UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

POLÍTICA DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO

BOGOTÁ D.C. ABRIL 2024

VERSIÓN 05

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

TABLA DE CONTENIDO

1. PROCESO 3
2. OBJETIVO 3
3. ALCANCE 3
4. DEFINICIONES 3
5. DISPOSICIONES GENERALES 4
6. CONTENIDO 5
6.1 INFORMACIÓN QUE SE DEBE RESPALDAR 5
6.2 RESTAURACIÓN DE INFORMACIÓN 6
6.3 GESTIÓN DE LA INFORMACIÓN EN CASO DE TRASLADO DE DEPENDENCIA 7
6.4 ESTRATEGIAS DE BACKUP 7
6.5 PLAN DE PRUEBAS DE RESTAURACIÓN DE BACKUP 8
6.6 BACKUP DE CORREO INSTITUCIONAL 8

1. PROCESO

Gestión de Tecnologías de la Información.

2. OBJETIVO

Establecer los lineamientos que se requieren para gestionar las copias de respaldo realizadas mediante herramientas especializadas con el fin de asegurar la confidencialidad, disponibilidad e integridad de la información institucional de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC.

3. ALCANCE

Aplica para la información institucional, Bases de Datos y configuraciones, herramientas y sistemas de información en producción en la USPEC.

4. DEFINICIONES

- **AGENTES:** accesos determinados por las herramientas de backup que deben ser instalados en los equipos objeto de copias de seguridad.
- **COPIA DE RESPALDO (EN INGLÉS BACKUP):** una copia de respaldo, copia de seguridad o backup es un proceso a través del cual se resguarda en forma segura la información contenida en un medio de almacenamiento en un medio o ubicación distinta al origen, con el fin de poder recuperarla en caso de falla del primer alojamiento de datos.
- **COPIA INCREMENTAL:** es una tarea de backup donde se copian únicamente los archivos que han sido incorporados o modificados desde la copia de seguridad anterior.
- **COPIA TOTAL:** es un proceso donde se copian la totalidad de archivos y directorios seleccionados.
- **ESCRITORIO VIRTUAL**: estación de trabajo que existe virtualmente y al que se puede acceder desde cualquier lugar a través de internet.
- **GOOGLE DRIVE**: plataforma de colaboración y almacenamiento en la nube proporcionado por la compañía Google.
- **INCIDENTES:** se cataloga como incidente todo evento que represente un daño significativo sobre la información, o que atente contra los principios fundamentales, como disponibilidad, confidencialidad e integridad.
- **NAS:** servidor de almacenamiento en red.
- **RED:** enlace de comunicaciones que se puede establecer mediante canales o interfaces cableadas o inalámbricas.
- **RESTAURACIÓN:** recuperar la información (archivos) a partir de una copia de seguridad (medio externo).
- **SERVIDOR DE ARCHIVOS (FILE SERVER EN INGLÉS):** servidor que permite a los clientes de la Red acceder a sus recursos de almacenamiento.

- **SERVIDOR:** computadora de gran capacidad que realiza tareas en beneficio de otras computadoras llamadas clientes, también provee almacenamiento a los equipos cliente, todo esto mediante una conexión de red.

- **USUARIO**: puede ser un Servidor público, Funcionario o Contratista de la USPEC, que hace parte de la gestión de los diferentes procesos y procedimientos de la Entidad.

5. DISPOSICIONES GENERALES

La Oficina de Tecnología es la encargada de gestionar el respaldo de la información institucional, así como su custodia a través de las diferentes herramientas especializadas en la generación y gestión de backup.

Actualmente la Entidad cuenta con una infraestructura tecnológica, que son servidores que almacenan información institucional, perfiles de escritorios virtuales e imágenes de seguridad de los servidores virtuales, que deben contar con el agente de backup asignado para mantener las copias de seguridad sincronizadas con la herramienta de backup en nube dispuesta por la entidad.

Es importante indicar que cada usuario cuenta con diferentes niveles de acceso (lectura, escritura o lectura-escritura) a las carpetas de los servidores de archivos (file server) asociadas a su cargo o funciones asignadas. En el caso de las carpetas compartidas, es responsabilidad de cada líder de proceso o jefe de dependencia, la asignación de los niveles de acceso (permisos de lectura, escritura o total), así como las indicaciones respecto a su estructura y gestión.

Es responsabilidad de cada usuario almacenar la información institucional, en las ubicaciones lógicas establecidas por la Oficina de Tecnología – OTEC: “Escritorio” y “Mis Documentos” con la diferencia que en Escritorio se debe almacenar únicamente información de carácter público, según lo establecido en la política de escritorio y pantalla limpios, contenida en la Política de Seguridad, Privacidad de Información y Seguridad Digital de la USPEC. La Oficina de Tecnología no se hace responsable por la pérdida de información que no se guarde en estas ubicaciones. De igual manera, se indica que no está permitido almacenar información de carácter personal en los equipos de la Entidad.

