



**DIRECCIÓN GENERAL
DE SANIDAD MILITAR**

2026

**Gestión Tecnologías de la
Información y las
Comunicaciones - PROGTIC**

**PLAN DE
CONTINUIDAD DEL
NEGOCIO**

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2024	Versión Inicial. Elaboración por primera vez del documento. NOTA PROASIG - PROPLAES: Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército y Armada Nacional, Jefatura Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0124014880202 , de fecha -30 de diciembre de 2024
2	Diciembre 2025	El Plan de Gestión de Continuidad del Negocio -DIGSA 2025 establece un marco estratégico para garantizar la operación continua de la DIGSA ante eventos disruptivos. Entre sus componentes clave se incluyen la identificación de procesos críticos, estrategias de recuperación ante fallos de infraestructura, ciberataques o desastres naturales, definición de roles y responsabilidades, y actividades programadas para el año 2025 como pruebas de recuperación, capacitación en ciberseguridad y monitoreo de redes. Aprobado en Comité Institucional de Gestión y Desempeño mediante Acta No. 0125014358302 del 24 de diciembre de 2025, por el Comité Institucional de Gestión y Desempeño. NOTA PROASIG: 1. Este documento fue revisado por PROASIG. PROPLAES libera el documento. 2. La información registrada en el documento es responsabilidad del proceso que lo emite. Fue traducido a lenguaje claro.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

CONTROL DE APROBACIÓN

Aprobó:	Comité de Gestión y Desempeño Institucional Acta No.0125014358302 de 2025		
Revisó:	PD. Julio Cesar Salgado Guerrero Gestión Tecnológicas de la Información y las Comunicaciones PROGTIC Gestor de Calidad		CR. John Jairo Villabon Ramos Subdirector Técnico y de Gestión DIGSA
	TC. Jorge Darwin Guevara Guerrero Coordinador Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA		SP. Miguel Ángel Cardozo Líder Área Seguridad de la Información DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión PROASIG		
	PD. Roberto Rodríguez Perdomo Grupo Sistema Integral de Información – Tecnologías de La Información y las Comunicaciones DIGSA Área de Seguridad de la Información		
Elaboró:			

 DIGSA	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

CONTENIDO

1.	PRESENTACIÓN	6
2.	OBJETIVO	6
3.	ALCANCE	6
4.	APLICACIÓN	7
5.	FUNDAMENTO NORMATIVO.....	7
6.	DEFINICIONES	8
7.	ACRONIMOS.....	9
8.	POLÍTICAS DE OPERACION	9
9.	EJECUCION	11
9.1.	Eventos y Estrategias de Recuperación	11
9.2.	Estrategias de Recuperación	12
9.3.	Posibles pruebas de recuperación de TI.....	14
9.4.	Identificar Activos o Sistemas Críticos de TI	15
9.5.	Identificación de Procesos Críticos.....	18
9.6.	Roles y Responsabilidades	18
9.7.	Identificación De Amenazas	19
9.8.	Gestión de Operación Infraestructura y Sistema de Información	21
9.9.	Gestión de Copias de Seguridad	25
10.	BIBLIOGRAFÍA	28

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

LISTA TABLAS

Tabla 1. Posibles Eventos y Estrategias de Recuperación	12
Tabla 2. Posibles pruebas de recuperación de TI	14
Tabla 3. Identificación de Procesos Críticos	15
Tabla 4. Identificación de Activos Críticos	16
Tabla 5. Tiempos de Recuperación.....	17
Tabla 6. Matriz de Roles y Responsabilidades	18

LISTA ILUSTRACIONES

Ilustración 1. Diagrama de dependencia.	18
Ilustración 2. Fuentes de Amenazas	20

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

1. PRESENTACIÓN

La Gestión de la Continuidad del Negocio (GCN) es un proceso estratégico que garantiza la capacidad de una organización para continuar operando en caso de incidentes o interrupciones disruptivas. Su objetivo principal es minimizar el impacto de estos eventos y restaurar las operaciones críticas en el menor tiempo posible. Ante la creciente necesidad de asegurar la continuidad de los servicios y la protección de la información, la DIGSA ha implementado un plan de GCN desde el 1 de junio de 2021. Este plan, alineado con la política de gobierno digital, la dimensión 3 del MIPG, el plan de desarrollo y las políticas de seguridad informática institucionales, busca asegurar la continuidad de los procesos críticos de la organización.

El plan de GCN de la DIGSA identifica los procesos críticos, evalúa los posibles riesgos y define las acciones necesarias para garantizar su continuidad. Al integrar los requisitos de la GCN con otros aspectos como seguridad de la información, operaciones, personal y logística, se asegura una respuesta integral ante cualquier eventualidad.

Beneficios de la GCN para la DIGSA:

- Minimización de riesgos: Identificación y mitigación de amenazas que puedan afectar las operaciones.
- Protección de activos: Salvaguarda de la información y los sistemas críticos.
- Continuidad de los servicios: Mantenimiento de la prestación de servicios a los usuarios.
- Cumplimiento normativo: Adhesión a los requisitos legales y regulatorios.
- Mejora de la reputación: Demostración de un compromiso con la resiliencia organizacional.
- Al implementar la GCN, la DIGSA demuestra su compromiso con la protección de los intereses de sus usuarios y garantiza la continuidad de sus operaciones, incluso en situaciones adversas.

2. OBJETIVO

Garantizar la continuidad del negocio asegurando que los procesos críticos de la Dirección General de Sanidad Militar, no se vean interrumpidos por Amenazas, desastres o incidentes. A través de la identificación de riesgos y la protección de los activos de la información, la minimización del tiempo de inactividad y la continuidad de las operaciones. Esta práctica, complementada por las buenas medidas de seguridad y privacidad de la información.

3. ALCANCE

El Plan de Continuidad de Negocio en Tecnologías de la Información definido en este documento está asociado al proceso de Gestión Tecnológica, para el restablecimiento de los sistemas de información e infraestructura tecnológica que soportan los procesos misionales, dependencias y grupos que conforman la estructura organizacional de la entidad.

Alcance:

- Identificación de activos críticos: Determinar las aplicaciones, sistemas y datos esenciales para las operaciones.
- Definición de tiempos de recuperación: Establecer plazos máximos para restaurar los servicios y evitar pérdidas significativas.
- Desarrollo de procedimientos: Crear guías detalladas para responder a diferentes tipos de incidentes y recuperar los sistemas afectados.
- Capacitación del personal: Asegurar que el personal clave conozca y pueda ejecutar el plan en caso de emergencia.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

- Pruebas y mantenimiento: Implementar un programa regular de pruebas y actualizaciones para garantizar la efectividad del plan.

Beneficios:

- Minimización de pérdidas: Reducción de las consecuencias financieras y de reputación asociadas a interrupciones del servicio.
- Mayor resiliencia: Aumento de la capacidad de la organización para enfrentar eventos disruptivos.
- Cumplimiento normativo: Adhesión a los estándares de seguridad y continuidad del negocio.

4. APLICACIÓN

- DIGSA, DISAN/JEFSA

5. FUNDAMENTO NORMATIVO

Proveedor	Entrada - insumo
Ley 44 de 1993	Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
Ley 527 de 1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1712 de 2012	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1008 del 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Proveedor	Entrada - insumo
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Resolución 7870 de 2022	Por la cual se emite y adopta la política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa.
Resolución 02277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Lineamiento MSPI	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas
Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7	Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 Departamento Administrativo de la Función Pública. 2025.

