

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28 PAGINA: 1 de 16

UNIVERSIDAD DE CUNDINAMARCA

**MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y
RECUPERACIÓN DE BACKUP DE INFORMACIÓN.**

**FUSAGASUGÁ
2025**

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28 PAGINA: 2 de 16

UNIVERSIDAD DE CUNDINAMARCA

**MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y
RECUPERACIÓN DE BACKUP DE INFORMACIÓN.**

Elaborado por: DIRECCIÓN DE SISTEMAS Y TECNOLOGÍA

**FUSAGASUGÁ
2025**

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 3 de 16

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	4
2.	OBJETIVO	5
2.1	OBJETIVOS ESPECÍFICOS.....	5
3.	ALCANCE.....	5
4.	DEFINICIONES	5
5.	LINEAMIENTOS PARA EL RESPALDO DE LA INFORMACIÓN	7
6.	ROLES Y RESPONSABILIDADES	8
6.1	EN SERVICIOS Y RECURSOS INFORMÁTICOS EN CUSTODIA DE LA UNIVERSIDAD DE CUNDINAMARCA	8
6.2	EN SERVICIOS INFORMÁTICOS PROVISTOS POR LA UNIVERSIDAD DE CUNDINAMARCA CUYA GESTIÓN DE LA INFORMACIÓN SEA PRINCIPALMENTE POR LOS USUARIOS.....	9
7.	DEFINICION DE CRITICIDAD DE SERVIDORES DE MAQUINAS VIRTUALES	9
8.	PROCESO DE BACKUP EN RECURSOS/SERVICIOS INFORMÁTICOS	10
8.1	DE BASES DE DATOS	10
8.2	DE SITIOS WEB.....	11
8.3	SERVIDORES (MÁQUINAS VIRTUALES Y FISICAS)	11
8.4	DE CORREO ELECTRÓNICO	11
8.5	DE SWITCHES.....	12
8.6	DE COMPUTADORES (ARCHIVOS DIGITALES)	12
9.	SEGUIMIENTO Y COMPROBACIÓN DE BACKUP	13
10.	ALMACENAMIENTO Y RECUPERACIÓN DE BACKUP EN RECURSOS/SERVICIOS INFORMÁTICOS	13
10.1	DE BASES DE DATOS.....	13
10.2	SERVIDORES (MÁQUINAS VIRTUALES Y FISICAS)	13
10.3	DE CORREO ELECTRÓNICO	14
10.4	DE SWITCHES (CONFIGURACIÓN)	14
10.5	DE COMPUTADORES (ARCHIVOS DIGITALES)	14
11.	NORMATIVIDAD.....	14
12.	BIBLIOGRAFÍA Y WEBGRAFÍA.....	15

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28 PAGINA: 4 de 16

1. INTRODUCCIÓN

A medida que los recursos informáticos y diversas tecnologías adquieren mayor relevancia dentro de las organizaciones, con el objetivo de incrementar la productividad de sus operaciones y gestionar sus activos, la información se ha consolidado como uno de los recursos más valiosos. Sin embargo, paralelamente, también han avanzado las actividades ilícitas destinadas a acceder o extraer datos de gran importancia, afectando directamente a las organizaciones víctimas de estos ataques. En este contexto, el presente documento tiene como objetivo establecer y detallar un conjunto de acciones que garanticen la confidencialidad, integridad y disponibilidad de la información, mediante una adecuada gestión de copias de seguridad que abarque toda la infraestructura de Tecnologías de la Información (T.I.) de la Universidad de Cundinamarca, considerando la normatividad nacional y los estándares internacionales establecidos.

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 5 de 16

2. OBJETIVO

Establecer las actividades necesarias para la ejecución de copias de seguridad (incluyendo el proceso, seguimiento y recuperación de respaldos) de los activos de información en la Universidad de Cundinamarca.

2.1 OBJETIVOS ESPECÍFICOS

- Asignar roles y responsabilidades durante toda la gestión de Backups.
- Establecer actividades para realizar Backups de diversas fuentes almacenadas tanto en servicios como en recursos informáticos.
- Verificar la integridad de los datos contenidos en las copias de seguridad a través de las actividades de seguimiento especificadas.
- Definir actividades de almacenamiento y recuperación de Backups con el fin de contribuir a la disponibilidad de la información.

3. ALCANCE

Asegurar que la información contenida en los Activos de la Información de la Universidad de Cundinamarca cuente con copias de seguridad, con el fin de garantizar la disponibilidad e integridad de la misma.