Importante. Según las directrices definidas por la Dirección de Infraestructura, para el personal que se encuentra vinculado como **contratista**, solo se respalda la información almacenada en la carpeta compartida definida por la dependencia, la información alojada en ”Mis Documentos” y “Escritorio”, no cuenta con respaldo. En el caso de las aplicaciones o sistemas alojados externamente, el proveedor debe garantizar el servicio de backup de la información.

A través de la Ley 23 de 1982, sobre derechos de autor, capítulo VI “Disposiciones especiales a ciertas obras”, artículo 91, se cita:

“*Los derechos de autor sobre las obras creadas por empleados o funcionarios públicos, en cumplimiento de las obligaciones constitucionales y legales de su cargo, son propiedad de la entidad pública correspondiente”*

Los derechos patrimoniales que surjan de la producción intelectual que el servidor o contratista realice en cumplimiento de las actividades propias de su contrato o con ocasión de ellas, pertenecen a la Entidad, y por tanto por este mismo acto se entienden cedidos por parte del servidor a favor de la Entidad.

Teniendo en cuenta lo anterior, se indica que la información generada por los usuarios y almacenada en las carpetas Escritorio y Mis Documentos, así como en las carpetas compartidas, hace parte de los activos de la Entidad.

De tal manera que, cuando un usuario cesa sus funciones o culmina la ejecución de su contrato con la USPEC, no se entrega copia de los buzones de correo institucionales a su cargo, ni de la información alojada en los servidores de

archivos, excepto por orden judicial, por solicitud de la Oficina de Oficina Asesora Jurídica - Grupo de Instrucción de Control Interno Disciplinario como parte de un proceso de investigación o por algún otro tipo de solicitud realizada por Entes de control.

Ante este tipo de solicitudes la Oficina de Tecnología se compromete a permitir el acceso de consulta a la información requerida. Para lo antes citado, se debe remitir la solicitud a través del correo de Mesa de Servicio de la Entidad, mesadeservicios@uspec.gov.co y a través del mismo medio, se informa la disponibilidad para consultar la información requerida.

Condiciones:

1. Si se requiere el backup por parte de un usuario diferente al titular de la información, este solo se debe solicitar por parte del Director o Jefe actual de la dependencia a la cual pertenecía el usuario y sobre esta información se otorga únicamente permiso de consulta, por un periodo de 15 días hábiles.

2. Para la información de los usuarios que se retiran de la Entidad se les realiza un backup (Mis Documentos y Escritorio) y se almacena en el Servidor de Archivos (file server). La información relacionada a la gestión del cargo, actividades contractuales o con ocasión de ellas debe ser entregada y almacenada en los medios dispuestos por la Oficina de Tecnología.

3. El líder de área o jefe inmediato debe validar que toda la información relacionada a la gestión del cargo, actividades contractuales o con ocasión de ellas, se encuentre disponible y almacenada en los medios dispuestos por la Oficina de Tecnología.

4. Una vez finalizado el vínculo laboral o contractual se debe realizar el proceso formal de entrega de información y paz y salvo, según lo establecido en el procedimiento **TI-PR-008 Gestión de Acceso de Usuario**.

Si un exfuncionario público, requiere acceso a la información con el fin de elaborar su informe de gestión, debe solicitarlo a través del correo de la Mesa de Servicio mesadeservicios@uspec.gov.co, esta solicitud se debe elaborar en un periodo no mayor a 15 días hábiles luego de haber salido de su cargo. La Oficina de Tecnología informa el horario y lugar en el cual puede acceder a su información; se aclara que se otorga únicamente permiso de consulta.

6. CONTENIDO

6.1 INFORMACIÓN QUE SE DEBE RESPALDAR

- **Servidor de Archivos (File Server):** se debe respaldar las carpetas de los usuarios (“Escritorio” y "Mis documentos”). En estas carpetas se debe respaldar únicamente la información generada por cada usuario en sus labores diarias.

- **Aplicaciones Web y Bases de Datos:** cada dependencia responsable de un activo de tipo software que se encuentre alojado en los servidores de la Entidad, debe solicitar a través del administrador del sistema o aplicación, a la Oficina de Tecnología mediante la herramienta de Mesa de Servicio, la generación de la copia de respaldo de la aplicación que tiene a cargo.

  El administrador del backup de la OTEC informa a través de correo, la ruta en la cual se debe almacenar la información que requiere ser respalda; posteriormente se lleva a cabo el backup teniendo en cuenta las condiciones relacionadas en el presente documento.