6. DEFINICIONES

Activación:	Acto de declarar que los acuerdos de la entidad para la continuidad de negocio deben llevarse a la práctica con el fin de continuar la entrega de productos o servicios clave.
Activos de información:	Es aquel elemento de información que tiene valor para la Dirección General de Sanidad Militar-DIGSA, el cual recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, transmitida o soportada por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, talento humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.
Amenaza:	Evento que puede desencadenar un incidente produciendo daños materiales o inmateriales a la Entidad.
Análisis de impacto al negocio:	Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas.
Confidencialidad:	Garantía en que se acceda a la información de la compañía únicamente por los usuarios autorizados, por lo tanto, no deberá estar disponible ni será revelada a individuos, procesos u organizaciones sin la respectiva autorización. El conocimiento o divulgación de la información sin autorización impacta negativamente a la Dirección General de Sanidad Militar-DIGSA.
Continuidad del negocio:	Capacidad de la Entidad para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.
Desastre:	Problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un período de tiempo, superior a lo que la Entidad puede soportar sin sufrir perjuicios considerables para el negocio.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Disponibilidad:	La información manejada en la compañía deberá estar disponible, en el momento y forma que se requiera, dejando un registro del suministro de la misma y realizando el seguimiento pertinente del uso que se da a dicha información.
Estrategia de recuperación:	Secuencia de actividades con el fin de brindar continuidad de la operación de los procesos en una contingencia de impacto menor o mayor.
Evento:	Ocurrencia o cambio de un conjunto particular de circunstancias.
Impacto:	Es la consecuencia de la materialización de una amenaza sobre un activo.
Incidente:	Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o una reducción en la calidad de ese servicio.
Integridad:	Exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
Propietario del activo de información:	Grupo de trabajo, Oficina, Dirección o Delegatura, que tiene como responsabilidad velar por la protección del activo de información. Tiene responsabilidad de controlar la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.
Riesgo:	Estimación del grado de exposición de un activo a que una amenaza se materialice sobre él, causando daños a la Entidad.
Trabajo Remoto:	Desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual, generalmente empleando medios informáticos.
Vulnerabilidad:	Debilidad o falta de control asociada a un proceso o recurso que puede ser explotada provocando un daño sobre dicho proceso.

7. ACRONIMOS

ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
AREIN:	Área de Seguridad de la Información
ARIBD:	Área de administración del Sistema y Base de Datos
CCI:	Infraestructura Crítica Cibernética.
IGSA:	Dirección General de Sanidad Militar.
MSPI:	Modelo de Seguridad y Privacidad de la Información.
SGSI:	Sistema de Gestión de Seguridad de la Información.
SISAM:	Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones

8. POLÍTICAS DE OPERACION

8.1	El propósito de este plan es activar la ejecución de la recuperación de la operación de TI de Dirección General de Sanidad Militar - DIGSA, en el evento o situación que se interrumpan sus actividades normales y fallen los requerimientos mínimos de operación de los sistemas de información e infraestructura tecnológica.
8.2	La Dirección General de Sanidad Militar - DIGSA tiene como responsabilidad evaluar la necesidad y requerimientos que debe tener preparados para responder ante un evento de interrupción con el propósito de asegurar la disponibilidad de los sistemas de información, la infraestructura e integridad de los datos. Por lo tanto, es importante establecer 3 objetivos específicos.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

8.3	Definir los roles y las responsabilidades a los funcionarios del Grupo de Recursos Informáticos en la aplicación del Plan de Continuidad del Negocio, estrategia de recuperación tecnológica y responsables de los activos de información de otras dependencias.
8.4	Asegurar que los procedimientos de recuperación de la infraestructura tecnológica de la Entidad, establecida dentro estrategia de recuperación sean ejecutados frente a un evento de interrupción.
8.5	Establecer procedimientos de recuperación viables en términos de costo-beneficio que permita restablecer la disponibilidad de la información para la Entidad.
8.6	Los roles y responsabilidades que puede asignar la Entidad en caso que suceda un evento de interrupción con afectación significativa a la disponibilidad de la infraestructura tecnológica de Dirección General de Sanidad Militar - DIGSA, con el fin de actuar y tomar decisiones teniendo en cuenta el grado de afectación.
8.7	Líder principal de la estrategia de recuperación de TI: Directivo de Dirección General de Sanidad Militar - DIGSA o quien haga sus veces, con capacidad para la toma de decisiones.
8.8	Líder Alterno de la Estrategia de recuperación: Directivo de la Dirección General de Sanidad Militar-DIGSA o quien haga sus veces, con capacidad para la toma de decisiones ante situaciones críticas con conocimiento general de los sistemas de información e infraestructura tecnológica de la Entidad. Apoyará al Líder principal en la toma de decisiones. Realizará las mismas tareas del líder principal, en caso de estar ausente este.
8.9	Equipo de Recuperación Tecnológica: Este equipo deberá estar conformado por funcionarios del grupo de Tecnologías de la Información con conocimientos en gestión tecnológica o que dirijan procesos de gestión tecnológica. De igual forma, pueden ser funcionarios de otras dependencias con las capacidades y conocimientos en aspectos de tecnología, quienes bajo la coordinación y orientación del Líder principal de Recuperación Tecnológica, deberán evaluar los daños causados por cualquier tipo de siniestro para ejecutar la recuperación de la infraestructura, el hardware, software y las telecomunicaciones necesarias para garantizar la operación de los procesos en las dependencias de la Dirección General de Sanidad Militar-DIGSA. - Evaluar la disponibilidad de la infraestructura de procesamiento de información. - Coordinar el restablecimiento de la infraestructura tecnológica necesaria para la operación en continuidad de los procedimientos críticos. - Verificar la disponibilidad de la infraestructura de comunicaciones necesaria para la recuperación de las aplicaciones en el centro de operación en contingencia y el centro de cómputo alternativo. - Verificar la disponibilidad de requerimientos de Hardware y Software necesarios para el centro de cómputo alternativo. - Coordinar y ejecutar las labores de restauración de hardware, sistema operativo, aplicaciones, y bases de datos que soportan los procedimientos críticos de la Entidad. - Comunicar y explicar a todos los usuarios internos las limitaciones con las cuales tendrán que desempeñar sus funciones según sea el caso. - Coordinar las actividades necesarias para la creación y configuración de usuarios en el sistema operativo y/o aplicación.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

