



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Junio 2021	Versión Inicial. NOTA PROASIG - PROPLAES: 1. Este documento fue revisado por PROASIG, cumple con los requisitos establecidos en el formato establecido por el Sistema Integrado de Gestión SIG, para aprobarlo en la SVE; PROPLAES libera el documento. 2. Dada la reestructuración de la DIGSA, se ajustaron las políticas de operación para el control de la información documentada de los procesos para el SIG, por lo que este documento queda en V1. 3. La información registrada en el documento es responsabilidad del proceso que lo emite.



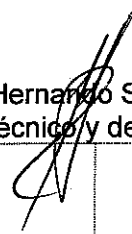
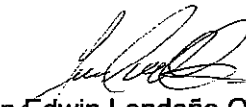
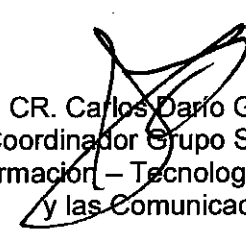
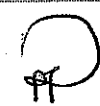
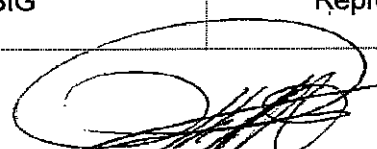
MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

CONTROL DE APROBACIÓN

Aprobó:	 CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	 C3. Jhon Edwin Londoño Quimbayo Gestor de Calidad PROGTIC	 CR. Carlos Darío González Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones DIGSA
	 SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG - PROASIG	 PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	 PD. Pedro Ignacio Rodríguez Castro Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones DIGSA Área Infraestructura, Redes y Comunicaciones DIGSA	



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

1. Presentación

Este procedimiento surge de la necesidad de aplicar en caso de contingencia lo correspondiente a la recuperación del activo más valioso de la Entidad como es la Información y por tanto la infraestructura tecnológica, por lo que se presenta como la Gestión de Continuidad del Negocio en Tecnologías de la Información.

2. Objetivo.

Definir los lineamientos para asegurar la recuperación efectiva de la infraestructura tecnológica de la Dirección General de Sanidad Militar-DIGSA, en aspectos de seguridad de la información, con el fin de generar una respuesta oportuna ante la ocurrencia de eventos de desastre o interrupción mayor que afecten la disponibilidad de las operaciones de la Entidad y por tanto gestionar la Continuidad del Negocio en Tecnologías de la Información.

3. Alcance - Aplicación

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.

4. 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.



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

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.
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.

5. Acrónimos

ANS:	Acuerdo de Niveles de Servicio. Acuerdo escrito entre el proveedor de servicios y el cliente sobre los niveles de servicio acordados entre ambas partes.
BIA:	Análisis de Impacto de Negocios.
CAD:	Centro Alterno de Datos.
CLOUD:	Nube (informática ofrecer servicios de computación a través de una red-Internet).
DIGSA:	Dirección General de Sanidad Militar.
DRP:	Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alternativo de procesamiento.
PCN:	Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder, recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

RTO: Tiempo objetivo de recuperación. Periodo de tiempo después de un incidente en el que un producto y/o servicio debe ser reanudado o los recursos deben ser reanudados.

SGSI: Sistema de Gestión de Seguridad de la Información.

SISAM: Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones

TI: Tecnología de la Información.

6. Políticas de Operación

6.1	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.
6.2	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.
6.3	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.
6.4	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.
6.5	Establecer procedimientos de recuperación viables en términos de costo-beneficio que permita restablecer la disponibilidad de la información para la Entidad.
6.6	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.
6.7	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.
6.8	Líder Alternativo 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.



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

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.

6.9

- 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 alterno.
- Verificar la disponibilidad de requerimientos de Hardware y Software necesarios para el centro de cómputo alterno.
- 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.

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.

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.



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

Evento	Descripción	Estrategia
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.

