1. OBJETO:

Establecer las actividades pertinentes para el resguardo en forma segura de la información definida por los usuarios como importante o critica para el desarrollo de sus funciones u obligaciones contractuales, la información que se encuentra en los servidores, así como la configuración de equipos de networking y la recuperación cuando sea requerido.

2. ALCANCE:

Este procedimiento aplica para salvaguardar la información contenida o almacenada en equipos de cómputo de la Entidad asignados a funcionarios o contratistas y la almacenada en los servidores de la entidad.

Inicia con la identificación de la información que se requiere respaldar, continua la ejecución y verificación, las actividades para la restauración de los respaldos y sus pruebas respectivas y finaliza con la elaboración del informe de gestión.

3. DEFINICIONES:

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización y por lo tanto se debe proteger.

Backup o Respaldo: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un dispositivo electrónico de almacenamiento o en la nube, con el fin de poder recuperar la información en caso de un incidente de seguridad de la información.

Tipo Incremental: Copia de seguridad de los datos modificados desde la última copia realizada.

Tipo Full o Completo: Copia de seguridad de todos los datos en un solo respaldo. Para optimizar tiempos de operación, suelen combinarse con los respaldos de tipo incremental.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Evento: Cualquier cambio de estado que tenga importancia para la gestión de un servicio o elemento de configuración. Los eventos generalmente se reconocen a través de notificaciones creadas por un servicio TI, elemento de configuración o herramienta de monitoreo.

GPO: Termino en ingles que significa “Objetos de directiva de grupo” y son un conjunto de ajustes para la configuración del sistema y cómo los usuarios interactuarán en una infraestructura de Directorio Activo (Active Directory).

Hash: Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los hashes son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones

Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Log o Logs: Registro o Registros. Termino técnico usado para los datos que se genera en los sistemas (Servidores, Aplicaciones, Programas, etc) en forma de trazas textuales en el que constan cronológicamente los acontecimientos que afectan a un sistema o el conjunto de cambios que generan.

NAS: Dispositivos de almacenamiento conectado a la red.

OneDrive: Servicio de alojamiento de archivos en la nube de Microsoft.

Retención: Hace referencia al periodo de tiempo en que se reescribe o se guarda un Backup o Respaldo.

SandBox: Termino en ingles que significa “Caja de Arena” y denota un entorno controlado. Se usa como mecanismo de seguridad para disponer de un entorno aislado del resto del sistema operativo.

Servidor: Computador especializado conectado a una red, generalmente local, que comparte sus servicios y recursos con otros puestos de trabajo en la red.

SnapShot: Copia instantánea de la imagen de un servidor.

Usuario final: Persona o personas que manipulan directamente los recursos tecnológicos de la Entidad.

Wipe: Algoritmo usado para la eliminación de forma segura de una información o dispositivo.

4. NORMATIVA:

NUMERO	DESCRIPCIÓN
Decreto 235 del 28 de enero de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 415 del 7 de marzo de 2016	Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

5. LINEAMIENTOS DE OPERACIÓN:

5.1. RESPALDOS

No se debe almacenar en servidores, equipos de cómputo o en cualquier medio de almacenamiento de la Entidad, información personal, música, vídeos, documentos transitorios y otros que no sean relevantes para el cumplimiento de las funciones y obligaciones contractuales.

La información de los usuarios finales debe estar almacenada en OneDrive o en el servicio de almacenamiento de archivos en la nube que disponga la Entidad. En caso de no tener cuenta en el sistema de almacenamiento en la nube dado por la OTIC, almacenar la información en el directorio “\Mis Documentos”.

Es responsabilidad de los Líderes de Proceso, Subdirectores, Director (a) o Jefes de Oficina, identificar y solicitar a la Oficina TIC el respaldo de la información crítica que se encuentre en directorios o medios de almacenamiento diferentes a los establecidos en el lineamiento anterior o en bases de datos y servidores que no se encuentren bajo la custodia de la Oficina TIC, por medio de la mesa de ayuda soporte.tecnico@uaesp.gov.co.

