

	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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		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.



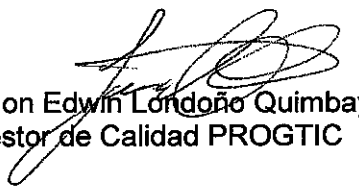
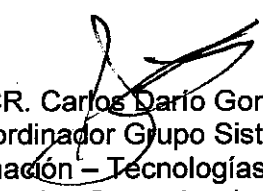
MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TÉCNICA Y DE GESTIÓN
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN – TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Copias de Respaldo
y Recuperación DIGSA

MDN-COGFM-PROGTIC-DIGSA-
PT.95.1-16

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. Jaime Ernesto Gutiérrez Plazas Grupo Sistema Integral de Información – Tecnologías de la Información y las 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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

1. Presentación

Este procedimiento surge de la necesidad de definir y documentar la Gestión de copias de respaldo y recuperación, como parte integral del Sistema de Gestión de Seguridad de la Información, enmarcados dentro del Modelo de Seguridad y Privacidad de la Información - MSPI.

2. Objetivo

Realizar copias de respaldo de la información de los servidores de datos, aplicaciones y correo electrónico, así como de la configuración y establecer las actividades de recuperación y custodia de las mismas.

3. Alcance - Aplicación

Este procedimiento inicia con la necesidad que toda información de la DIGSA contenida, registrada o almacenada en las bases de datos de sus 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, y termina con la verificación de la información, la cual haya sido copiada al medio de almacenamiento.

4. Definiciones

Administrador:	Es el funcionario designado por el responsable del grupo a cargo de
Software de backups:	brindar soporte y asistencia a la generación de copias de respaldo.
Archivos de Log:	Hace referencia al registro oficial de eventos durante un rango de tiempo en particular, es usado para registrar datos o información quien, que, cuando, donde y porque un evento ocurre para un dispositivo en particular o aplicación.
Centro de cómputo:	Sitio en el cual se encuentran alojados todos los equipos de cómputo y elementos activos de la red corporativa de la DIGSA (Servidores, SWITCHES, Elementos de comunicaciones, UPS, cableado, red eléctrica, etc.).
Copia de Respaldo:	(BACKUPS): Es la actividad de resguardar en forma segura la información contenida en un medio de almacenamiento de origen (disco duro) mediante un medio secundario de almacenamiento, distinto al origen (otro disco duro, servidor, etc.), y que puede utilizarse para restaurar el original después de una eventual pérdida de datos.
Copia Diferencial:	Es un proceso donde se copian todos los archivos que han sido creados y/o modificados desde la última copia completa.
Copia Incremental:	Es un proceso donde se copian todos los archivos que han sido creados o modificados desde la copia de respaldo anterior.
Medio Secundario de Almacenamiento	Dispositivo para guardar información con el fin de preservarla, tales como: cintas magnéticas, discos duros, CD, DVD, entre otros.
NAS:	(Network Attached Store) Equipo de Almacenamiento en red.
Servidor:	Es un equipo de cómputo cuyo propósito es proveer datos o servicios de modo que otros computadores los puedan utilizar.

	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 Copias de Respaldo y Recuperación DIGSA MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16 Proceso Gestión de Tecnologías de la Información y las Comunicaciones
---	--	--

5. Acrónimos

COGFM: Comando General de las Fuerzas Miliare.
DIGSA: Dirección General de Sanidad Militar.
SISAM: Grupo Sistema Integral de Información - Tecnologías de la Información y las Telecomunicaciones.
TRD: Tablas de retención documental.

6. Proveedor – entrada (insumo) para el desarrollo del procedimiento

Proveedor	Entrada - insumo
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).	El Modelo de Seguridad y Privacidad de la Información (MSPI).
Ministerio de Defensa Nacional	Directiva Permanente 913 del 19-04-2013, “Guía y procedimientos en tecnología de Información y Comunicaciones para el Sector Defensa”.
Ministerio de Defensa Nacional	Directiva Permanente 018 de 2014 “Políticas de Seguridad de la información para el Sector Defensa”.
Comando General de las FFMM	Directiva Permanente 154 de 2014 “Políticas de seguridad de la información para las Fuerzas Militares”.

7. Políticas de Operación

7.1	Toda información de la DIGSA contenida, registrada o almacenada en las bases de datos de sus 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.
7.2	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.
7.3	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.
7.4	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.
7.5	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.