6.10	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.
6.10.1	Restauración de la infraestructura tecnológica en un nuevo centro de datos.
6.10.2	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. • 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 Alternativo 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 Alternativo 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 Alternativo 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 Alternativo 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 Alternativo de Datos (CAD). • Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Alternativo 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 Alternativo 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.
6.10.3	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.

	MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Procedimiento Gestión de Continuidad del Negocio en Tecnologías de la Información DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-18
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

	• 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.
6.10.4	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.
6.10.5	A continuación, se identifican los tipos de pruebas que pueden ser aplicados por Entidad.

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
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

 MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Procedimiento Gestión de Continuidad del Negocio en Tecnologías de la Información DIGSA MDN-COGFM-PROGTIC-DIGSA-PT.95.1-18 Proceso Gestión de Tecnologías de la Información y las Comunicaciones
---	---

Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución
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

7. Descripción de Actividades

Descripción	Registro(s)
1. Diseñar estrategias de recuperación tecnológica considerando la naturaleza y disponibilidad de recursos, realizando una evaluación detallada de: - Los recursos que son propios y se encuentran disponibles. - Posibles acuerdos recíprocos con otras oficinas o entidades. - Recursos que se pueden gestionar o tener disponibles con terceros. Responsable: Líder Principal de la Estrategia de Recuperación de TI.	• Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alterno de procesamiento. • Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder, recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.
2. Describir formalmente los escenarios que están cubiertos, al igual que las ventajas y desventajas (riesgos) de dichas estrategias. Responsable: Líder Principal de la Estrategia de Recuperación de TI / Equipo de Recuperación Tecnológica.	• Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alterno de procesamiento. • Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder,



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

Descripción	Registro(s)
	recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.
3. Establecer si el tiempo estimado de solución reportado supera el tiempo objetivo de recuperación (RTO), en cuyo caso se deberán iniciar las actividades de recuperación según el escenario de afectación. Responsable: Líder Principal de la Estrategia de Recuperación de TI / Equipo de Recuperación Tecnológica.	Matriz BIA "Análisis de impacto al negocio".
4. Evaluar el nivel de contingencia presentada y actuar de acuerdo al evento. Según la criticidad, se activará el plan de falla parcial para los servicios tecnológicos que aplique o se activará un Centro alternativo de operaciones tecnológicas destinado por el proveedor. Responsable: Líder Principal de la Estrategia de Recuperación de TI / Equipo de Recuperación Tecnológica / Comité de Seguridad de la Información o quien haga sus veces.	Procedimiento Gestión de Incidentes
5. Valorar 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 (alternativo) centro de datos. Responsable: Equipo de Evaluación de Daños de TI / Comité de Seguridad de la Información o quien haga sus veces.	Registros, evidencias.
6. Realizar la valoración 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 otro centro de datos geográficamente separado del Centro de Datos Principal y demás condiciones que la DIGSA considere necesarios. Responsable: Equipo de Evaluación de Daños de TI / Comité de Seguridad de la Información o quien haga sus veces.	- Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alternativo de procesamiento. - Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder, recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

Descripción	Registro(s)
7. Evaluar la estrategia de continuidad de la operación en caso de materializarse un desastre o situación que ponga en riesgo la disponibilidad de la infraestructura tecnológica de la Entidad. Responsable: Líder Principal de la Estrategia de Recuperación de TI.	• Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alternativo de procesamiento. • Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder, recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.
8. Ejecutar pruebas que permitan validar la estrategia de recuperación con el fin de realizar mejoras e identificar las fallas para ser corregidas, preparando a la Entidad para enfrentar incidentes reales. Responsable: Equipo de Evaluación de Daños de TI / Comité de Seguridad de la Información o quien haga sus veces.	Formato Plan de Pruebas
9. Activar la estrategia de recuperación según el evento presentado teniendo en cuenta las fases de planeación, alerta, recuperación y vuelta a la normalidad. Responsable: Líder Principal de la Estrategia de Recuperación de TI o quien haga sus veces.	• Plan de Recuperación de Desastres. Procedimientos detallados para recuperar la operación en un sitio alternativo de procesamiento. • Plan de continuidad del Negocio. Procedimientos documentados que guían a la Entidad para responder, recuperar, reanudar, restaurar a un nivel predefinido de operación debido a interrupción.
Fin	