Ningún usuario final debe realizar copias de la información contenida en los equipos asignados en medios de almacenamiento extraíbles o sistemas de almacenamiento en la nube no autorizadas por la Entidad para evitar riesgos de fuga de información, excepto, aquellos autorizados por sus líderes de proceso, Jefes de Oficina, Subdirectores o Dirección, para el estricto cumplimiento de sus funciones u obligaciones contractuales, en cuyo caso, estos dispositivos deben estar listados en el inventario de activos información del proceso correspondiente e implementar controles de seguridad adecuados, como el cifrado de información o del dispositivo en caso de contener Información Pública Clasificada o Reservada (Artículos 18, 19 y 21 de la ley 1712 de 2014).

Los responsables de la gestión de respaldos de la Oficina TIC, deben aplicar los siguientes criterios para el respaldo de la información de la Entidad.

ELEMENTOS	TIPO	FRECUENCIA	RETENCIÓN
Servidores Críticos (Sistema, Datos y Servicios)	Incremental	Diario	8 puntos de recuperación diaria.
	Full	Inicial	
Servidores No Críticos (Sistema, Datos y Servicios)	Incremental	Semanal	1 mes
	Full	Inicial	
Bodega ORFEO – Vigencia actual (último año)	Incrementales	4 horas	Semanal
	Full	Semanal	
Bodega ORFEO – Almacenamiento Histórico 2011-Inicio Vigencia Actual	Full	Anual (Mensual de marzo a junio)	Anual
Dispositivos de networking (Dispositivos de seguridad perimetral, Configuraciones, Firmware)	Full	Semanal	1 mes
Usuario Final (File Server)	Incremental	Diario	10 años (Directivos) 5 años (Usuarios finales)
	Full	Inicial	
Usuario Final (OneDrive)	Incremental	Diario	
	Full	Merge - incremental	
Correo electrónico / Teams / Sharepoint (Herramientas colaborativas)	Incremental – Diferencial.	Diario	10 años (Directivos) 5 años (Usuarios finales)
	Full	Merge - incremental	

Los responsables de la gestión de respaldos de la Oficina TIC, deben cifrar los respaldos para garantizar la confidencialidad e Integridad de la información, usando algoritmos de cifrados recomendados por fabricantes o robustos.

Los responsables de la gestión de respaldos de la Oficina TIC, deben configurar los respaldos en los siguientes medios.

Servidores de misionalidad critica = Local y Replica en la Nube.

Servidores de Apoyo = Respaldo Local.

Correo electrónico = Nube

Usuarios directivos (Jefes de Oficina, Subdirectores y Dirección General) = Local y Replica en la Nube.

Usuarios finales, no directivos = Nube.

5.2. RESTAURACIÓN

Para solicitar la restauración de información o para la realización de pruebas de restauración y respaldos, se debe realizar a través de la mesa de ayuda soporte.tecnico@uaesp.gov.co.

No debe realizarse la restauración de la información en equipos personales o que no se encuentren bajo la custodia de la Entidad.

Para la recuperación de información, en caso de pérdida total, deberá realizarse con el respaldo más reciente.

La Oficina TIC deberá realizar pruebas de restauración de respaldos con el fin de asegurar la integridad de estos y el estado de los medios de almacenamiento, de acuerdo con el siguiente cronograma:

Tabla 1 Cronograma de pruebas de restauración de respaldos.

ELEMENTOS	MES											
	01	02	03	04	05	06	07	08	09	10	11	12
SERVIDORES / BASES DE DATOS / NETWORKING												
INFORMACIÓN DE USUARIOS FINALES (FileServer)												
CORREO ELECTRÓNICO / MICROSOFT TEAMS / SHAREPOINT												

Al finalizar las pruebas de restauración se deberá elaborar un informe que contenga, mínimo, la siguiente información:

- Fecha de la prueba
- Equipos (Usuarios)
- Checksum del backup u otros criterios de aceptación.
- ¿Se recuperó correctamente? (Si/No)
- Inconvenientes encontrados / recomendaciones de seguridad.

Las pruebas deberán hacerse atendiendo la política de protección y privacidad de datos personales.