	• Coordinar la correcta operación del Hardware y Software de comunicaciones requeridas por las aplicaciones críticas. • Soportar a los equipos en continuidad en cualquier requerimiento de Hardware o Software, comunicando al Líder de Continuidad la necesidad de contratación o compra, para su debido trámite. • Realizar la restauración de la última copia disponible de la información, sistemas operativos, bases de datos y aplicaciones de la Dirección General de Sanidad Militar-DIGSA, en caso de presentarse un evento de interrupción significativo que afecte la integridad y disponibilidad de la información y sea necesaria la restauración en instalaciones de procesamiento diferentes con las que cuenta la Entidad. Comité de seguridad de la información: responsable de dar soporte a los equipos de continuidad de todas las áreas, en la definición, implementación, pruebas y actualización de la Dirección General de Sanidad Militar-DIGSA, para los procesos o áreas que estén bajo su responsabilidad. Dar soporte a los Líderes de Procedimiento, en la identificación y actualización del nivel de riesgo de Seguridad de la Información. • Monitorear la efectividad de los controles de seguridad física y lógica de las instalaciones de procesamiento de información, el acceso, respaldo de la información. • Verificar la funcionalidad y efectividad de los controles en las fases de planeación, alerta, transición, recuperación y vuelta a la normalidad con el fin de que se salvaguarde la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. • Coordinar las pruebas que permitan evaluar los controles de seguridad de la información, luego de la activación de las estrategias de recuperación. Teniendo en cuenta los posibles riesgos de continuidad del negocio que se pueden presentar a nivel de infraestructura tecnológica, en la siguiente descripción, se detallan las posibles estrategias enfocadas a la recuperación de la Entidad que podrán ser evaluadas, implementadas y aprobadas por la Alta Dirección, según la situación contingente que se pueda presentar.
--	---

9. EJECUCION

9.1. Eventos y Estrategias de Recuperación

Este capítulo describe los riesgos que pueden afectar la continuidad operativa, desde desastres naturales y fallos tecnológicos hasta interrupciones por terceros, y establece las estrategias para garantizar la recuperación rápida y eficaz. Se incluyen acciones como la activación de planes alternos, traslado de operaciones, teletrabajo y contingencias tecnológicas, con el objetivo de minimizar impactos en procesos críticos, proteger activos esenciales y asegurar el cumplimiento normativo, fortaleciendo la resiliencia organizacional y la cultura preventiva.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tabla 1. Posibles Eventos y Estrategias de Recuperación

Evento	Descripción	Estrategia
Desastre, pérdida total de sitio	Este evento integra todos los eventos que causen daños a los funcionarios, a la infraestructura física de la sede principal y a la infraestructura tecnológica de la Entidad.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres. - Recuperación de procesos mediante la ejecución de ER - Estrategias de Recuperación y estrategias de continuidad, bajo el escenario de afectación de sitio (traslado a sitio de terceros, teletrabajo o activación de Centro Alterno de Operaciones).
Daño de infraestructura tecnológica	Afectación parcial o total de la infraestructura tecnológica disponible en el Centro de Datos.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres.
Falla de proveedores críticos	Incumplimiento de los servicios contratados, afectando la operación.	- Los supervisores del contrato deberán validar la respuesta de los proveedores críticos de sus procesos, establecer cláusulas de continuidad y contingencia, establecer ANS (acuerdos de nivel de servicio) para operación normal y en contingencia; realizar seguimiento a los ANS establecidos.

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

9.2. Estrategias de Recuperación

No	Descripción
1	Las estrategias de recuperación que se describen a continuación se presentan como un referente para la Entidad, con el fin de ser evaluadas por parte de la Alta Dirección de la Entidad aquella que se ajuste a las necesidades actuales y futuras de la Dirección General de Sanidad Militar-DIGSA, con relación a la continuidad de carácter tecnológico de la Entidad en caso de presentarse un evento de interrupción mayor.
2	Restauración de la infraestructura tecnológica en un nuevo centro de datos.
3	Consiste en que luego de la evaluación de los daños, en caso de que la afectación sea muy significativa y no se cuente con instalaciones de procesamiento de información, se requiera restaurar la infraestructura en un nuevo centro de datos. Para poder activar la estrategia de recuperación es necesaria previamente realizar las siguientes actividades: • Tener actualizado el inventario de hardware, software de la Entidad, principalmente el de dispositivos de red e infraestructura tecnológica con el fin de solicitar al proveedor de los equipos o prestador de los servicios equipos con características similares. • Realizar la contratación de acuerdo a las políticas definidas por la Dirección General de Sanidad Militar-DIGSA.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

No	Descripción
	• Restaurar con una copia de respaldo de las bases de datos, aplicaciones, sistemas operativos e información con el fin de restablecerlas en el nuevo centro de datos. • Establecer la topología de la red del nuevo Centro de Datos. • Verificar la disponibilidad de las aplicaciones e información en el nuevo Centro de Datos. • Verificar la conexión entre el Centro de Datos Principal y el Centro Alterno de Procesamiento de Datos. • Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Principal de Procesamiento de Datos, dando continuidad a los controles que salvaguarden la seguridad de la información. • Realizar pruebas de conexión desde la sede alterna destinada por la Entidad que le permitan simular eventos de interrupción, evaluando tiempos de restauración y recuperación de los procesos críticos de la Entidad. • Verificar la disponibilidad de las aplicaciones y la información restaurada. • Validar que los funcionarios que se encuentran en el Centro Alterno de Operaciones (CAO) o en el sitio de recuperación operativa designada, puedan acceder normalmente a la información y las aplicaciones definidas en los elementos mínimos de recuperación de cada uno de los procedimientos. • Monitorear y verificar la disponibilidad de las aplicaciones, unidades de red, repositorios de información que requieran los procesos críticos de la Entidad. Replicación de la Información en un Centro Alterno de Datos (CAD): Esta estrategia de interrupción puede activarse en el evento en el que el Centro de Datos Principal, presente una afectación mayor que no permita la conexión a los servidores y por ende genere indisponibilidad de las aplicaciones y la información que está alojada en el Centro de Datos de la Entidad, redireccionando el tráfico de datos al Centro Alterno de Datos (CAD). Para activar la estrategia de recuperación es necesaria tener en cuenta las siguientes actividades: • Realizar el cambio de línea host, re- direccionando el tráfico de datos del Centro de Datos Principal al Centro Alterno de Datos (CAD). • Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Alterno de Datos (CAD), dando continuidad a los controles que salvaguarden la seguridad de la información. • Realizar pruebas de conectividad desde la sede de la Procuraduría Principal, los Puntos de Atención (Procuradurías Regionales) y/o el Centro Alterno de Operaciones (CAO), validando que en caso de contingencia se pueda dar continuidad a los servicios prestados por la Dirección General de Sanidad Militar-DIGSA.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

No	Descripción
4	Aprovisionamiento de los servicios en la nube (CLOUD): Consiste en realizar la replicación en línea o definir la periodicidad de ejecución de las copias de respaldo remotamente a los servidores virtuales alojados en la nube de las aplicaciones, bases de datos de las aplicaciones e información crítica. Para poder activar la estrategia de recuperación es necesaria previamente realizar las siguientes actividades: - Realizar la evaluación de los recursos tecnológicos necesarios a nivel de almacenamiento, gestión de la capacidad futura de procesamiento, controles de seguridad física y lógica, niveles de escalamiento, niveles de disponibilidad de la infraestructura, redundancia de la infraestructura en servidores virtuales alojados en una nube privada y demás condiciones que la Dirección General de Sanidad Militar-DIGSA, considere necesarios. - Solicitar el presupuesto para la siguiente vigencia con el fin de iniciar el proceso de contratación del servicio de CLOUD para la replicación de la data almacenada en el Centro de Datos Principal de la Entidad. - Realizar la gestión contractual con el proveedor de acuerdo con las políticas de la Entidad.
5	Las pruebas se deberán realizar de acuerdo con el cronograma de ejecución de pruebas a la estrategia de recuperación tecnológica y el alcance de los escenarios de recuperación establecida por la Entidad. Estos serán los posibles a probar: - Pérdida de un canal de telecomunicaciones de la Entidad. - Interrupción en el suministro eléctrico. - Interrupción del aire acondicionado central en el DATACENTER. - Desastre natural con destrucción parcial o total de las instalaciones de la sede principal.
6	A continuación, se identifican los tipos de pruebas que pueden ser aplicados por Entidad.

