacer pruebas de retorno de la operación al Datacenter Principal.

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

## 8. BIBLIOGRAFÍA

- NTC – ISO 22301:2019 “Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos.”
- Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.

## 9. GLOSARIO<sup>5</sup> ISO 22301

**Alta dirección:** Persona o grupo de personas quienes dirigen y controlan una organización desde su alto nivel.

**Acción Correctiva:** Acción para eliminar la causa de una no conformidad y prevenir la recurrencia.

**Acuerdos de ayuda mutua:** Entendimiento entre dos o más entidades para hacer o brindar asistencia a los demás.

**Actividad:** Procesos o conjunto de procesos emprendidos por la organización que desarrollan o soportan uno o más productos y servicios.

**Actividades priorizadas:** Actividades que deben ser priorizadas siguiente a un incidente con el fin de mitigar los impactos.

**Administración de la continuidad de negocios:** Proceso holístico gerencial que identifica las amenazas potenciales en la organización y el impacto de dichas amenazas en las operaciones si se llegasen a dar. Persigue mejorar la resiliencia para establecer la capacidad de la empresa para construir la capacidad de una respuesta efectiva a la salvaguarda de los intereses de las partes involucradas, reputación, marca y actividades para crear valor.

**Administración de Riesgos:** Actividades coordinadas para direccionar y controlar una organización con relación a los riesgos.

**Alta dirección:** Persona o grupo de personas quienes dirigen y controlan una organización desde su alto nivel.

**Análisis de Impacto en el Negocio (BIA):** Proceso de análisis de actividades y efecto que en un negocio podría tener sobre ellas la interrupción de procesos.


**Apetito de Riesgo:** Monto de riesgo que una organización acepta o retiene.

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

**Auditoría Interna:** Auditoría conducida por o en nombre de la misma organización para revisar la administración del SGCN la cual debe formar parte de la organización y autodeclaración de conformidad.

**Competencia:** Habilidad para aplicar conocimiento y las habilidades para lograr resultados.

<sup>5</sup> Tomado de la Norma Técnica Colombiana NTC-ISO/IEC 22301

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

**Conformidad:** Cumplimiento de un requerimiento.

**Continuidad de Negocios:** capacidad de la organización para continuar desarrollando los productos o servicios en un nivel aceptable predefinidos, posterior a un incidente.

**Corrección:** Acción para eliminar una no conformidad detectada.

**Ejercicio:** Procesos de entrenamiento para evaluar, practicar e implementar mejoras en una organización.

**Evaluación de desempeño:** Proceso para determinar los resultados de la medición.

**Evaluación de Riesgo:** Cubrimiento de los procesos de identificación, análisis y evaluación de riesgos.

**Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.

**Incidente:** Situación que puede ser o podría dar lugar a una interrupción, pérdidas, emergencias o crisis.

**Información Documentada:** Información requerida para ser controlada y mantenerla por una organización y el medio el cual la contiene.

**Infraestructura:** Sistemas, equipos y servicios necesarios para la operación de una organización.

**Invocación:** Acto de declaración para que en la continuidad de negocios de la organización sea necesario poner en práctica un desarrollo continuo de productos o servicios claves para la misma organización.

**Máximo corte aceptable (MAO):** Tiempo que podría tomar para que los efectos adversos que se puedan dar como resultado de no proveer un producto/servicio o desarrollar una actividad, pueda llegar a ser inaceptable.

**Máximo período de interrupción tolerable (MTPD):** Ver MAO

**Mejora Continua:** Actividades recurrentes para desarrollar la mejora.

**Mínimo objetivo de continuidad de negocios (MBCO):** Nivel mínimo de servicios y/o productos que es aceptable a que la organización logre los objetivos del negocio durante la interrupción.


**Monitoreo:** Determinación del estado de un sistema, un proceso o una actividad.

**No conformidad:** No cumplir con un requerimiento.

**Partes Interesadas:** Personas u organizaciones que pueden resultar afectadas o afectar a ellos mismos o a un tercero por alguna decisión respecto a una actividad.