4. DEFINICIONES

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ARCHIVO DIGITAL: Es la información almacenada en algún medio que puede ser utilizada por aplicaciones de algún componente electrónico. Cada archivo se diferencia del resto debido a que tiene un nombre propio y una extensión que lo identifica.

BACKUP O COPIA DE SEGURIDAD: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos.

BASE DE DATOS RELACIONAL: Es una recopilación de elementos de datos con relaciones predefinidas entre ellos. Estos elementos se organizan como un conjunto

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 6 de 16

de tablas con columnas y filas. Las tablas se utilizan para guardar información sobre los objetos que se van a representar en la base de datos.

completa y las copias de seguridad incrementales posteriores.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTROL PREVENTIVO: Control que evita que se produzca un riesgo, error, omisión o acto deliberado.

DESASTRE: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

RECURSOS INFORMÁTICOS: Son los componentes de hardware y software que son necesarios para el buen funcionamiento de los dispositivos y periféricos que pertenecen a una red, en este caso se habla de Routers, Servidores y DVR'S (CCTV).

RESTAURACIÓN: Proceso mediante el cual se pone algo en su estado inicial, en este contexto a través de un medio extraíble que contiene la copia de seguridad.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

SERVICIOS INFORMÁTICOS: Es un conjunto de actividades que buscan responder a las necesidades de un cliente para este caso se refiere a los siguientes recursos: Bases de Datos, Sitio Web, Máquina Virtual, Correo Electrónico y Archivos Digitales.

	MACROPROCESO DE APOYO		CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA		VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS		VIGENCIA: 2025-04-28
			PAGINA: 7 de 16

5. LINEAMIENTOS PARA EL RESPALDO DE LA INFORMACIÓN

Las copias de respaldo de la información se realizarán de manera periódica en los recursos y servicios informáticos, utilizando los parámetros establecidos y las herramientas necesarias designadas por el área de Servicios Tecnológicos. Para prevenir la pérdida de información, se realizarán pruebas periódicas en las copias de seguridad para verificar que la información se encuentra almacenada correctamente.

RECURSO O SERVICIO INFORMÁTICO	HERRAMIENTA PARA REALIZAR BACKUP	DONDE SE ALMACENA EL BACKUP	ENCARGADO DE REALIZAR BACKUP	PERIODICIDAD DEL BACKUP	PERIODICIDAD DE PRUEBAS A LOS BACKUP
Servidores	Veeam Backup	Servidor dedicado para VeeamBackup	Administrador de servidores adscrito a la Dirección de Sistemas y Tecnología	Diaria, semana y mensual	Mensual
Bases de datos	Rman, export data pump y VeeamBackup	Servidor dedicado para VeeamBackup	DBA y administrador de servidores adscritos a la Dirección de Sistemas y Tecnología	Diaria	Bimestral
Correo electrónico	Tenant Microsoft 365	Nube (Tenant centro de administración 365)	Ingeniera administradora de Microsoft office 365	Por solicitud del usuario	Por solicitud del usuario
Equipos de computo	7zip, One Drive	Nube, disco duro externo de cada oficina o unidad que facilita la dependencia administrativa	Ingenieros del área de servicios tecnológicos / equipo de mantenimientos	Por solicitud del usuario.	Por solicitud del usuario.
Switches	Command line interface	SharePoint	Ingeniero del área de servicios tecnológicos encargados de redes	Semestral	Semestral

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28 PAGINA: 8 de 16

6. ROLES Y RESPONSABILIDADES

6.1 EN SERVICIOS Y RECURSOS INFORMÁTICOS EN CUSTODIA DE LA UNIVERSIDAD DE CUNDINAMARCA

- **SERVIDORES (MÁQUINAS VIRTUALES Y FÍSICAS)** Para las máquinas virtuales disponibles en la infraestructura tecnológica de la Universidad de Cundinamarca, el ingeniero administrador de servidores, adscrito a la Dirección de Sistemas y Tecnología, será el encargado de realizar los procesos de respaldo (Backup) y revisión.

Por otro lado, el respaldo y la revisión de las máquinas virtuales o servidores que se encuentren fuera de la infraestructura tecnológica de la Universidad de Cundinamarca serán responsabilidad de las oficinas que los utilicen para el cumplimiento de sus objetivos.