9.3. Posibles pruebas de recuperación de TI

Tabla 2. Posibles pruebas de recuperación de TI

Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución
Escritorio	Estas pruebas son realizadas por la Grupo de Recursos Informáticos donde se revisan las estrategias de recuperación simulando un escenario a seguir. Aquí básicamente se realizan pruebas tales como el árbol de llamadas con el fin de verificar que los funcionarios que hacen parte de la activación del plan tienen claro su rol y a quienes comunicar.	Según se requiera

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución
Componente / Modular	Prueba de validación de un elemento específico del plan, en forma aislada. Ejemplo: árboles de llamadas, información del directorio de continuidad, recuperación de un aplicativo específico, activación de canales alternos de comunicación, entre otros.	Según se requiera
Respaldo	Se valida de forma colectiva la disponibilidad de las aplicaciones y/o sistemas de información, estas pruebas se pueden realizar de forma independiente por proceso.	Periódicamente
Simulaciones	Integra varios tipos de procedimientos críticos/o áreas dentro de la organización, bajo un escenario “artificial”. Por ejemplo, áreas como: evacuación, comunicación, procesos, TI, proveedores, entre otras. Puede o no ejecutarse en el ambiente alterno.	Al menos cada dos años
Funcional / actividades críticas	Prueba en el ambiente alterno establecido, de una o más actividades críticas, por un periodo preestablecido de tiempo. Lo anterior, sin generar impacto en la operación normal.	Al menos una vez al año

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

9.4. Identificar Activos o Sistemas Críticos de TI

Los sistemas de tecnologías de información pueden ser muy complejos debido a la gran cantidad de interdependencias que pueden tener en elementos de software y de hardware. En esta actividad se trata de analizar los diferentes sistemas de TI con el fin de determinar las funciones o servicios críticos que se desprenden de ellos y también se busca identificar elementos críticos requeridos para realizar estas funciones o prestar estos servicios.

La tabla siguiente muestra los niveles de criticidad, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema.

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

Tabla 3. Identificación de Procesos Críticos

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Valor	Interpretación del proceso crítico
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

Tabla 4. Identificación de Activos Críticos

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	Aplicación Misional	A	1	Sistema de Información para la afiliación, atención, prestación y aseguramiento de los Usuarios del SSFM
Aplicaciones	Nomina	A	1	Sistemas de Información de Nomina SSFM
Web	Sitio web Entidad	A	1	Pagina Institucional DIGSA
Base de Datos	SQL nómina	A	1	Contenedor de aplicaciones en SQL
Seguridad de Información	Firewall, CORE, File Server, Web server, Switch Core, SOC NOC, Acces Point.	A	1	Servicio de firewall de la Entidad
Sistemas de Almacenamiento	NAS (Network, Área, Storage)	A	1	Capacidad de almacenamiento en la NAS
Comunicaciones	Acceso Local a Internet, LAN server, Red WAN, Red LAN	C	4	Comunicación de Internet del usuario local
Data Center	Centro de Datos	A	1	Servicio de Centro de datos de la Entidad
Data Center	Centro de Datos	A	1	Centro de Datos Fortaleza
Proveedores de Aplicaciones y/o comunicaciones	Interno/externo	B	2	Desarrollo Interno o contratado por externos. Canales de Comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad.

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios. Como complemento de esta actividad (identificación de activos) se realiza, el diagrama de dependencia

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN		
	Plan	De Gestión de Continuidad del Negocio DIGSA		
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5		
	Vigente	Diciembre de 2025		Versión: 2

que nos indican la conformación y criticidad de ciertos elementos de un sistema, tal como se muestra en la Figura No.1.

Tabla 5. Tiempos de Recuperación

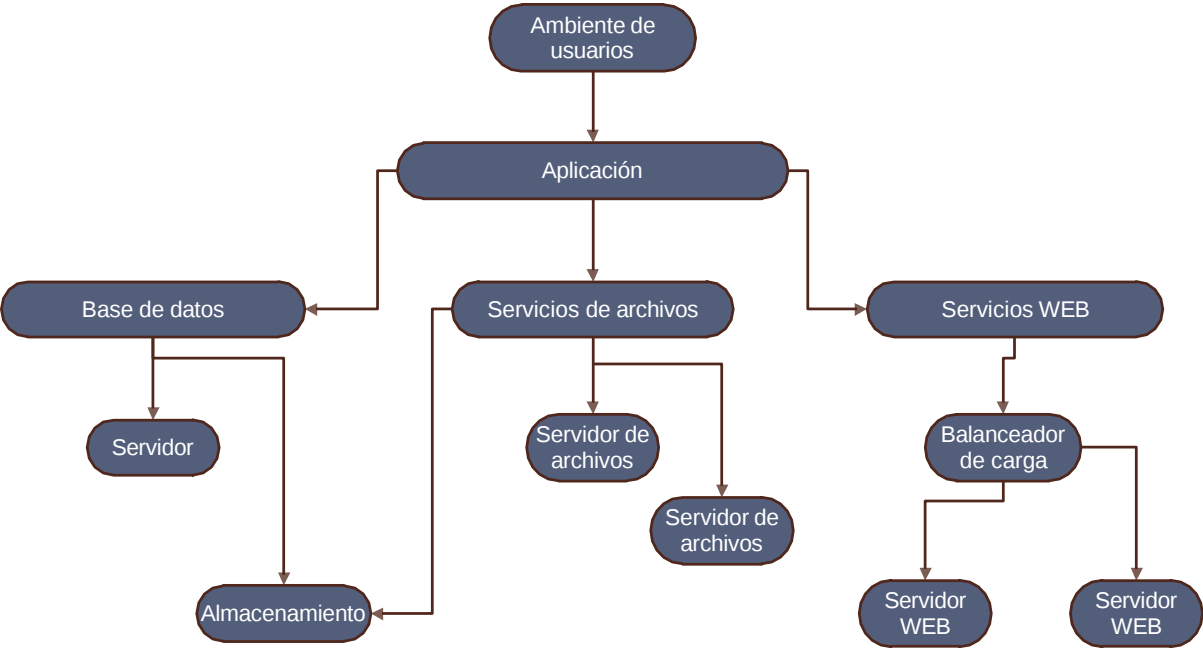
ID	TIPO DE ELEMENTO	NOMBRE	PROCESO	IMPACTO	Tolerancia a Fallas (Horas)	RPO (Horas)	RTO (Horas)	WRT (Horas)	MTD (Horas)
1	Aplicaciones	Aplicaciones	Aplicación Misional	Nivel A	1,0	1,0	1,0	1,0	1,0
2	Aplicaciones	Aplicaciones	Nomina	Nivel A	1,0	1,0	1,0	1,0	1,0
3	Web	Web	Sitio web Entidad	Nivel A	1,0	1,0	2,0	2,0	3,0
4	Base de Datos	Base de Datos	SQL nómina	Nivel A	1,0	0,3	1,0	1,0	1,0
5	Seguridad de Información	Seguridad de Información	Firewall, CORE, File Server, Web server, Switch Core, SOC NOC, Acces Point.	Nivel A	1,0	0,3	1,0	1,0	0,3
6	Sistemas de Almacenamiento	Sistemas de Almacenamiento	NAS (Network, Área, Storage)	Nivel A	1,0	0,3	1,0	1,0	0,3
7	Comunicaciones	Comunicaciones	Acceso Local a Internet, LAN server, Red WAN, Red LAN	Nivel C	4,0	1,0	1,0	1,0	0,3
8	Data Center	Data Center	Centro de Datos	Nivel A	1,0	1,0	1,0	1,0	0,3
9	Data Center	Data Center	Centro de Datos	Nivel A	1,0	1,0	1,0	1,0	0,3
10	Proveedores de Aplicaciones y/o comunicaciones	Proveedores de Aplicaciones y/o comunicaciones	Interno/externo	Nivel B	2,0	1,0	1,0	1,0	1,0
11	Recurso Humano	Recurso Humano	Internos/externos	Nivel C	3,0	1,0	1,0	1,0	1,0