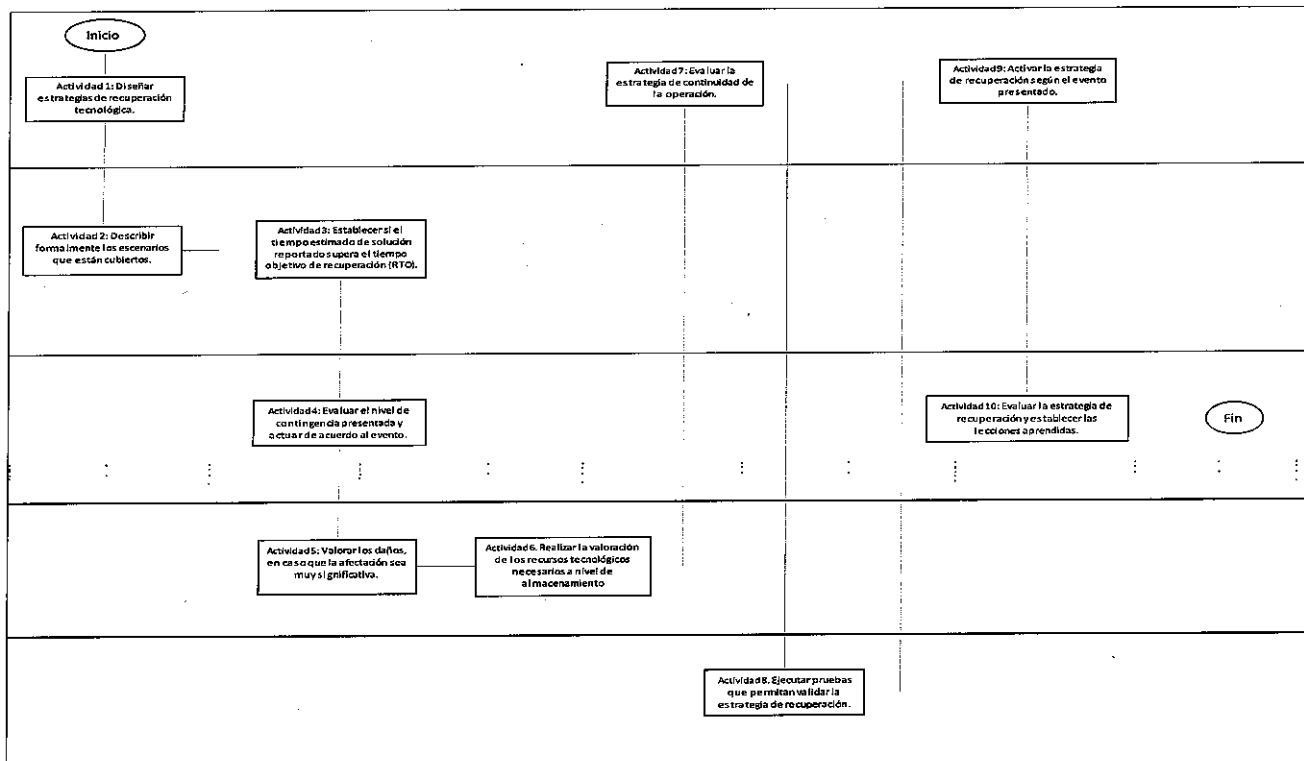
MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Continuidad del
Negocio en Tecnologías de la Información
DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-18

Proceso Gestión de Tecnologías de la
Información y las Comunicaciones

8. Flujograma



Flujograma del Procedimiento Gestión de Continuidad del Negocio.

9. Documentos y registros relacionados

9.1	Formato Plan de Pruebas.
9.2	Matriz BIA "Análisis de impacto al negocio".

Fin