- **BASES DE DATOS** Si las bases de datos pertenecen a la infraestructura tecnológica de la Universidad de Cundinamarca, el Administrador de Bases de Datos (DBA) y el administrador de servidores, adscritos a la Dirección de Sistemas y Tecnología, serán los encargados de ejecutar los procesos de respaldo (Backup) y revisión.

Por otro lado, si las bases de datos forman parte de otros entornos o procesos fuera de la infraestructura tecnológica de la Universidad de Cundinamarca, la oficina responsable de su funcionamiento y custodia deberá cumplir con los planes de respaldo y revisión establecidos en este manual.

- **CORREO ELECTRÓNICO** La Dirección de Sistemas y tecnología será la responsable de la realización del seguimiento al correo institucional bajo el dominio @ucundinamarca.edu.co cuyas cuentas tiene proceso de Backups y revisión por el proveedor contratado.
Los demás correos que las oficinas utilicen estas deberán realizarle el proceso de Backups y revisión correspondiente.

- **EQUIPOS DE COMPUTO** Los ingenieros del equipo de Mantenimiento, adscritos a la Dirección de Sistemas y Tecnología, serán responsables de realizar las copias de seguridad de la información de los equipos de cómputo (Administrativos) incluidos en el cronograma de mantenimientos preventivos vigente. Asimismo, cada usuario deberá garantizar el correcto almacenamiento de su información en OneDrive.

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 9 de 16

- **SWITCH** Los ingenieros administradores de red adscritos a la Dirección de Sistemas y Tecnología serán los responsables de realizar el proceso de Backup y de su respectivo almacenamiento.

6.2 EN SERVICIOS INFORMÁTICOS PROVISTOS POR LA UNIVERSIDAD DE CUNDINAMARCA CUYA GESTIÓN DE LA INFORMACIÓN SEA PRINCIPALMENTE POR LOS USUARIOS.

El proceso de Backups de los correos electrónicos institucionales es responsabilidad de cada usuario, el cual debe realizar el siguiente proceso si requiere esta información: Se debe dirigir a la oficina de Servicios Tecnológicos y hacer el requerimiento de este proceso, que se ejecutará por medio de cada buzón de correo generando un archivo **.pst** que se deberá importar a otro correo electrónico para poder visualizarlo.

7. DEFINICIÓN DE CRITICIDAD DE SERVIDORES DE MÁQUINAS VIRTUALES

La Universidad de Cundinamarca dispone de un total de 83 servidores, distribuidos entre sistemas operativos Windows y Linux, que desempeñan diversas funciones esenciales para los servicios internos de la institución. Entre estos servicios se incluyen la página web institucional, la plataforma y otros sistemas utilizados por la comunidad académica, administrativa y personal externo.

En línea con la misión institucional, que se fundamenta en ser una organización social del conocimiento y el aprendizaje, democrática, autónoma, formadora y agente de la transmodernidad, los servicios integrados en los servidores se clasifican según su criticidad en tres niveles:

- **Criticidad alta:** Corresponde a aquellos servicios y servidores cuya interrupción, debido a fallos de software o hardware, un ataque de ransomware, corrupción de datos u otras situaciones comprometedoras, impediría que la universidad cumpliera con su misión y objetivos fundamentales. Estos servicios son esenciales para el funcionamiento y la continuidad de la institución.
- **Criticidad media:** Engloba los servicios y servidores que, si bien sufre una afectación por fallos de software o hardware, ataques de ransomware o corrupción de información, solo afectarían a un grupo específico de usuarios. No obstante, su interrupción no comprometería directamente el cumplimiento de la misión institucional, pero podría impactar el desempeño de actividades relacionadas con ciertos usuarios o áreas.

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 10 de 16

- **Criticidad baja:** Incluye los servicios y servidores cuya afectación, ya sea por fallos técnicos o incidentes de seguridad, no tendría un impacto significativo en los servicios generales de la institución. Aunque su interrupción podría generar inconvenientes menores, no afectaría de manera crucial el cumplimiento de la misión ni interrumpiría operaciones clave de la universidad.

Esta clasificación de la criticidad de los servicios ayuda a priorizar las estrategias de seguridad, respaldo y recuperación, permitiendo a la universidad mantener la continuidad operativa y garantizar la integridad de los servicios que ofrecen a su comunidad.

