1. **NOMBRE DE LA POLÍTICA:** Política de Generación y Restauración de Copias de Respaldo.

2. OBJETIVO

Establecer los lineamientos que se requieren para gestionar las copias de respaldo realizadas mediante herramientas especializadas con el fin de asegurar la disponibilidad de la información institucional del Instituto de Cultura y Turismo de Bolívar – ICULTUR.

3. ALCANCE

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

4. GLOSARIO

- **Copia de respaldo (backup):** Es la actividad de resguardar en forma segura la información contenida en un medio de almacenamiento en un medio o ubicación distinta al origen.
- **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.
- **File Server:** Servidor que permite a los clientes de la Red acceder a sus recursos de almacenamiento.
- **Google Drive o Drive:** Almacenamiento en la nube proporcionado por la compañía Google.
- **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.
- **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.
- **Red:** Enlace de comunicaciones que se puede establecer mediante canales o interfaces cableadas o inalámbricas.
- **Ticket:** Número de caso generado con la herramienta de mesa de ayuda de la entidad, para atención de incidentes y/o solicitudes.
- **Restauración:** Recuperar la información (archivos) a partir de una copia de seguridad (medio externo)

- **Usuario**: Puede ser un Servidor público y/o Contratista del Instituto de Cultura y Turismo - ICULTUR.
- **Eliminar de forma segura:** Se refiere a borrado seguro de información de un dispositivo, con el fin que no se pueda recuperar ni acceder a ella bajo ningún escenario.
- **Agentes:** Accesos determinados por las herramientas de backup que deben ser instalados en los equipos objeto de copias de seguridad.
- **Restore:** Tarea relacionada con el backup que consiste en la recuperación de archivos o carpetas eliminadas.

5. LINEAMIENTOS GENERALES

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

Los agentes especializados (si aplican) deben ser instalados y configurados en cada uno de los servidores con información institucional a ser respaldada, cada copia debe ser almacenada en Nube Privada, o en un medio de almacenamiento local según sea la necesidad. La información a ser respaldada se encuentra detallada en el numeral 5.1.

Es importante indicar que cada servidor público y/o contratista cuenta con diferentes niveles de acceso (lectura, escritura o lectura-escritura) a las carpetas asociadas a su labor en los servidores de archivos (files server). En el caso de las carpetas compartidas, es responsabilidad de cada líder de proceso o jefe de dependencias la asignación de los niveles de acceso (permisos de lectura, escritura o total).

Es responsabilidad de cada usuario almacenar la información institucional en las rutas establecidas por la OTEC (Escritorio, Mis Documentos). La Oficina de Tecnología no se hace responsable por la pérdida de información que no sea guardada en estas ubicaciones. De igual manera no está permitido almacenar información personal en los equipos de la Entidad.

Los lineamientos contenidos en este documento se le darán a conocer al usuario al momento de la entrega de un cliente liviano, PC o computador portátil, por parte del personal de la mesa de ayuda.

En el caso de las aplicaciones o sistemas alojados externamente, el proveedor deberá garantizar el servicio de backup de la información.

La información generada por los usuarios y almacenada en las carpetas Escritorio y Mis Documentos, hace parte de los activos de la Entidad. Para obtener copias de la información, se deben tener en cuenta los siguientes criterios:

- **Entrega de backup al personal vinculado con la Entidad:** la entrega se debe gestionar a través del formato "TI-FO-050 Solicitud de Backup Institucional", el cual debe contar con la aprobación del jefe inmediato o supervisor de contrato para la entrega de la información requerida y debe constar que dentro de los datos a respaldar no se disponga información de carácter confidencial o reservado de la Entidad. Este formato se debe remitir a la mesa de ayuda - HELPTIC con el fin de darle la debida gestión por parte de la OTEC.

- **Entrega de backup al personal desvinculado de la Entidad:** la persona que requiere acceso a la cuenta de correo deberá remitir la solicitud a través de los canales dispuestos por la Entidad para atención a la ciudadanía (ver canales de atención y comunicación), informando en el contenido de la solicitud la dependencia a la cual se encontraba vinculado. El jefe de dicha dependencia debe evaluar la solicitud y de considerarlo pertinente debe remitir el formato "TI-FO-050 Solicitud de backup" a la Oficina de Tecnología a través de la mesa de ayuda - HELPTIC, aprobando la entrega del backup y debe constar que dentro de la información a entregar no se disponga de información de carácter confidencial o reservado de la Entidad.