	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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

7.6	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.
-----	--

8. Descripción de Actividades y puntos de control

8.1 Copias de respaldo

Descripción	Registro(s)
1. Definir o actualizar los estándares para la creación de copias de respaldo (BACKUPS), Custodia y Recuperación; incluyendo o modificando la información a respaldar de acuerdo a las solicitudes de las diferentes dependencias DIGSA. Responsable: Coordinador Grupo SISAM Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Estándares para la creación de copias de respaldo (BACKUPS), Custodia y Recuperación.
2. Configurar el software de backups de acuerdo a los parámetros de la Política de Creación de Copias de respaldo (BACKUPS), Custodia y Recuperación, teniendo en cuenta la información relevante que requiere ser respaldada y la normatividad vigente. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Logs registrados en la consola administrativa del software de backup, indicando el resultado satisfactorio o de error del respectivo backup.
3. Se verifica la ejecución de las copias de respaldo por medio de la consola administrativa que nos ofrece el software de Backups. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información. Ver punto de control de Copia de respaldo	Logs registrados en la consola administrativa del software de backup, indicando el resultado satisfactorio o de error del respectivo backup.
4. Revisar si se realizaron todas las tareas de BACKUPS de forma correcta. Si se realizan todas las tareas de forma correcta, continua con la actividad No. 7, si NO continua con la actividad No.5 por falla. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información	Consola administrativa del software de backup.

	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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

Descripción	Registro(s)
Ver punto de control de Copia de respaldo	
5. Aplicar las medidas correctivas a las tareas de BACKUPS con el falló. Si las tareas se ejecutaron satisfactoriamente: continúa con la actividad No. 7, sino continúa con la actividad No. 6 por persistencia del fallo. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Consola administrativa del software de backup.
6. Escalar el incidente al Grupo SISAM y/o delegado interno/externo. Si la tarea se solucionó continua con la actividad No. 7, si NO regresa al numeral 5. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Correo electrónico al encargado de la aplicación o proceso.
7. Realizar la custodia de la información de acuerdo a la Política de creación de copias de respaldo (BACKUPS), Custodia y Recuperación, en los elementos tecnológicos dispuestos. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Se almacena en Cintas ya sea diaria, semanal o mensual.
Fin	

Verificar la ejecución de las copias de respaldo a través de la consola administrativa que ofrece el software que cuanta la Dirección General de Sanidad Militar.

Puntos de control de Copia de respaldo

Actividad donde se controla:	Consola administrativa que ofrece el software de copias de seguridad.
Como se controla:	Logs registrados en la consola administrativa del software de backup, indicando el resultado satisfactorio o de error del respectivo backup.
Criterio de aceptación	Se mide en porcentaje la aceptación de las copias si es 100% se determina que fue exitoso.
Acción a tomar (si no cumple criterio de aceptación):	Si genera errores se verifica el tipo de error para establecer la acción a seguir.

	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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

Registro de la acción tomada:	Logs de almacenamiento que genera la consola administrativa.
Responsable del control:	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.

8.2 Recuperar Copias de respaldo

Descripción	Registro(s)
1. Identificar la copia de respaldo requerida para la restauración, previa descripción del sistema de información, base de datos y/o servidores a restablecer cuando se presente un evento adverso, incidente o solicitud de acuerdo a la Política de creación de copias de respaldo (BACKUPS), Custodia y Recuperación. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información.	Solicitud por correo electrónico o escrita del encargado de la aplicación o proceso indicando la solicitud de los archivos a restaurar.
2. Revisar si la copia de respaldo está en custodia externa. Si la información está en custodia externa, continuar con la actividad No. 3. Sino está en custodia externa, continuar con la actividad 5. Responsable: Profesional de Defensa con experticia la administración de software de respaldo en copias de información. Ver punto de control de Recuperar Copias de respaldo	Planilla-soporte de entrega de copias de respaldo en custodia externa.
3. Solicitar al proveedor o custodio la copia de respaldo a recuperar o medio externo. Responsable: Área de Infraestructura – Encargado de los Backups.	Correo electrónico encargado de los Backups y/o soportes de recibo de medios en custodia externa.
4. Recepcionar la copia de respaldo o medio externo entregado por el proveedor o custodio de las copias de respaldo. Responsable: Custodio de las copias de seguridad.	Correo electrónico o mediante oficio encargado de la custodia de los Backups en cinta magnética.
5. Configurar la plataforma tecnológica para proceder con la recuperación, con las condiciones requeridas para ejecutar la tarea y las pruebas. Responsable: Profesional de Defensa con experticia la administración de servidores.	Soportes ejecución tarea y /o Formato de Recuperación de BACKUPS.