8. PROCESO DE BACKUP EN RECURSOS/SERVICIOS INFORMÁTICOS

Ante algún posible desastre o incidente de seguridad, los activos de T.I. como los mencionados a continuación pueden resultar expuestos comprometiendo la confidencialidad, integridad y disponibilidad de la información. A continuación, se especifican las actividades a realizar para minimizar la probabilidad de que se materialice un riesgo de seguridad.

8.1 DE BASES DE DATOS

Para realizar proceso de Backups en bases de datos se debe tener una tarea automática que se ejecute diariamente en horario nocturno. A continuación, los dos tipos de Backups que se realizan.

- **EXPORT:** Para la copia de seguridad se realiza de manera diaria, a la 1:00 de la mañana.
- **RMAN:** Para la copia de seguridad se realiza diariamente a las 9 de la noche, a excepción de los archivos transaccionales se realiza cada 6 horas y se tiene considerado que esto cambie para que se realice con una periodicidad de 30 minutos.

Estos Backups arrojan logs que se almacenan en el servidor productivo en estas rutas:

- /backups/expdp/BDUNICUN
- /backups/rman/BDUNICUN
- G:\DATABASE\PROFIN10\LOGS

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 11 de 16

Una vez los Backups sean almacenados en las rutas definidas se realiza la vinculación con la herramienta VeeamBackup para poder llevar los backups del servidor productivo a la herramienta y así almacenarlos en el espacio disponible.

En estos logs se visualiza lo siguiente:

- **Estado de los filesystem:** Es el almacenamiento disponible y si se requiere depurar o adquirir más almacenamiento.
- **Ultimo reinicio del servidor:** Registro de las caídas de los servidores.
- **Estado de los procesos de Oracle:** Revisión de que los procesos y servicios estén funcionando correctamente.
- **Validación de tamaño del tablespace:** Espacio utilizado y asignado para los archivos.
- **Ultimo reinicio base de datos.**
- **Estado backups:** Si fue exitoso o tuvo algún error.
- **Validación espacio de los discos de ASM:** Valida el estado de los discos, redundancias y balanceo de operaciones.

8.2 DE SITIOS WEB

En los sitios web institucionales se debe realizar dos tareas de Backups respectivamente: La primera aplicará para las correspondientes bases de datos, se llevará a cabo diariamente y el tipo de Backups será completo. La segunda comprende el directorio raíz del sitio web, se ejecutará semanalmente después del mediodía a excepción de actualizaciones o modificaciones considerables, en estos casos se ejecutará la tarea antes de los ajustes a realizar.

8.3 SERVIDORES (MÁQUINAS VIRTUALES Y FÍSICAS)

Para realizar el proceso de copia de seguridad de un servidor (máquina virtual) que se encuentre alojado en la Infraestructura Tecnológica de la Universidad de Cundinamarca, se deberá definir en que criticidad se encuentra la máquina para así mismo asignarle una periodicidad las cuales pueden ser mensuales, semanales o diarias, una vez se defina la criticidad y la periodicidad, haciendo uso de la herramienta VeeamBackup se incluiría a la maquina en uno de los trabajos previamente creados y configurados, los cuales se ejecutan automáticamente según la periodicidad a cierto horario con el fin de prevenir saturaciones, estos backups son almacenados en la misma herramienta la cual cuenta con 25TB de almacenamiento y se encuentra en un entorno físico y de red seguro.

8.4 DE CORREO ELECTRÓNICO

Al ser un servicio de carácter institucional, cada usuario debe establecer la frecuencia y la forma en que realiza Backups de la información asociada a su cuenta de correo, esto tomando en cuenta que el servicio Exchange sea local o hibrido, una

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28 PAGINA: 12 de 16

recomendación puede ser, sincronizar la cuenta de correo en un programa cliente de correo electrónico como Microsoft Outlook de escritorio, este programa genera un archivo con extensión **.pst** que contiene la configuración y los correos electrónicos asociados a la cuenta. Este archivo puede ser almacenado en un medio externo o en un servicio de almacenamiento en la nube (Ejemplo: OneDrive) como copia de seguridad y por lo menos la tarea de Backups debe realizarse cada mes.