- **Controladores de Dominio:** para el caso del Controlador de Dominio, se realiza un backup utilizando la herramienta de copias de seguridad de Windows de cada Servidor y esta se aloja en una ubicación determinada (File Server) para su respectivo respaldo la nube.

  De los servidores Windows, se respalda el System State, DHCP y DNS; se debe tener en cuenta que el System State varía dependiendo del rol de la máquina Windows Server que se esté utilizando y sobre él se encuentra la configuración de los servidores y estaciones.

  En las operaciones de Backup y restore del System State se incluyen todos los datos del sistema, no se puede seleccionar al backup o al restore componentes individuales debido a la dependencia entre cada uno de sus componentes, sin embargo, los datos del System State se pueden restaurar en una localización alterna en la cual solamente los archivos de registro, el directorio de archivos del sysvol, y el sistema de archivos de Boot sean restaurados. La base de datos del Directorio Activo, la base de datos del servicio de certificado (si lo hay), y la base de datos de los componentes de servicios de clases registradas no se pueden restaurar en localizaciones alternas.

  Se debe hacer la copia de seguridad del System State sobre un archivo en el disco duro, para que desde otro servidor a través de la red se realice el backup a esta copia.

  Nota: las Copias de respaldo de las aplicaciones externas como del Portal Web, Humano, INFODOC (Gestor Documental, PQRD, Central de Cuentas), Inventarios, buzones de correo institucionales se realizan por el tercero, responsable de la administración de la información de acuerdo con las Políticas de Seguridad de la Información.

6.2 RESTAURACIÓN DE INFORMACIÓN

En caso de que algún usuario que se encuentre vinculado con la Entidad requiera la restauración de archivos alojados en el servidor de archivos (File Server), se debe realizar la petición a través de la herramienta de gestión de casos dispuesta por Oficina de Tecnología y gestionada por el personal de Mesa de Servicio, indicando los siguientes datos:

- Nombre exacto del archivo o carpeta a restaurar.
- Ruta completa donde se encontraba el archivo o carpeta a restaurar.
- Fecha de su eliminación.

El administrador del backup procede a restaurar la información solicitada. En el caso que no se encuentre la misma, se procede a informar al usuario y a registrar el incidente a través de la Mesa de Servicio.

Para la restauración de información se debe tener en cuenta las siguientes directrices:

- Si se requiere restaurar un archivo o carpeta que fuera creado o modificado el mismo día de la solicitud, no es posible su recuperación, debido a que la copia de seguridad se realiza en horas de la noche (A las 22:00 horas), dando, así como tiempo máximo estipulado de pérdida de información catorce (14) horas.

- Para las restauraciones en general se crea una carpeta en un File Server donde se realiza la tarea de restauración de las carpetas y archivos requeridos y allí se conserva el log generado por la herramienta, correspondiente a la tarea realizada.

- Las tareas de restauración son ejecutadas desde la consola de administración de la herramienta que se encuentre contratada para tal fin, allí se selecciona el dispositivo (Server) y los archivos y carpetas a los cuales se les realiza la restauración, indicando la ruta donde son restaurados.

6.3 GESTIÓN DE LA INFORMACIÓN EN CASO DE TRASLADO DE DEPENDENCIA

Con el fin de asegurar la continuidad de las actividades a cargo de la dependencia a la que pertenece un usuario que se traslada de área, se debe tener en cuenta las siguientes consideraciones:

- El traslado debe ser notificado a la Oficina de Tecnología, a través de correo electrónico dirigido al Coordinador de Telecomunicaciones y al administrador del backup, con el fin de generar la copia respectiva en la carpeta usuarios inactivos. A esta información se brinda acceso solo de lectura al usuario que quede a cargo, este remplazo debe ser definido por el jefe del área respectiva.

- En caso de que la persona que fungía como funcionario y cambie su vínculo a contratista en otra dependencia, se otorga permiso solo de lectura por un periodo de 15 días hábiles. En el caso que la persona quede asignado a la misma dependencia, continúa con el mismo acceso a la información.

- Si la persona que se traslada requiere para ejercer sus funciones o desarrollar sus actividades en el nuevo cargo o contrato, información que gestionaba a través de la dependencia anterior, debe realizar la solicitud al jefe de la anterior dependencia con la debida justificación y solo este último puede autorizar el acceso a la misma a través de correo enviado al buzón mesadeservicios@uspec.gov.co en este caso, se otorga un permiso solo de lectura por un periodo de 15 días hábiles. Si la información a la cual se requiere acceder se encuentra catalogada como reservada o clasificada, se deber tener en cuenta los lineamientos establecidos a través del instructivo **TI-IN-006 Transferencia de información Institucional**.