	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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

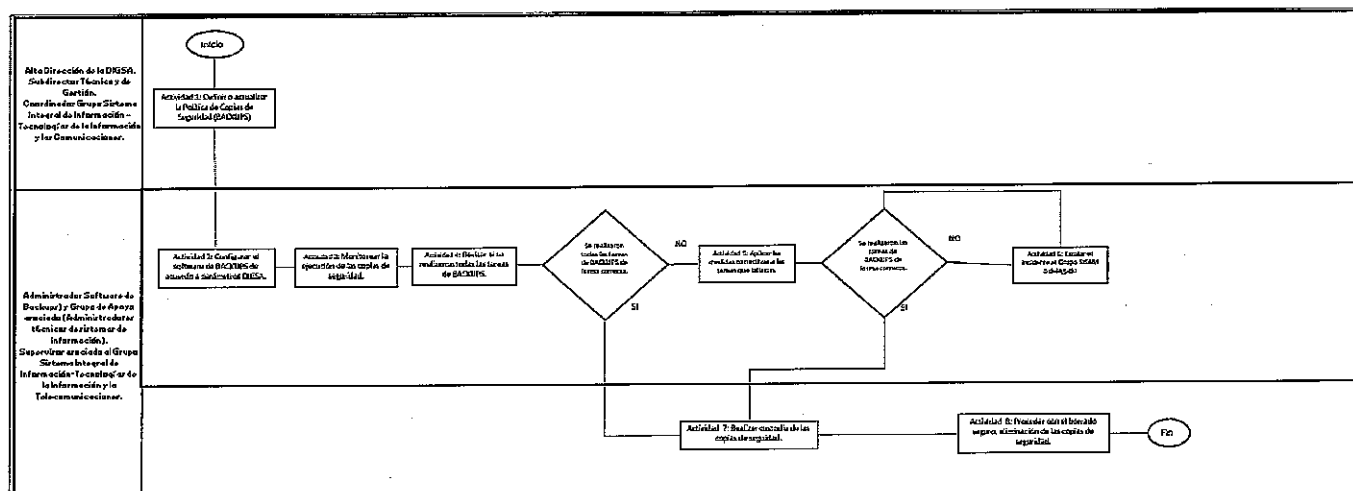
Descripción	Registro(s)
6. Ejecutar la tarea de recuperación en la plataforma tecnológica predispuesta. Si la recuperación es exitosa Finaliza la actividad. Sino continúa con la actividad No. 5. Responsable: Área de Infraestructura – Encargado de los Backups.	Log de ejecución de la tarea de recuperación. Soportes ejecución tarea y /o Formato de Recuperación de BACKUPS.
Fin	

Punto de control de Recuperar Copias de respaldo

Actividad donde se controla:	Consola administrativa que ofrece el software de copias de seguridad, indicando que fue exitosa el restablecimiento de la información solicitada.
Como se controla:	Logs registrados en la consola administrativa del software de backup, indicando el resultado satisfactorio o de error del respectivo backup.
Criterio de aceptación	Verificación en tamaño e integridad de la información restaurada.
Acción a tomar (si no cumple criterio de aceptación):	Enviar correo electrónico al dueño del proceso especificando observaciones de incumplimiento.
Registro de la acción tomada:	Logs de almacenamiento que genera la consola administrativa.
Responsable del control:	Profesional de Defensa con experticia la administración de software de respaldo en copias de información.

9. Flujograma

Flujograma del Procedimiento Gestión de Copias de Respaldo y Recuperación SGSI de la 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 Copias de Respaldo y Recuperación DIGSA
		MDN-COGFM-PROGTIC-DIGSA-PT.95.1-16
		Proceso Gestión de Tecnologías de la Información y las Comunicaciones

10. Documentos y registros relacionados

10.1	Correo electrónico del encargado de los Backups con soportes.
10.2	Formato Reporte de resultados de las tareas de BACKUPS.

Fin