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

9.5. Identificación de Procesos Críticos

Ilustración 1. Diagrama de dependencia.



Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

9.6. Roles y Responsabilidades

Tabla 6. Matriz de Roles y Responsabilidades

MATRIZ DE ROLES Y RESPONSABILIDADES					
ITEM	ROLES Y/O TAREAS ASIGNADAS	RESPONSABLE DE CADA AREA DE TRABAJO EN SISAM			
		ÁREA DE OPERACIONES TIC	ÁREA DE GOBIERNO TIC	ÁREA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	ÁREA GESTIÓN DE SISTEMAS DE INFORMACIÓN, APLICACIONES Y BASE DE DATOS
1	INFRAESTRUCTURA	Líder Área Infraestructura, Redes y Comunicaciones - ARECO			
2	TELECOMUNICACIONES				
3	SEGURIDAD INFORMÁTICA				
4	PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)				
5	OFICIAL SEGURIDAD INFORMATICA			Área Seguridad de la Información Oficial de Seguridad de la Información.	

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

MATRIZ DE ROLES Y RESPONSABILIDADES					
ITEM	ROLES Y/O TAREAS ASIGNADAS	RESPONSABLE DE CADA AREA DE TRABAJO EN SISAM			
		ÁREA DE OPERACIONES TIC	ÁREA DE GOBIERNO TIC	ÁREA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	ÁREA GESTIÓN DE SISTEMAS DE INFORMACIÓN, APLICACIONES Y BASE DE DATOS
6	INNOVACION, GESTIÓN, SEGUIMIENTO Y MEJORA CONTINUA		Coordinación SISAM Líder Área Infraestructura, Redes y Comunicaciones - ARECO		
7	MESA DE SERVICIO				
8	GOBIERNO DIGITAL				
9	CATALOGO DE SERVICIOS				
10	INVENTARIO				
11	CONTROL DE ACCESO				
12	SAP (mantenimiento SAP)				
13	GESTIÓN MESA DE SERVICIO				
14	ZENDESK (Enfermeras profesionales- apoyo funcional con los proveedores).				Área Administración del Sistema y Base de Datos
15	GESTIÓN BASE DE DATOS				
16	GESTIÓN DE APLICACIONES				
17	GESTIÓN DE SISTEMAS DE INFORMACIÓN				
18					
19					
20					

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN

9.7. Identificación De Amenazas

Las amenazas pueden ser el resultado de actos deliberados o mal intencionados que afectan los activos de los procesos. Las organizaciones enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los activos de TI se realizarán entrevistas con expertos de DIGSA, quienes suministrarán información sobre cuáles son las amenazas con mayor impacto desde la perspectiva de continuidad del servicio o servicios de TI, las que podrían llegar a afectar la continuidad de las operaciones de TI, y, por consiguiente, podrían causar una pérdida financiera o afectación de la imagen de la compañía.

Una vez identificadas las amenazas, y con el propósito de complementar y de validar la lista de amenazas encontradas, se realiza una verificación contra algunas de las fuentes de amenazas especificadas en Figura No. 2. Fuentes de amenazas., agrupándolas para el análisis de riesgo como amenazas de tipo natural, intencionales (humanas) o accidentales.

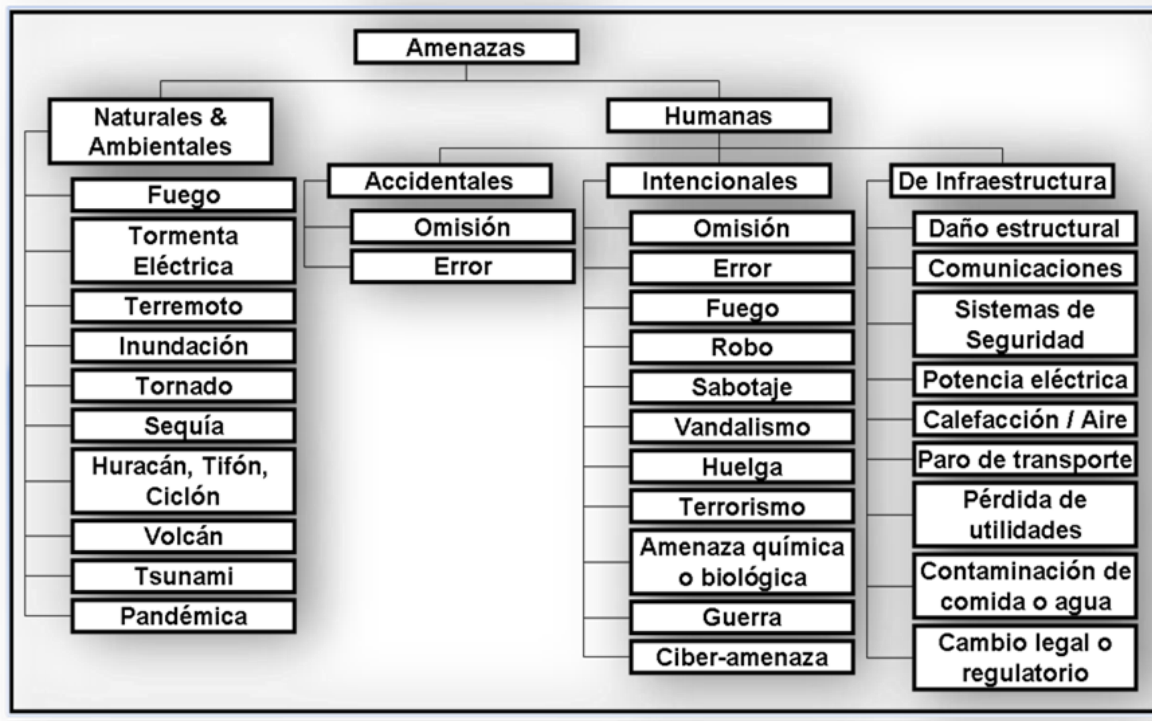
En esta actividad se establece el conjunto de vulnerabilidades que posee cada activo crítico de TI, que, en caso de ser explotadas por una o varias amenazas, afectarían la continuidad de las operaciones.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Las vulnerabilidades, por su parte, son debilidades o ausencia de controles que un activo perteneciente a un proceso pueda tener. Algunas vulnerabilidades consideradas dentro de esta metodología son:

- Ausencia de políticas.
- Configuraciones no seguras
- Errores de configuración.
- Errores de mantenimiento.
- Errores del administrador.
- Errores en código.
- Exposición a materiales peligrosos.
- Fallas de usuarios.
- Manuales de uso no documentados.
- Medidas de protección de acceso inadecuadas.
- Medidas de protección física inadecuadas.
- Procesos o procedimientos no documentados.
- Usuario desinformado.
- Tecnología inadecuada.
- Debilidad o inexistencia de controles.
- Condiciones de locales inadecuadas o no seguras.

