1. Objetivo, alcance y convenciones

Objetivo	Contar con copias de seguridad de los diferentes sistemas de información del Ministerio como son: archivos, aplicaciones y bases de datos con el fin de poder recuperar la información en caso de un incidente.
Alcance	Inicia con la solicitud de incluir un servidor, aplicación o base de datos a las políticas de Backup y culmina con la solución y confirmación del cierre de esta.

Convenciones	**Punto de Verificación**	**Nota**	**Evidencias**	**Interacción con otros procesos**	**Tiempos**	
					Mínimo	**Máximo**
						

2. Disposiciones Generales

1. POLÍTICAS GENERALES

- El horario de atención de la Mesa de Servicios es de lunes a sábado entre las 7:00 a.m. y las 9:00 p.m. en jornada continua.
- Todos los servidores y bases de datos deben tener una política de Backup, como mínimo de manera mensual.
- Todo sistema no transaccional debe tener un respaldo semanal, mensual y anual.
- Los ambientes de pruebas y certificación podrán tener como máximo un respaldo semanal, es decir no podrán tener respaldos diarios.
- Las bases de datos deben estar respaldadas por integración y el servidor que las contiene debe tener un respaldo mensual.
- Se deben realizar pruebas de restauración periódicamente para garantizar el correcto funcionamiento de las copias de seguridad.
- Las copias de seguridad deberán almacenarse en un lugar diferente a la sede donde se han realizado el respaldo.

2. Disposiciones Generales

- Mediante una solicitud o una orden de cambio se podrá solicitar la inclusión de un servidor o base de datos a las políticas de Backup.
- Los coordinadores de la oficina de tecnología son los únicos autorizados a solicitar la modificación de una política de Backup existente.
- No se podrá eliminar o desactivar una política de Backup asociada a un sistema de información que se encuentre activo.
- Se debe llevar un registro de las políticas de Backup donde se indique el tipo de respaldo, la retención, quien lo solicito, numero de RFC o solicitud de inclusión en las políticas de Backup.
- Todas las políticas de Backup deben tener una retención de 3 años.

2. TÉRMINOS Y DEFINICIONES

Los términos y definiciones mencionados a continuación se toman con base al Glosario de términos de ITIL en español[1]:

- **BACKUP:** Es una copia de los datos que sirve de protección en caso de pérdida de la integridad o la disponibilidad de los originales.

- **ACUERDOS DE NIVELES DE SERVICIO (ANS):** Es un contrato escrito entre un proveedor de servicio y el cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

- **SOLICITUD:** Es una petición formal por parte de un usuario para que algo sea provisto - por ejemplo, una solicitud de información o asesoría; restablecer una contraseña, o instalar una estación de trabajo para un nuevo usuario. Las solicitudes de servicios son gestionadas por el proceso de cumplimiento de solicitud, generalmente en conjunto con el service desk. Las solicitudes de servicio pueden estar vinculadas con una solicitud de cambio como parte del cumplimiento de la solicitud.

[1] AXELOS Limited. 2011. ITIL español (Latinoamericano) glosario. Ed. 1

2. Disposiciones Generales

- **RFC - SOLICITUD DE CAMBIO:** Es una propuesta formal para hacer un cambio. Incluye los detalles del cambio propuesto, y puede ser registrado en papel o electrónicamente. A menudo, el término es mal utilizado para referirse a un registro de cambio, o al propio cambio.

- **CONFIDENCIALIDAD:** Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. En general, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

- **DISPONIBILIDAD:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

- **INTEGRIDAD:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. En general, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, es decir la información debe ser correcta y completa.

- **ESCALAMIENTO:** Es cuando una actividad obtiene recursos adicionales necesarios para cumplir con los objetivos de nivel de servicio o con las expectativas del usuario. Un escalamiento puede ser necesario en cualquier proceso de gestión de servicio de TI, comúnmente se asocia a la gestión de incidentes, gestión de problemas y la gestión de atención de quejas de los usuarios. Hay dos tipos de escalamiento: escalamiento funcional y escalamiento jerárquico.

- **INFRAESTRUCTURA DE TI:** Es todo el hardware, software, redes, instalaciones, etc., que se necesitan para desarrollar, probar, entregar, monitorear, controlar o dar soporte a servicios de TI y a aplicaciones. El término incluye toda la tecnología de información, pero no a las personas, procesos y documentación asociados.