6. DESCRIPCIÓN DE ACTIVIDADES:

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	RESPALDOS			
1	**Identificar los elementos** Identifica los elementos e información crítica que ha de ser respaldada en los directorios establecidos en los lineamientos de operación. Nota: Para la información contenida en los equipos de cómputo de usuario final, deberá estar organizada de acuerdo con los lineamientos de operación.	GTI-FM-08 Registro de activos de información e índice de información clasificada y reservada UAESP	Usuario final	
2	**Configurar GPO** Configura y valida aplicación de GPO y redireccionamiento hacia el File Server. Verifica que la GPO esté correcta y verifica la inclusión del equipo en el Directorio Activo antes de continuar.	Instrucción = GP update/status	Soporte de primer nivel.	Estado GPO
3	**Configurar herramientas de respaldo** Configura la o las herramientas de respaldo de acuerdo con los criterios para la gestión de respaldo establecidos en los lineamientos de operación. Nota: Se deben cifrar los respaldos para garantizar la confidencialidad e Integridad de la información.	Herramienta de respaldo	Técnico / Contratista / Profesional Universitario Oficina TIC	Logs en la herramienta
4	**Ejecutar tarea de respaldo** Realiza el respaldo de forma automática cifrando la información y las llaves son almacenadas en el repositorio interno propio de la herramienta.	Herramienta de respaldo	Herramienta de respaldo	Logs en la herramienta
5	**Replicar el respaldo** Replica los respaldos de elementos críticos, que se encuentra en la NAS, al almacenamiento en nube.	Herramienta de respaldo	Herramienta de respaldo	Logs en la herramienta de respaldo
6	**Revisar ejecución** Revisa diariamente los registros de las herramientas en busca de fallos o errores.	Alertas y Registros de la Herramienta	Técnico / Contratista / Profesional Universitario Oficina TIC	Logs en la herramienta de respaldo

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	¿La ejecución es correcta? Si: Continúa con la actividad No 9. No: Continúa con la actividad No 7.			
7	**Revisar y corregir** Revisa y realiza las acciones necesarias para corregir la falla o error en el respaldo.	Herramienta de respaldo	Técnico / Contratista / Profesional Universitario Oficina TIC	Logs en la herramienta de respaldo
	¿El respaldo es crítico? Si: Continúa con la actividad No 8. No: se esperará a la siguiente ejecución automática, Continúa con la actividad No 6.			
8	**Ejecutar respaldo de forma Manual** Ejecuta la tarea de respaldo de forma manual. Continúa con la actividad No 6.	Herramienta de respaldo	Técnico / Contratista / Profesional Universitario Oficina TIC	Logs en la herramienta de respaldo
9	**Realizar el informe mensual** Realiza el informe mensual de la gestión de respaldo. Este informe deberá contener el grado de cumplimiento, las fallas más relevantes si las hubo y lecciones aprendidas cuando aplique. <u>Nota</u>: Cada 6 meses incluir el capacity planning		Técnico / Contratista / Profesional Universitario Oficina TIC	Informe mensual / o Capacity Planning
RESTAURACIÓN Y PRUEBAS				
1	**Realizar la selección** <u>Para restauración</u>: Selecciona del listado de la herramienta de respaldo el usuario requerido o elemento a restaurar. <u>Para pruebas:</u> • Servidores / Bases de datos: Se selecciona los servidores requeridos por aplicación. • Usuario final / Herramientas colaborativas: Selecciona 3 usuarios al azar del		Administrador de infraestructura o encargado OTIC	