Ilustración 2. Fuentes de Amenazas



Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

9.8. Gestión de Operación Infraestructura y Sistema de Información

Tipo	Descripción
Planeación	Es responsabilidad de la Dirección General de Sanidad Militar, a través de del Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones - SISAM evaluar de manera permanente la necesidad y los requerimientos necesarios para responder ante cualquier evento de interrupción, con el propósito de garantizar la disponibilidad de los sistemas de información, la infraestructura tecnológica y la integridad de los datos que soportan los procesos misionales y administrativos de la entidad.
Estructura	Definir, documentar y comunicar los roles y responsabilidades de los funcionarios del Grupo de Recursos Informáticos en la aplicación del Plan de Continuidad del Negocio y la estrategia de recuperación tecnológica, así como establecer la responsabilidad sobre los activos de información en las demás dependencias, garantizando la correcta coordinación y cumplimiento de las acciones necesarias para asegurar la disponibilidad, integridad y protección de la información en DIGSA.
Aseguramiento	Asegurar que los procedimientos para la recuperación de la infraestructura tecnológica de la Entidad, definidos dentro de la estrategia de recuperación, sean ejecutados de manera efectiva ante cualquier evento de interrupción, garantizando la continuidad operativa y la disponibilidad de los servicios críticos de información en DIGSA.
Directriz	Establecer procedimientos de recuperación que sean viables en términos de costo-beneficio, garantizando el restablecimiento oportuno de la disponibilidad de la información para la Entidad y asegurando la continuidad de los servicios críticos en DIGSA.
Coordinación	Definir y asignar los roles y responsabilidades que la Entidad establecerá en caso de presentarse un evento de interrupción que afecte significativamente la disponibilidad de la infraestructura tecnológica de la Dirección General de Sanidad Militar (DIGSA), con el propósito de garantizar una actuación oportuna y la toma de decisiones basadas en el grado de afectación.
Dirección	El Líder principal de la estrategia de recuperación de TI será un directivo de la Dirección General de Sanidad Militar (DIGSA) o quien haga sus veces, con la autoridad y capacidad necesarias para la toma de decisiones que garanticen la ejecución efectiva de las acciones de recuperación tecnológica y la continuidad operativa de los servicios críticos.
Roles y Responsabilidades	Designar como líder principal de la estrategia de recuperación de Tecnologías de la Información al Directivo de la Dirección General de Sanidad Militar (DIGSA) o a quien lo represente, otorgándole la capacidad para la toma de decisiones necesarias que garanticen la ejecución efectiva del Plan de Continuidad del Negocio y la estrategia de recuperación tecnológica. • Apoyará al Líder principal en la toma de decisiones. • Realizará las mismas tareas del líder principal, en caso de estar ausente este.
Organización	El Equipo de Recuperación Tecnológica deberá estar conformado por funcionarios del Grupo de Tecnologías de la Información con conocimientos en gestión tecnológica o que dirijan procesos relacionados, así como por funcionarios de otras dependencias que cuenten con capacidades y conocimientos en aspectos tecnológicos; bajo la coordinación del Líder principal de Recuperación Tecnológica, este equipo será responsable de evaluar los daños ocasionados por cualquier siniestro y ejecutar la recuperación de la infraestructura, hardware, software y telecomunicaciones necesarias para garantizar la continuidad operativa de los procesos en las dependencias de la Dirección General de Sanidad Militar (DIGSA), realizando las siguientes actividades: • Evaluar la disponibilidad de la infraestructura de procesamiento de información.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción
	• Coordinar el restablecimiento de la infraestructura tecnológica necesaria para la operación en continuidad de los procedimientos críticos. • Verificar la disponibilidad de la infraestructura de comunicaciones necesaria para la recuperación de las aplicaciones en el centro de operación en contingencia y el centro de cómputo alternativo. • Verificar la disponibilidad de requerimientos de Hardware y Software necesarios para el centro de cómputo alternativo. • Coordinar y ejecutar las labores de restauración de hardware, sistema operativo, aplicaciones, y bases de datos que soportan los procedimientos críticos de la Entidad. • Comunicar y explicar a todos los usuarios internos las limitaciones con las cuales tendrán que desempeñar sus funciones según sea el caso. • Coordinar las actividades necesarias para la creación y configuración de usuarios en el sistema operativo y/o aplicación. • Coordinar la correcta operación del Hardware y Software de comunicaciones requeridas por las aplicaciones críticas. • Soportar a los equipos en continuidad en cualquier requerimiento de Hardware o Software, comunicando al Líder de Continuidad la necesidad de contratación o compra, para su debido trámite. • Realizar la restauración de la última copia disponible de la información, sistemas operativos, bases de datos y aplicaciones de la Dirección General de Sanidad Militar-DIGSA, en caso de presentarse un evento de interrupción significativo que afecte la integridad y disponibilidad de la información y sea necesaria la restauración en instalaciones de procesamiento diferentes con las que cuenta la Entidad.
Continuidad	El Comité de Seguridad de la Información será responsable de brindar soporte a los equipos de continuidad de todas las áreas en la definición, implementación, pruebas y actualización de los procesos bajo su responsabilidad en la Dirección General de Sanidad Militar (DIGSA), así como de apoyar a los Líderes de Procedimiento en la identificación y actualización del nivel de riesgo asociado a la Seguridad de la Información, garantizando la protección y continuidad de los servicios críticos, realizando las siguiente actividades: • Monitorear la efectividad de los controles de seguridad física y lógica de las instalaciones de procesamiento de información, el acceso, respaldo de la información. • Verificar la funcionalidad y efectividad de los controles en las fases de planeación, alerta, transición, recuperación y vuelta a la normalidad con el fin de que se salvaguarde la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. • Coordinar las pruebas que permitan evaluar los controles de seguridad de la información, luego de la activación de las estrategias de recuperación.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción		
Gestión de Riesgos	Considerando los posibles riesgos que puedan afectar la continuidad del negocio a nivel de infraestructura tecnológica, se deberán definir, evaluar, implementar y aprobar por la Alta Dirección las estrategias orientadas a la recuperación de la Entidad, conforme a la situación contingente que se presente, garantizando la disponibilidad y resiliencia de los servicios críticos en DIGSA.		
	Posibles eventos y estrategias de recuperación		
	Evento	Descripción	Estrategia
	Desastre, pérdida total de sitio	Este evento integra todos los eventos que causen daños a los funcionarios, a la infraestructura física de la sede principal y a la infraestructura tecnológica de la Entidad.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres.
			- Recuperación de procesos mediante la ejecución de ER - Estrategias de Recuperación y estrategias de continuidad, bajo el escenario de afectación de sitio (traslado a sitio de terceros, teletrabajo o activación de Centro Alterno de Operaciones).
Daño de infraestructura tecnológica	Afectación parcial o total de la infraestructura tecnológica disponible en el Centro de Datos.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres.	
Falla de proveedores críticos	Incumplimiento de los servicios contratados, afectando la operación.	- Los supervisores del contrato deberán validar la respuesta de los proveedores críticos de sus procesos, establecer cláusulas de continuidad y contingencia, establecer ANS (acuerdos de nivel de servicio) para operación normal y en contingencia; realizar seguimiento a los ANS establecidos.	
Disponibilidad Tecnológica.	Las estrategias de recuperación que se describen a continuación se presentan como un referente para la Entidad, con el fin de ser evaluadas por parte de la Alta Dirección de la Entidad aquella que se ajuste a las necesidades actuales y futuras de la Dirección General de Sanidad Militar-DIGSA, en relación a la continuidad de carácter tecnológico de la Entidad en caso de presentarse un evento de interrupción mayor.		
Disponibilidad Tecnológica.	En caso de que la afectación a la infraestructura tecnológica sea significativa y no se disponga de instalaciones para el procesamiento de información, se deberá restaurar la infraestructura en un nuevo centro de datos, garantizando la continuidad operativa mediante la ejecución de actividades como: ○ Restauración de la infraestructura tecnológica en un nuevo centro de datos. ○ Tener actualizado el inventario de hardware, software de la Entidad, principalmente el de dispositivos de red e infraestructura tecnológica con el fin de solicitar al proveedor de los equipos o prestador de los servicios equipos con características similares. ○ Realizar la contratación de acuerdo a las políticas definidas por la Dirección General de Sanidad Militar-DIGSA.		