- **ITIL:** Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Informatión Technology Infrastructure Library), es un conjunto de conceptos y buenas prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

2. Disposiciones Generales

- **MEN**: Ministerio de Educación Nacional.
- **MESA DE SERVICIOS**: Es una unidad funcional con una estructura que tiene la responsabilidad de mantener la comunicación con usuarios finales y responder de una manera oportuna, eficiente y con alta calidad a las solicitudes de servicios de TI.
- **OTSI:** Oficina de Tecnología y Sistemas de Información.
- **TI**: "Tecnologías de Información" Se conoce como Tecnologías de Información a las herramientas para el manejo y procesamiento de información, específicamente para la captura, transformación, almacenamiento, protección y recuperación de datos e información.[2]
- **BACKUP FULL:** Es una copia completa de todo el conjunto de datos (servidor o base de datos)
- **BACKUP INCREMENTAL:** Es el respaldo de los datos que han cambiado desde la última copia de seguridad.
- **BACKUP TIPO SNAPSHOT:** Conserva el estado y los datos de una máquina virtual en el momento que toma un snapshot.
- **BACKUP TIPO FILE SYSTEM**: Este tipo de backup respalda una ruta especifica de la máquina virtual.
- **BACKUP TIPO INTEGRACIÓN:** Este tipo de backup este asociado a las bases de datos y sus diferentes motores, permitiendo tomar la copia de seguridad de los datos de forma autónoma y directa sobre el motor y las instancias que lo conforman.

3. FUNCIONES ROLES

GESTOR DE BACKUP

- Realizar seguimiento al procedimiento y al cumplimiento de los ANS durante la gestión de las solicitudes o RFC.
- Velar porque el procedimiento se siga y ser guía a la operación en las dudas que tengan respecto al mismo.

[2] MinTic. *¿Qué es una carrera TI?* - Talento Digital. Talento Digital MinTic. https://talentodigital.mintic.gov.co/

2. Disposiciones Generales

- Velar porque cada política es ejecutada de manera satisfactoria y en caso de falla volver a ejecutarla.

4. MATRIZ RACI

Actividades	Solicitante (Usuarios internos MEN - Operador)	Agente Mesa de Servicios (Operador de Servicios TI)	Analista Soporte Técnico (Operador de Servicios TI)	Gestor de Backup (Operador de Servicios TI)	Gestor de cambio (Operador de Servicios TI)	Gestor de aplicaciones (Operador de Servicios TI)	Gestor de base de datos (Operador de Servicios TI)	Gestor de infraestructura (Operador de Servicios TI)
Generar requerimiento RFC o solicitud	R							
Recibir y validar la solicitud		R/A		R/A	R/A			
Notificación por correo de la actividad realizada (inclusión, eliminación o restauración)	I			R/A				
Alistamiento de servidores				I				R/A
Restauración de servidores				R/A				I

2. Disposiciones Generales

Configuración de aplicación				I		R/A		
Configuración de base de datos				I		I	R/A	
Pruebas funcionales	R/A			I				
Documentar en CA, adjuntar evidencias y resolver caso	I			R/A				

R: Responsable de la correcta ejecución de la actividad.
A: Responsable por la calidad y resultados de la actividad.
C: Consultado (Brinda información o conocimiento)
I: Informado (recibe información sobre la ejecución o calidad de la actividad)

5. ENTRADAS Y SALIDAS DEL PROCEDIMIENTO

A continuación, se relacionan las diferentes entradas y salidas de la gestión de incidentes de los servicios de TI administrados por el operador:

ENTRADAS PROCEDIMIENTO	SALIDA PROCEDIMIENTO
• Procedimiento de cambios.	• Solicitudes de cambio
• Procedimiento de gestión de solicitudes.	• Solicitudes registradas, gestionadas y solucionadas.
• Eventos críticos	• Solicitudes de cambio

2. Disposiciones Generales

• Fallas del servicio	• Incidentes registrados, gestionados y solucionados.
• Fallas derivadas de cambios.	• Solicitudes de cambio
• Fallas derivadas de solicitudes.	• Solicitudes registradas, gestionadas y solucionadas.