6.4 ESTRATEGIAS DE BACKUP

La programación y configuración de las copias de seguridad se genera por medio de la consola de administración de la herramienta, donde se selecciona el dispositivo al cual se realiza la copia y de igual forma los archivos y carpetas que son objeto de respaldo; allí se configuran las opciones de la copia de seguridad tales como horas y días para la realización de esta, ruta en la cual se almacenan los datos, exclusión de tipos de archivos (si las hay), tiempo de retención, entre otros.

Es de anotar, que el dispositivo objeto de la copia debe tener previamente instalado el software de backup (agente) si se requiere y no presentar ningún tipo de restricción para navegación de internet o cargue de archivos.

Frecuencia: el período establecido para la ejecución de la copia de seguridad es diario, es decir cada 24 horas, iniciando a las 20:00 horas cada día.

Tipo de Backup: la primera copia de respaldo generada es total, de ahí en adelante las copias de respaldo generadas son de tipo incremental, esto significa que se resguarda la información que se haya incorporado o modificado desde la última copia de respaldo realizada. La retención de estas copias de seguridad se establece en 60 días calendario, lo que implica que el día 61 se sobrescribe la copia total correspondiente al día uno (1) y se genera una nueva copia total de la información y así sucesivamente.

6.5 PLAN DE PRUEBAS DE RESTAURACIÓN DE BACKUP

Para llevar a cabo las pruebas de restauración de información se debe tener en cuenta los siguientes aspectos:

- La Oficina de Tecnología realiza anualmente el plan de pruebas de restauración de información, incluyendo actividades, estimación de fechas, responsables, relevancia de la información (dependencias, aplicaciones) entre otros.

- Se debe conservar el log del registro de la tarea de restauración, con el fin de validar que se ejecutó la tarea satisfactoriamente. En caso de que no se realice la restauración correctamente, se debe analizar las causas y ejecutar la actividad nuevamente.

- Las copias de seguridad se realizan en una nube privada, por lo tanto, no requieren de ubicación de almacenamiento físico especial dentro de la Entidad.

- El tiempo de duración de la restauración depende del tipo de conexión y tamaño de la data a restaurar.

- La información respaldada debe quedar encriptada en el momento de la generación del backup.

- Las pruebas de restauraciones deben ser periódicas, por lo menos una cada 30 días, las carpetas y archivos a restaurar se seleccionan aleatoriamente, se selecciona la ubicación donde se realiza la restauración, esta puede ser en su ubicación original para el caso de información eliminada por un usuario o en una carpeta creada para tal fin (por seguridad se recomienda esta última opción, para evitar que se sobrescriban archivos existentes ya modificados por un usuario).

6.6 BACKUP DE CORREO INSTITUCIONAL

Una vez haya transcurrido un mes de notificado el retiro del usuario, se da inicio a la gestión del Backup de correo, de la siguiente manera:

- A través de la herramienta de retención de correos del servicio de correo electrónico, se realiza el respaldo y copias de seguridad del buzón y almacenamiento en nube, es directamente proporcional el tiempo de ejecución de la labor con el peso del buzón.

- Se exporta un archivo comprimido con el contenido del correo (. PST'S) y una carpeta adicional con los archivos contenidos dentro del drive. Esta información se almacena en volúmenes disponibles en la infraestructura “NAS”.

- Para verificar el correcto funcionamiento del Backup, se exporta un PST a la herramienta de Microsoft Office Outlook, esta gestión se realiza en un almacenamiento físico de la infraestructura.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	30/08/2016	Todos	Se crea el documento.
02	24/06/2020	Todos	Se actualizan todos los numerales del documento.
03	14/08/2020	5	Se actualiza el numeral 5 "Lineamientos generales" modificando los criterios para la entrega de backups.
	04/10/2021	N/A	Se ajustan los códigos de los documentos de acuerdo con la actualización del Mapa de Procesos Institucional. La versión del documento se mantiene debido a que su contenido no se modificó.
04	30/06/2023	5	Se actualiza el numeral 5 modificando los lineamientos generales, la restauración de la información y backup de correo institucional. Se adicionaron lineamientos para la gestión de la información en caso de traslado de dependencia.
05	15/04/2024	2, 4, 5, 6	Se ajusta el objetivo, definiciones, disposiciones generales y el contenido, de acuerdo a lo establecido en la Ley 23 de 1982, sobre Derechos de Autor. La presente versión de la política se aprobó por el Comité Institucional de Gestión y Desempeño, a través del acta No. 150424 del 15/04/2024.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Imelda Muñoz Mancipe	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Jefe Oficina de Tecnología	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
Nombre: Daniel Ricardo Muñoz Alvarado		
Cargo: Oficial de Seguridad de Información		
Dependencia: Dirección General		