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción
	- Restaurar con una copia de respaldo de las bases de datos, aplicaciones, sistemas operativos e información con el fin de restablecerlas en el nuevo centro de datos. - Establecer la topología de la red del nuevo Centro de Datos. - Verificar la disponibilidad de las aplicaciones e información en el nuevo Centro de Datos. - Verificar la conexión entre el Centro de Datos Principal y el Centro Alterno de Procesamiento de Datos. - Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Principal de Procesamiento de Datos, dando continuidad a los controles que salvaguarden la seguridad de la información. - Realizar pruebas de conexión desde la sede alterna destinada por la Entidad que le permitan simular eventos de interrupción, evaluando tiempos de restauración y recuperación de los procesos críticos de la Entidad. - Verificar la disponibilidad de las aplicaciones y la información restaurada. - Validar que los funcionarios que se encuentran en el Centro Alterno de Operaciones (CAO) o en el sitio de recuperación operativa designada, puedan acceder normalmente a la información y las aplicaciones definidas en los elementos mínimos de recuperación de cada uno de los procedimientos. - Monitorear y verificar la disponibilidad de las aplicaciones, unidades de red, repositorios de información que requieran los procesos críticos de la Entidad
Disponibilidad Tecnológica.	En caso de que el Centro de Datos Principal presente una afectación mayor que impida la conexión a los servidores y genere indisponibilidad de aplicaciones e información, se deberá activar la estrategia de replicación de datos redireccionando el tráfico hacia el Centro Alterno de Datos (CAD), garantizando la continuidad operativa mediante actividades como mantener actualizados los mecanismos de replicación, verificar la integridad y sincronización de la información, asegurar la conectividad entre el centro principal y el alterno, validar la disponibilidad de aplicaciones críticas, y realizar pruebas periódicas que confirmen la eficacia del proceso de recuperación. Para activar la estrategia de recuperación es necesaria tener en cuenta las siguientes actividades: - Realizar el cambio de línea host, re- direccionando el tráfico de datos del Centro de Datos Principal al Centro Alterno de Datos (CAD). - Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Alterno de Datos (CAD), dando continuidad a los controles que salvaguarden la seguridad de la información. - Realizar pruebas de conectividad desde la sede de la Procuraduría Principal, los Puntos de Atención (Procuradurías Regionales) y/o el Centro Alterno de Operaciones (CAO), validando que en caso de contingencia se pueda dar continuidad a los servicios prestados por la Dirección General de Sanidad Militar-DIGSA.
	Se deberá garantizar el aprovisionamiento de servicios en la nube mediante la replicación en línea o la ejecución periódica de copias de respaldo de aplicaciones, bases de datos e información crítica hacia servidores virtuales alojados en la nube, asegurando la continuidad operativa y la disponibilidad de los servicios esenciales en caso de contingencia, Para poder activar la estrategia de recuperación es necesaria previamente realizar las siguientes actividades: - Realizar la evaluación de los recursos tecnológicos necesarios a nivel de almacenamiento, gestión de la capacidad futura de procesamiento, controles de seguridad física y lógica, niveles de escalamiento, niveles de disponibilidad de la infraestructura, redundancia de la infraestructura en servidores virtuales alojados en una nube privada y demás condiciones que la Dirección General de Sanidad Militar-DIGSA, considere necesarios. - Solicitar el presupuesto para la siguiente vigencia con el fin de iniciar el proceso de contratación del servicio de cloud para la replicación de la data almacenada en el Centro de Datos Principal de la Entidad. - Realizar la gestión contractual con el proveedor de acuerdo con las políticas de la Entidad.
Disponibilidad Tecnológica.	Las pruebas deberán ejecutarse conforme al cronograma establecido por la Entidad para la estrategia de recuperación tecnológica, considerando el alcance definido para los escenarios de recuperación, con el fin de garantizar la efectividad y continuidad de los procesos críticos. Estos serán los posibles a probar: Pérdida de un canal de telecomunicaciones de la Entidad.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción																				
	○ Interrupción en el suministro eléctrico. ○ Interrupción del aire acondicionado central en el Datacenter. ○ Desastre natural con destrucción parcial o total de las instalaciones de la sede principal. Tipos de pruebas que pueden ser aplicados por Entidad.																				
	<table><tr><th>Tipo de Prueba</th><th>Descripción</th><th>Frecuencia sugerida de ejecución</th></tr><tr><td>Escritorio</td><td>Estas pruebas son realizadas por la Grupo de Recursos Informáticos donde se revisan las estrategias de recuperación simulando un escenario a seguir. Aquí básicamente se realizan pruebas tales como el árbol de llamadas con el fin de verificar que los funcionarios que hacen parte de la activación del plan tienen claro su rol y a quienes comunicar.</td><td>Según se requiera</td></tr><tr><td>Componente / Modular</td><td>Prueba de validación de un elemento específico del plan, en forma aislada. Ejemplo: árboles de llamadas, información del directorio de continuidad, recuperación de un aplicativo específico, activación de canales alternos de comunicación, entre otros.</td><td>Según se requiera</td></tr><tr><td>Respaldo</td><td>Se valida de forma colectiva la disponibilidad de las aplicaciones y/o sistemas de información, estas pruebas se pueden realizar de forma independiente por proceso.</td><td>Periódicamente</td></tr><tr><td>Simulaciones</td><td>Integra varios tipos de procedimientos críticos/o áreas dentro de la organización, bajo un escenario “artificial”. Por ejemplo, áreas como: evacuación, comunicación, procesos, TI, proveedores, entre otras. Puede o no ejecutarse en el ambiente alterno.</td><td>Al menos cada dos años</td></tr><tr><td>Funcional / actividades críticas</td><td>Prueba en el ambiente alterno establecido, de una o más actividades críticas, por un periodo preestablecido de tiempo. Lo anterior, sin generar impacto en la operación normal.</td><td>Al menos una vez al año</td></tr></table>	Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución	Escritorio	Estas pruebas son realizadas por la Grupo de Recursos Informáticos donde se revisan las estrategias de recuperación simulando un escenario a seguir. Aquí básicamente se realizan pruebas tales como el árbol de llamadas con el fin de verificar que los funcionarios que hacen parte de la activación del plan tienen claro su rol y a quienes comunicar.	Según se requiera	Componente / Modular	Prueba de validación de un elemento específico del plan, en forma aislada. Ejemplo: árboles de llamadas, información del directorio de continuidad, recuperación de un aplicativo específico, activación de canales alternos de comunicación, entre otros.	Según se requiera	Respaldo	Se valida de forma colectiva la disponibilidad de las aplicaciones y/o sistemas de información, estas pruebas se pueden realizar de forma independiente por proceso.	Periódicamente	Simulaciones	Integra varios tipos de procedimientos críticos/o áreas dentro de la organización, bajo un escenario “artificial”. Por ejemplo, áreas como: evacuación, comunicación, procesos, TI, proveedores, entre otras. Puede o no ejecutarse en el ambiente alterno.	Al menos cada dos años	Funcional / actividades críticas	Prueba en el ambiente alterno establecido, de una o más actividades críticas, por un periodo preestablecido de tiempo. Lo anterior, sin generar impacto en la operación normal.	Al menos una vez al año		
Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución																			
Escritorio	Estas pruebas son realizadas por la Grupo de Recursos Informáticos donde se revisan las estrategias de recuperación simulando un escenario a seguir. Aquí básicamente se realizan pruebas tales como el árbol de llamadas con el fin de verificar que los funcionarios que hacen parte de la activación del plan tienen claro su rol y a quienes comunicar.	Según se requiera																			
Componente / Modular	Prueba de validación de un elemento específico del plan, en forma aislada. Ejemplo: árboles de llamadas, información del directorio de continuidad, recuperación de un aplicativo específico, activación de canales alternos de comunicación, entre otros.	Según se requiera																			
Respaldo	Se valida de forma colectiva la disponibilidad de las aplicaciones y/o sistemas de información, estas pruebas se pueden realizar de forma independiente por proceso.	Periódicamente																			
Simulaciones	Integra varios tipos de procedimientos críticos/o áreas dentro de la organización, bajo un escenario “artificial”. Por ejemplo, áreas como: evacuación, comunicación, procesos, TI, proveedores, entre otras. Puede o no ejecutarse en el ambiente alterno.	Al menos cada dos años																			
Funcional / actividades críticas	Prueba en el ambiente alterno establecido, de una o más actividades críticas, por un periodo preestablecido de tiempo. Lo anterior, sin generar impacto en la operación normal.	Al menos una vez al año																			