6. PROCEDIMIENTOS ASOCIADOS

PROCEDIMIENTO	DESCRIPCIÓN
Gestión de Solicitudes	Este procedimiento se activará cuando el Analista de la mesa de servicios detecte que lo reportado por el usuario no corresponde con una afectación que se deba manejar como un Incidente al no degradar o interrumpir la calidad de un servicio.
Gestión de Eventos	Los incidentes pueden ser reportados por las herramientas de monitorización de eventos. Los eventos críticos que impacten los servicios TIC del ministerio serán reportados como incidentes y serán gestionados por medio de la gestión de incidentes.
Gestión de Cambios	Cuando se requiere un cambio para implementar una solución temporal o una resolución, éste necesitará registrarse como un RFC, y procesarse a través de la Gestión de Cambios. A su vez, la Gestión de Incidencias podrá detectar y resolver incidencias que surjan de cambios fallidos.
Gestión de la Disponibilidad	Esta Gestión usará los datos de Gestión de Incidencias para determinar la disponibilidad de los servicios de TI y determinar dónde se puede mejorar el ciclo de vida de la incidencia.

2. Disposiciones Generales

Gestión de Incidentes Mayores	Esta gestión se activará las veces en que el incidente reportado impacte de manera negativa y degrade los servicios ofrecidos por el MEN.
Gestión de Incidentes de Seguridad de la Información	Esta gestión se activará cuando se evidencie una afectación que atente contra la Confidencialidad, Integridad y Disponibilidad de los Activos y servicios del MEN.

7. DOCUMENTOS RELACIONADOS

- ST-PR-14 Procedimiento Gestión de Incidentes
- ST-PR-17 Procedimiento Gestión de incidentes mayores
- ST-PR-18 Procedimiento Gestión de incidentes de seguridad de la información
- ST-PR-12 Procedimiento Gestión de cambios
- ST-PR-05 Procedimiento Gestión de Solicitudes

SOLICITAR BACKUP				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
1	**CREACIÓN DE LA SOLICITUD O RFC** El usuario interno o del operador realiza la solicitud de un Backup, esta puede corresponder a: 1. Lanzar una tarea de Backup: continuar con la actividad 2. 2. Inclusión a las políticas de Backup: Continuar con la actividad 4. 3. Restauración de un Backup de algún sistema de información: Continua con la actividad 10.	Usuarios Internos y/u operador de servicio	Permanente	Herramienta de Gestión CA
2.	**EJECUTAR TAREA DE BACKUP** Se lanza la tarea y una vez culminada se debe enviar evidencia de la actividad al usuario que ha realizado la solicitud.	Gestor de Backup	3 horas	Herramienta de Gestión CA
3.	**CIERRE DE CASO** Se documenta y cierra el caso en la Herramienta de Gestión CA Service Desk. Finaliza procedimiento	Gestor de Backup	0.5 hora	Herramienta de Gestión CA
4	**NOTIFICAR CASO O RFC** El usuario interno o del operador, solicita la inclusión de un servidor o base de datos a las políticas de Backup donde debe especificar el tipo de Backup que se debe realizar (Tipo Snapshot, File System y por Integración) y la periodicidad (diario, semanal, mensual y anual).	Usuarios Internos y/u operador de servicio	Permanente	Herramienta de Gestión CA Service Desk Manager.

	Si la solicitud corresponde a un ambiente de pruebas o certificación el respaldo no podrá ser diario, de preferencia debe ser mensual.			
5	**VALIDAR EL TIPO DE BACKUP A CONFIGURAR** Dependiendo del tipo de backup que se esté solicitando se tomara una acción diferente, las opciones que se tienen son: Tipo snapshot - Continuar con la actividad 6 Tipo File System - Continuar con la actividad 6 Tipo Integración – Continuar con la actividad 8	Gestor de Backup	0.5 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.
6	**INCLUIR SERVIDOR O FILE SYSTEM EN LAS POLITICAS DE BACKUP** Se configura la herramienta para realizar la copia de seguridad con la periodicidad solicitada.	Gestor de Backup	0.5 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.
7	**PROCEDER CON EL CIRRE DE LA SOLICITUD O DE LA ORDEN DE CAMBIO** Se debe enviar evidencia de la configuración realizada al usuario que ha realizado la solicitud y actualizar el archivo de políticas de Backup. Finaliza procedimiento	Gestor de Backup	0.5 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
8	**INCLUIR BASE DE DATOS POR INTEGRACIÓN** El gestor de Backup debe coordinar con los especialistas de redes y sistemas operativos la configuración de una tarjeta de	Gestor de Backup	2 hora	

	red con direccionamiento de Backup y la instalación del agente para su posterior configuración.			Herramienta de Gestión CA Service Desk Manager.
9	**PROCEDER CON EL CIRRE DE LA SOLICITUD O DE LA ORDEN DE CAMBIO** Se debe enviar evidencia de la configuración realizada al usuario que ha realizado la solicitud y actualizar el archivo de políticas de Backup. Finaliza el procedimiento	Gestor de Backup	0.5 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.