Adicional a la recomendación anterior y tomando como referencia que el servicio de Exchange en la universidad es totalmente nube, Microsoft cuenta con herramientas de recuperación de desastres, los cuales tienen cobertura sobre todos los usuarios del servicio (empresas, organizaciones) de Exchange server online, por tal motivo los correos de la organización pueden tener disponibilidad 24/7 desde cualquier equipo, puesto que los respaldos de estos servicios, están en regiones separadas por cientos de km, y ante la falla de uno, entra en funcionamiento un segundo, y hasta un tercer servicio de replicación de productos, por tal motivo la creación de un backup local del correo no es netamente necesaria. Sin embargo, para términos de auditoría o consultas de correo, el tenant de Microsoft 365, con la herramienta de cumplimiento de Microsoft, permite realizar las consultas y generar los archivos descargables **.pst** de los correos de los usuarios activos y no activos dentro de la organización.

8.5 DE SWITCHES

Para el proceso de Backups de Switches se hace de acuerdo a los cronogramas de mantenimiento mediante el EPIr001 “Mantenimiento Preventivo de Cuartos de Telecomunicaciones y Centros de Distribución Principal (TR’s y CD’s)” por semestre y para las sedes, seccionales y extensiones, es decir en cada sesión de mantenimiento se hace el proceso de backups de forma manual a los switches de distribución y acceso que se encuentran en los TR’s y CD’s en las fechas establecidas y proyectadas de acuerdo al cronograma.

8.6 DE COMPUTADORES (ARCHIVOS DIGITALES)

La información contenida en los equipos será responsabilidad del usuario que hace uso de este. En cuanto al sistema operativo y sus utilitarios la Dirección de Sistemas y Tecnología los tendrá guardados en un repositorio externo de almacenamiento en sus últimas versiones.

El funcionario encargado de los archivos deberá hacer una debida clasificación de estos obedeciendo a lo estipulado en la tabla de retención documental. Este proceso lo realizara el gestor que crea y gestiona su información, esto se realiza mediante la correcta sincronización de la herramienta OneDrive en el dispositivo con el correo del área institucional personal o del área, así mismo por parte de la Dirección de Sistemas y Tecnología se recomienda hacer uso de la herramienta SharePoint la cual cuenta con 4TB de almacenamiento por usuario.

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 13 de 16

En caso de solicitarse un Backup, el cual requiera el acompañamiento del personal del área de servicios tecnológicos, esta solicitud deberá realizarse mediante la plataforma institucional en el módulo de mesa de servicios a un clic, la oficina solicitante deberá facilitar al personal un disco duro para realizar el proceso y almacenar dicho Backup.

9. SEGUIMIENTO Y COMPROBACIÓN DE BACKUP

Cada vez que se realiza una tarea de Backups independientemente de la fuente de datos a respaldar, es necesario verificar la integridad de la copia de seguridad utilizando la lista de verificación que contiene los siguientes elementos:

- Fecha de ejecución del Backups.
- Nombre del activo que fue respaldado (nombreBD, directorio de usuario de dominio, nombre de sitio web, nombre del equipo en el dominio, etc.).
- Tamaño del archivo o directorio.
- Ubicación del Backups, este debe ser una ubicación específica diferente a la del servidor, se recomienda un disco externo o en la nube (Ejemplo: OneDrive).
- Para finalizar el seguimiento, se debe llevar registro de cada proceso de Backups realizado. Este registro será la bitácora de copias de seguridad general.

10. ALMACENAMIENTO Y RECUPERACIÓN DE BACKUP EN RECURSOS/SERVICIOS INFORMÁTICOS

10.1 DE BASES DE DATOS

Los archivos de base de datos relacionales serán almacenados en el almacenamiento cifrado de la herramienta VeeamBackup acompañados de su hash de creación y su permanencia en los mismos será dada su complejidad e importancia, se recomienda por lo menos sea de 6 meses. Para restaurar una base de datos el profesional encargado de esta actividad deberá atender la solicitud hecha a su jefe directo en la cual se indica como mínimo el nombre de la base de datos y la fecha de ejecución de proceso de Backups.

10.2 SERVIDORES (MÁQUINAS VIRTUALES Y FÍSICAS)

Las máquinas virtuales estarán almacenadas en un dispositivo externo cuyo disco estará cifrado, el tiempo de permanencia de cada máquina virtual será dada según su complejidad e importancia se recomienda sea mínimo 6 meses a partir de su fecha de almacenamiento. Para restaurar una máquina virtual el profesional encargado deberá atender la solicitud hecha a su jefe directo en la cual se indica como mínimo

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 14 de 16

el nombre de la máquina virtual o su sistema operativo y la fecha en la cual se quiere restablecer. Toda recuperación se deberá registrar en una bitácora.