9.9. Gestión de Copias de Seguridad

Tipo	Descripción
Seguridad de la Información	Las copias de respaldo deben garantizar en todo momento la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de controles técnicos y administrativos que aseguren el acceso restringido a personal autorizado, la verificación

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción
	de la integridad de los datos y la correcta conservación en medios seguros que permitan su recuperación oportuna en caso de contingencia.
Respaldo de la Información	Toda información de la DIGSA contenida, registrada o almacenada en las bases de datos de los diferentes sistemas de información, servidores y sus respectivos equipos de almacenamiento, deberá ser protegida mediante copias de respaldo, las cuales se tratarán de acuerdo a los lineamientos legales, técnicos y administrativos determinados conforme a los niveles de clasificación de la información y riesgos asociados. Las copias deben almacenarse en medios seguros (cintas, NAS, discos duros).
Administración Copias de Respaldo	Los tiempos de preservación de las copias de respaldo, se determinarán por parte de la Entidad para cada caso, teniendo en cuenta los requerimientos técnicos, administrativos, jurídicos, las políticas de acceso y recursos, y el Inventario de Activos de Información.
Verificación Copias de Respaldo	Las copias de respaldo deberán ser recuperadas y documentadas, asegurando el funcionamiento y disponibilidad de la información conforme a los propósitos de la DIGSA. Asimismo, se deberán realizar pruebas periódicas de restauración para su verificación y mejoramiento continuo.
Seguridad de la Información	Los responsables de ejecutar las copias de respaldo, durante la generación, transporte, almacenamiento y custodia, deberán velar por la confidencialidad e integridad de la información, para que los datos no sean manipulados por personas no autorizadas. A su vez, deberán registrarse todas las actividades desarrolladas frente al tratamiento y manipulación de las copias para llevar la trazabilidad.
Administración Copias de Respaldo	Al cumplirse el tiempo de almacenamiento de las copias de respaldo, se deberá proceder a efectuar el borrado seguro, eliminación o destrucción de la información o del medio de almacenamiento, verificando que la información respaldada no sea accedida por personas no autorizadas. Todas estas actividades, se deben registrar y en caso de requerirse puedan ser consultadas, por medio del supervisor del contrato.
Organización y Gestión	La información que las áreas y/o los funcionarios almacenan en sus carpetas compartidas (file server) como respaldo, debe ser únicamente de carácter institucional y se encuentra restringido el almacenamiento de información personal (fotos, música, archivos personales y otros). La información personal de los funcionarios será borrada sin previo aviso de los servidores de la DIGSA.
Organización y Gestión	Se prohíbe el almacenamiento de información personal en servidores institucionales, garantizando que todos los datos alojados correspondan exclusivamente a información corporativa y cumplan con las normativas de seguridad y protección establecidas por la organización.
Verificación de Integridad, Disponibilidad	Se deben realizar pruebas periódicas de restauración para garantizar la efectividad de las copias de respaldo, y toda recuperación debe ser documentada y validada por el responsable técnico, asegurando trazabilidad y cumplimiento de los procedimientos establecidos.

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

Tipo	Descripción			
Gestión de Verificación	La Dirección General de Sanidad Militar debe garantizar la verificación periódica de la correcta ejecución de las copias de respaldo mediante el uso exclusivo de la consola administrativa proporcionada por el software institucional. Esta verificación es obligatoria para asegurar la integridad, disponibilidad y confiabilidad de la información respaldada, cumpliendo con los estándares de seguridad y continuidad operativa establecidos por la entidad.			
	Actividad	Responsable	Registro	Punto de control
	Identificar respaldo requerido	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Solicitud escrita por cada usuario	Logs de recuperación
	Verificar custodia externa	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Planilla de custodia	Validación de ubicación
	Solicitar respaldo al proveedor	Infraestructura	Correo y soporte	Registro de entrega
	Recepcionar medio externo	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Oficio o correo	Confirmación de recepción
	Configurar plataforma	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Formato de recuperación	Condiciones técnicas
	Ejecutar recuperación	Infraestructura	Logs y formato	Verificación de integridad

	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	De Gestión de Continuidad del Negocio DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-5	
	Vigente	Diciembre de 2025	Versión: 2

10. BIBLIOGRAFÍA

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (2018). Manual de Gobierno Digital. Bogotá

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES, Fortalecimiento de la Gestión TI en el Estado, <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

ISO/IEC/27001(2013). Sistema de Gestión de Seguridad de la Información. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, Bogotá D.C.