3. Descriptivo del Procedimiento				
RESTAURACIÓN DE UN BACKUP				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
10	**NOTIFICAR SOLICITUD** El usuario interno o del operador solicita la restauración de: un servidor base de datos archivo	Usuarios Internos y/u operador de servicio	Permanente	Herramienta de Gestión CA Service Desk Manager.
11	**VALIDACION DE LA SOLICITUD** Se valida si la información será restaurada sobre el mismo sistema, de ser así se puede proceder de una vez con la ejecución de la tarea, de lo contrario se debe continuar con la actividad 14.	Gestor de Backup	0.0 hora 0.5 hora	Herramienta de Gestión CA

3. Descriptivo del Procedimiento				
RESTAURACIÓN DE UN BACKUP				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
				Service Desk Manager.
12	**INFORMAR AL USUARIO** Se informa al usuario indicando que la información ha sido restaurada para realizar las validaciones correspondientes	Gestor de Backup	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
13	**CIERRE DE CASO** Se documenta y cierra el caso en la Herramienta de Gestión CA Service Desk Finaliza procedimiento	Gestor de Backup	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
14	**ALISTAMIENTO** Se realiza la identificación de los componentes tecnológicos que conforman el servicio o aplicación, (servidores, bases de datos, otros). Una vez identificados los servidores que se necesitan para la restauración se debe verificar las cintas donde se almacenó el Backup con la fecha de tiempo requerida para el proceso de restauración y su ubicación, ya sea que se encuentren en la "Librería" (continuar con la actividad 16) o en custodia medios (sitio externo al Ministerio).	Gestor de Backup	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
15	**SOLICITAR CINTA** Con la identificación de la cinta se procede a solicitarla al proveedor de custodia.	Gestor de Backup	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.

3. Descriptivo del Procedimiento				
RESTAURACIÓN DE UN BACKUP				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
16	**APROVISIONAMIENTO** El aprovisionamiento o reserva de capacidad que se debe utilizar para el proceso de restauración, en esta etapa se define lo necesario para iniciar el proceso de restauración, servidores, direccionamiento, motor de base de datos, entre otros que permitirán tener el entorno asegurado donde se va a realizar la restauración. Si el caso corresponde a restaurar solo la aplicación se omite el paso 18.	Gestor de infraestructura	1 horas 2 horas	Herramienta de Gestión CA Service Desk Manager.
17	**RESTAURACIÓN SERVIDORES** Se crean los servidores de acuerdo con el sistema de información que se ha solicitado, se configura las tarjetas de red y se encienden estos.	Gestor de Backup	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
18	**RESTAURACIÓN DE BASES DE DATOS** Se configura la base de datos sobre los servidores restaurados, donde se instala el motor de base de datos y se restaura la data correspondiente.	Gestor de Base de datos	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
19	**CONFIGURACIÓN DE APLICACIÓN** Una vez la base de datos este con los servicios arriba se configura el servidor de aplicación y se suben servicios. Y se informa al usuario final para realizar pruebas funcionales.	Gestor de Base de aplicaciones	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
20	**PRUEBAS FUNCIONALES** El usuario final procede con las validaciones para corroborar el correcto funcionamiento.	Usuarios Internos y/u operador de servicio	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.

3. Descriptivo del Procedimiento				
RESTAURACIÓN DE UN BACKUP				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
21	**CIERRE DE CASO** Se documenta y cierra el caso en la Herramienta de Gestión CA Service Desk. Finaliza el procedimiento	Gestor de Backup	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.

4. Control de Cambios		
Versión	**Fecha de entrada en vigor**	**Naturaleza del cambio**
01	A partir de la publicación en el SIG	Creación del documento. Se crea debido a la inexistencia de documentación acerca del procedimiento de toma de backups y restauración de los mismos en caso de un incidente.

5. Ruta de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Edwar Aldemar Hidalgo	**Nombre**	Lina Vannesa Perdomo Castrillón	**Nombre**	Roger Quirama García
Cargo	Contratistas de la Oficina de Tecnología y Sistemas de Información	**Cargo**	Contratista de la Subdirección de Desarrollo Organizacional	**Cargo**	Jefe Oficina de Tecnología y Sistemas de Información