10.3 DE CORREO ELECTRÓNICO

Al ser un servicio de carácter institucional ofrecido por la Universidad de Cundinamarca, cada usuario tiene libertad de escoger el medio de almacenamiento en el cual reposará su copia de seguridad (disco duro externo, OneDrive, etc.), si se elige un disco duro externo, se recomienda que al menos la carpeta en la que se guardará la copia de seguridad esté cifrada. Para restaurar el correo electrónico teniendo presente el numeral 7.4 de este manual, es necesario importar el archivo de datos con extensión .pst y asociarlo a la cuenta de correo sincronizada previamente.

10.4 DE SWITCHES (CONFIGURACIÓN)

El Backup de la configuración de Switches quedará en el repositorio del SharePoint cuya unidad de almacenamiento estará cifrada para mayor seguridad. Para recuperar la configuración el profesional encargado deberá atender una solicitud hecha a su jefe directo en la cual se indique como mínimo marca y modelo de dispositivo de red, además de la fecha en la cual se quiere restablecer la configuración.

10.5 DE COMPUTADORES (ARCHIVOS DIGITALES)

Las copias de seguridad serán almacenadas en un dispositivo externo (Disco duro) del área solicitante, los cuales estarán cifrados y serán de custodia de los mismo, por lo cual en caso de solicitarse un archivo, directorio o carpeta la oficina pertinente deberá acceder al dispositivo donde se almaceno el Backup y en caso de ser necesario solicitar mediante mesa de servicios a un clic el apoyo del personal de servicios tecnológicos.

11. NORMATIVIDAD

- Artículo 15 de la Constitución Política de Colombia.
- Ley 1273 de 2009, protección de la información y los datos frente a delitos informáticos.
- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Resolución 000050 del 7 de mayo de 2018.
- Norma ISO/IEC 27001:2013 dominio A.12 sección 3, copias de seguridad de la información.

	MACROPROCESO DE APOYO	CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA	VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS	VIGENCIA: 2025-04-28
		PAGINA: 15 de 16

12. BIBLIOGRAFÍA Y WEBGRAFÍA

- <http://www.iso27000.es/glosario.html>
- https://es.wikipedia.org/wiki/Copia_de_seguridad
- <https://aws.amazon.com/es/relational-database/>

	MACROPROCESO DE APOYO		CÓDIGO: ASIM008
	PROCESO GESTIÓN SISTEMAS Y TECNOLOGÍA		VERSIÓN: 7
	MANUAL PARA REALIZAR PROCESO, SEGUIMIENTO Y RECUPERACIÓN DE BACKUPS		VIGENCIA: 2025-04-28
			PAGINA: 16 de 16

CONTROL DE CAMBIOS						
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO		
	AAAA	MM	DD			
1	2018	12	13	Emisión del documento.		
2	2019	04	09	Cambios generales.		
3	2021	12	07	Se actualiza documento en cumplimiento del manual de imagen institucional.		
4	2023	10	31	Se realiza actualización de los recursos y servicios tecnológicos a los que se realizan los backups. También se agregan lineamientos para cumplir con la norma ISO:27001 Numeral 12.3.1		
5	2024	08	21	Según la resolución rectoral 074 del 22 de julio del 2024, dando cumplimiento a la ley 2345 del 2023 "chao marcas" y dando alcance a la circular 006 "Cambio de identificador visual en los documentos de gestión documental" se realiza el cambio de logo en el documento.		
6	2025	04	04	Se agrega el apartado número 7 definición criticidad de máquinas virtuales		
7	2025	04	28	Se actualiza la información de los apartados número 5, 6, 8, 10 y 11. Se elimina el antiguo numeral 9 (Proceso de backup en recursos informáticos) y numeral 12 (Almacenamiento y recuperación de backup en recursos informáticos).		
ELABORÓ						
NOMBRES Y APELLIDOS			CARGO			
Lady Carolina Sánchez Barrera			Profesional IV			
Carlos Alberto Torres Barrios			Profesional III			
Kevin Farid Cubillos Castiblanco			Técnico III			
Oscar David Casallas Bernal			Técnico			
REVISÓ						
NOMBRES Y APELLIDOS			CARGO			
Jeniffer Castillo Fernández			Profesional Director de Área I			
APROBÓ (GESTOR RESPONSABLE DEL PROCESO)						
NOMBRES Y APELLIDOS		CARGO		FECHA		
				AAAA	MM	DD
Ana Lucia Hurtado Mesa		Directora de Sistemas y Tecnología		2025	04	28