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	listado de la herramienta de respaldo. Nota: En caso de que un usuario no contenga información, selecciona otro al azar. • Networking: Selecciona el servidor donde se centralizan los respaldos de las configuraciones de dispositivos de networking.			
2	**Realizar la restauración** <u>Para restauración</u>: Ejecuta la restauración desde la herramienta de respaldo, de acuerdo con los lineamientos de operación. <u>Para pruebas:</u> • Servidores/Bases de Datos/ Networking: Realiza o saca el checksum para validar integridad, con la herramienta de validación. • Usuario Final / Herramientas colaborativas: Realiza la restauración en un espacio reservado en la NAS.	Herramienta de respaldo	Administrador de infraestructura o encargado OTIC	Informe de pruebas de respaldo Logs en la herramienta de respaldo
3	**Realizar la comprobación** <u>Para servidores/Bases de Datos/ Networking</u>: • Verifica la integridad con la herramienta de validación disponible. <u>Para usuario final / Usuario Final</u>: • Verifica que el tamaño de la restauración con el de la nube. • Errores en el registro de eventos al hacer la restauración.	Herramienta de respaldo	Administrador de infraestructura o encargado OTIC / Técnico OTIC	Actualizar informe de pruebas de restauración Logs en la herramienta de respaldo
	¿Se detectó algún fallo o inconsistencia en la comprobación? Si: Continúa con la actividad No 4. No: Continúa con la actividad No 5. Nota: Si es una restauración, continúa con la actividad No 09 de la sección “RESPALDOS”.			

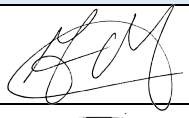
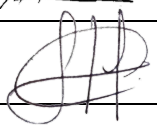
No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
4	**Revisar y corregir** Revisa las causas y realiza las acciones necesarias para corregir la falla o error de la restauración. Continúa con la actividad No 2.		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	
5	**Realizar Disposición Segura** <u>Para servidores/Bases de Datos/Networking</u>: • Nota: No aplica para elementos al contar con herramienta de validación. <u>Para usuario final / Herramientas colaborativas:</u> • Elimina el bloque de información de forma manual y segura usando un wipe, garantizando que no se recupere con alguna otra herramienta.		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Actualizar el informe de pruebas de respaldo
6	**Finalizar el Informe** Actualiza el informe con los resultados y los requerimientos establecidos en los lineamientos de operación para las pruebas de restauración.		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Informe final de pruebas de restauración
SOLICITUD DE RESPALDO DE CORREOS POR LÍDER DE PROCESO O TERCEROS AUTORIZADOS				
1	**Realizar la solicitud** Envía solicitud al jefe de la Oficina TIC.	Sistema de Gestión Documental	Líder de proceso Terceros autorizados	Memorando o Solicitud externa
2	**Realizar la aprobación** Aprueba la solicitud de copia del respaldo e informa al encargado de realizar las copias de seguridad.	Correo Electrónico	Jefe de la Oficina TIC	Aprobación por correo electrónico
3	**Realizar Copia** Realiza la copia del correo electrónico solicitado, en el medio de almacenamiento dispuesto por el solicitante y realizar un *Hash* para garantizar la integridad de la información.	Fase de Restauración y Pruebas Herramienta de respaldo	Técnico / Contratista / Profesional Universitario.	Logs en la herramienta de respaldo.
4	**Entregar copia de respaldo** Realiza la entrega al solicitante de la copia del correo electrónico.	Sistema de Gestión Documental	Jefe de la Oficina TIC	Memorando o Acta de entrega.

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	***Nota**: En el memorando o acta deberá constar el Hash generado*.			

7. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
01	30/11/2015	Se dividió el procedimiento SO-GTI-PCGB-04 Generación de Backups versión 04 del 30 de noviembre de 2012 en dos procedimientos, dando origen al presente documento.
02	06/08/2021	Se une con el procedimiento Generación de Backups de Equipos de cómputo y se ajusta el nombre de Generación de backups en servidores a Gestión de respaldos. Se define la etapa de Restauración y Pruebas y la etapa de solicitud de copias de correo electrónico para entes de control o externos.
03		Se incorporan lineamientos de operación para respaldos, pruebas de restauración y se amplía el procedimiento para estas pruebas.

8. AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Mauricio Suarez Mayorga	Profesional Universitario Oficina TIC	
	Oscar Ricardo Rodríguez Martínez	Contratista Oficina TIC	
	Juan Sebastián Perdomo Méndez	Profesional Universitario Oficina TIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina de Tecnologías de Información y las Comunicaciones	
	Luz Mary Palacios Castillo	Profesional Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa	Jefe Oficina Asesora de Planeación