Nota: Si se requiere el backup de un usuario diferente al titular de la información, este solo se podrá solicitar por parte de quien fuese su jefe inmediato o supervisor de contrato, o en caso de los directivos o jefes podrán solicitar el backup del personal a quien reemplacen.

A la información de los usuarios que se retiran de la Entidad se les realiza un backup (Mis Documentos y Escritorio) y se almacenará en el File Server (Unidad usuarios inactivos).

5.1 INFORMACIÓN QUE SE DEBE RESPALDAR

- **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, deberá solicitar a través del administrador del sistema o aplicación a la Oficina de Tecnología mediante la herramienta de mesa de ayuda, la generación de la copia de respaldo de la aplicación que tiene a cargo. El administrador del backup de ICULTUR informará a través de correo, la ruta en la cual se deberá almacenar la información que requiere ser respalda; posteriormente se llevará 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 realizará un backup utilizando la herramienta de copias de seguridad de Windows de cada Servidor y esta se alojará en una ubicación determinada (File Server) para su respectivo respaldo la nube.

  De los servidores Windows, se respaldará 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/o 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, aplicativos PQRD, Humano, buzones de correo institucionales serán realizadas por el tercero, responsable de la administración de la información de acuerdo con las Políticas de Seguridad de la Información.

5.2 RESTAURACIÓN DE INFORMACIÓN

En caso que algún Servidor público y/o Contratista requiera la restauración de archivos alojados en el File Server, se debe realizar la petición a través de la herramienta HELPDESK Icultur HELPDESK Mesa de Ayuda ICULTUR (google.com)
administrada por el personal de Mesa de Ayuda, 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 procederá a restaurar la información solicitada. En el caso que no se encuentre la misma, se procederá a informar al usuario y a registrar el incidente a través de la mesa de ayuda.

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

- Si se requiere restaurar un archivo o carpeta que fuera creado el mismo día de la solicitud, no será posible su recuperación, al igual que los archivos modificados y eliminados el mismo día, debido a que el backup se realiza en horas de la noche (22 horas), dando, así como tiempo máximo estipulado de pérdida de información catorce (14) horas.

- Para las restauraciones en general se creará una carpeta en un File Server donde se realizará la tarea de restauración de las carpetas y/o archivos requeridos y allí se conservará 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 seleccionará el dispositivo (Server) y los archivos y/o carpetas a los cuales se les realizará la restauración, indicando la ruta donde serán restaurados.

5.3 ESTRATEGIAS DE BACKUP

La programación y configuración de las copias de seguridad se generarán por medio de la consola de administración de la herramienta, donde se seleccionará el dispositivo al cual se realizará la copia y de igual forma los archivos y/o carpetas que serán objeto de respaldo; allí se configurarán las opciones de la copia de seguridad tales como horas y días para la realización de la misma, ruta en la cual se almacenarán los datos, exclusión de tipos de archivos (si las hay), tiempo de retención, etc. Es de anotar que el dispositivo objeto de la copia deberá 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 copa de respaldo generada será total, de ahí en adelante las copias de respaldo generadas serán 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 generará una nueva copia total de la información y así sucesivamente.

5.4 PLAN DE PRUEBAS DE RESTAURACIÓN DE BACKUP

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

- La Oficina de Tecnología elaborará 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 que no se realice la restauración correctamente, se deberán analizar las causas y ejecutar la tarea 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 dependerá 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/o archivos a restaurar se seleccionarán aleatoriamente, se seleccionará la ubicación donde se realizará 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).

5.5 BACKUP DE CORREO INSTITUCIONAL

El Backup de correo se gestiona de la siguiente manera:

- Solicitud masiva de generar Backup, es requerido al proveedor, para que con su gestión se realice el respaldo de una gran cantidad de cuentas. Estas son entregadas en formato pst (correo).

- El proveedor Icloud City, realiza respaldo y copias de seguridad del correo mediante un script personalizado que ejecuta el comando rsync que se comunica únicamente con un servidor exclusivo de backups ese trabajo es desde el backend del datacenter.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	30/01/2023	Todos	Se crea el documento.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Yolanda Barrios Arteaga	Nombre: Natacha González	Nombre: Mario Imbett
Cargo: Ingeniero de Sistemas	Cargo: Directora Administrativa y Financiera	Cargo: Jefe Oficina de Tics
Dependencia: Oficina de Tics	Dependencia: Oficina de Financiera	Dependencia: Oficina de Tics
	Nombre: Mario Imbett	
	Cargo: Ingeniero de Sistemas	
	Dependencia: Oficina de Tics	