**Plan de continuidad de negocios:** Procedimiento documentado que guía a la organización para responder, recuperar y restaurar a un nivel predefinido los niveles de la operación de la compañía tras una interrupción de la operación.

**Política:** Intenciones y dirección de una organización expresada formalmente por la alta dirección.

 <b>Agencia Nacional de Tierras</b>	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLOGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

**Procedimiento:** Vía específica para llevar una actividad o un proceso.

**Proceso:** Conjunto de actividades interrelacionadas en las que se transforman entradas en salidas.

**Productos y Servicios:** Beneficio que provee una organización para sus clientes, Proveedores y partes interesadas.

**Programa de continuidad de negocios:** Gestión continua y procesos de gobierno corporativo soportados por la alta dirección y utilizando recursos de forma apropiada para implementar y mantener la gestión de la continuidad de negocios.

**Pruebas:** Procedimiento para evaluar el SGCN

**Recursos:** Todos los activos, personas, habilidades, información, tecnología, premisas, proveedores, que una organización ha tenido disponible para su uso, cuando lo necesitó, alineado con la operación y el cumplimiento de los objetivos.

**Registro:** Conjunto de resultados logrados o evidencia de actividades desarrolladas.

**Requerimiento:** necesidad o expectativa que es fijada, generalmente implica obligatoriedad.

**Riesgo:** Efecto de un evento sobre los objetivos.

**RPO (Punto objetivo de recuperación):** Punto en el cual la información utilizada por una actividad debe ser restaurada para colocar en funcionamiento o habilitar dicha actividad.

**RTO (Recovery Time Objective):** Periodo de tiempo que sigue al incidente y en el cual:


- i. El producto o servicio debe ser restaurado, o
- ii. La actividad debe ser restaurada, o
- iii. Los recursos deben estar recuperados.

**SGCN:** Parte de la gestión general para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de la continuidad de negocios.

**Sistema de Administración:** Conjunto de elementos interrelacionados que interactúan para el establecimiento de políticas y objetivos, y que los procesos cumplan o logren dichos objetivos.

**Tercerizar:** Forma de establecer que una entidad externa desarrolle parte de las funciones, procesos u operación de una organización.



	<b>PLAN</b>	<b>RECUPERACIÓN DE DESASTRES TECNOLÓGICOS</b>	<b>CÓDIGO</b>	INTI-Plan-006
	<b>ACTIVIDAD</b>	GESTIÓN DE CONTINUIDAD DE NEGOCIO	<b>VERSIÓN</b>	1
	<b>PROCESO</b>	INTELIGENCIA Y SEGURIDAD DE LA INFORMACIÓN	<b>FECHA</b>	31/12/2025

HISTORIAL DE CAMBIOS		
Fecha	Versión	Descripción
30/12/2025	1	Primera versión del documento, creada con el propósito de definir los lineamientos técnicos para la recuperación de la infraestructura tecnológica y los servicios de información ante incidentes, reduciendo el impacto en la disponibilidad, integridad y continuidad de los sistemas institucionales.

APROBACIÓN				
	NOMBRE	CARGO	FIRMA	FECHA
ELABORÓ	Dianalin Neme Prada	Contratista - Subdirección de Sistemas de Información de Tierras	<b>ORIGINAL FIRMADO</b>	24/12/2025
ELABORÓ	Andrea Linney Sierra Ladino	Contratista - Subdirección de Sistemas de Información de Tierras	<b>ORIGINAL FIRMADO</b>	26/12/2025
REVISÓ	Diana Lucía Herrera Riaño	Subdirectora de Sistemas de Información de Tierras	<b>ORIGINAL FIRMADO</b>	29/12/2025
APROBÓ	<b>APROBACIÓN Y PUBLICACIÓN DEL PLAN</b> 5° Sesión Comité Institucional de Gestión y Desempeño del 30/12/2025			30/12/2025

*La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia.*

*La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.*