

1. OBJETO:

Asegurar la integridad y disponibilidad de los datos críticos que se encuentran en los servidores y repositorios de información de la Entidad.

2. ALCANCE:

Inicia con la identificación de la información que se requiere respaldar, la ejecución, verificación y las actividades para el respaldo, restauración y sus pruebas respectivas. Este procedimiento aplica para todos los procesos de la UAESP.

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 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.

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.

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

Incidencia Operativa: Evento no planificado que interrumpe o degrada un servicio o proceso de TI.

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. Término 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.

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.

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

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:

TABLA 1 NORMATIVA APLICABLE AL PROCEDIMIENTO

NUMERO	DESCRIPCIÓN
Resolución 02277 del 03 de junio del 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

Fuente: Normograma UAESP

5. LINEAMIENTOS DE OPERACIÓN

- 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 su momento.
- No se debe almacenar en servidores, equipos de cómputo o en cualquier medio de almacenamiento de la Entidad, información personal como música, vídeos, documentos, entre otros, y otra información que no sean relevantes para el cumplimiento de las funciones y obligaciones contractuales.
- 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 los lineamientos de operación o en bases de datos y servidores que no se encuentren bajo la custodia de la Oficina TIC.
- Para definir la criticidad, frecuencia y tiempos de retención se deberá evaluar requisitos legales, contractuales, disponibilidad y uso de los activos, entre otros.
- 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).

- Para la elaboración del plan de restauración de respaldos, de la actividad No 1 de este procedimiento, la Oficina TIC definirá, mínimo, las siguientes características: Tipo o método, frecuencia de los respaldos y retención.
- Los responsables de la gestión de respaldos de la Oficina TIC, deben activar o configurar las opciones de cifrado en los respaldos para asegurar la confidencialidad de la información, usando algoritmos de cifrados robustos o recomendados por los fabricantes y proveedores de las soluciones de respaldo.
- Antes de un cambio significativo en un servidor, se debe tomar un snapshot que permita revertir a un estado anterior funcional como estrategia de rollback o usarlo como modelo en pruebas u otra situación.
- En caso de tener un servidor, servicio, aplicativo, base de datos u otro elemento comprometido por un evento de seguridad, se deberá tomar un snapshot y antes de cualquier otra acción, notificar al oficial de seguridad para realizar los procedimientos de adquisición para análisis forense y activar los procedimientos de gestión de incidentes.
- Solo se atenderá la solicitud de restauración del responsable o custodio del activo, o previa autorización de la Dirección, Subdirección o Jefes de Oficina.
- No debe realizarse la restauración de la información en equipos personales o dispositivos que no se encuentren bajo la custodia de la Entidad, salvo requerimientos legales, contractuales o bajo autorización de un líder de proceso.
- Para la recuperación de información en caso de pérdida total, se deberá utilizar el respaldo más reciente que haya sido validado como íntegro y seguro, garantizando que su uso no comprometa la disponibilidad ni la seguridad de la información.

- La Oficina TIC deberá realizar pruebas de restauración de respaldos con el fin de asegurar la integridad y disponibilidad de la información, así como verificar el estado de los medios de almacenamiento, conforme al plan de respaldos que elabore internamente y en cumplimiento de la actividad No 1 de este procedimiento.
- La oficina TIC, una vez finalizada las pruebas de restauración, deberá elaborar un informe que contenga, mínimo, la siguiente información:
 - Fecha de la prueba
 - Equipos, Sistema, Servidor, Aplicación, Base de Datos o elemento probado.
 - Checksum del backup u otros criterios de aceptación de Integridad que se consideren necesarios o apliquen.
 - ¿Se recuperó correctamente? (Si/No).
 - Inconvenientes encontrados / recomendaciones de seguridad y de gestión.
 - Tiempos de restauración. Esto permitirá conocer los tiempos medios de restauración en caso de un incidente.
- Las pruebas deberán hacerse atendiendo la política de protección y privacidad de datos personales.

6. DESCRIPCIÓN DE ACTIVIDADES:

TABLA 2 DESCRIPCIÓN DE ACTIVIDADES

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
RESPALDOS				
1	Elaborar plan de trabajo Elabora o actualiza el plan de respaldos y recuperación de la información, identificando los elementos	Lineamientos de operación	Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Plan de pruebas aceptado por el Jefe de la OTIC

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	y la información crítica que debe ser respaldada, de acuerdo con los lineamientos de operación. El documento tendrá carácter interno y será considerado como información sensible, por el contenido que resguarda.			
2	Automatizar tareas Define y configura las tareas o “Jobs” en la herramienta de respaldos de acuerdo con el plan de trabajo definido en la actividad No 1. Nota: Se deben cifrar los respaldos para asegurar la confidencialidad e Integridad de la información.	Lineamientos de Operación y Plan de trabajo	Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Herramienta de respaldos
3	Verificar medios de almacenamiento para las copias de seguridad Verifica el estado o alertas de los medios de almacenamiento activos para respaldos con el fin de garantizar la ejecución y almacenamiento de los		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Informe mensual de gestión de riesgos

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	respaldos. Nota: Cuando las alertas sean críticas o que pongan en riesgo la ejecución de los respaldos, se debe solucionar o gestionar su solución.			
4	Replicar el respaldo Configura la réplica de los respaldos de elementos críticos, si el respaldo principal está en almacenamiento local, lo replica a la nube; si está en la nube, lo replica a otra región o zona de disponibilidad de la misma nube o a un medio alternativo, siempre que los recursos lo permitan.	Lineamiento de operación	Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Logs en la herramienta de respaldo
5	Verificar tareas de respaldo Verifica diariamente los registros de la herramienta de respaldos en busca de fallos o errores. En caso de encontrar fallas o errores críticos, gestiona y reporta al jefe inmediato en	Alertas y Registros de la Herramienta	Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Registro de eventos o Informe mensuales de gestión de riesgos

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	los informes de gestión de riesgos.			
	¿La ejecución es correcta? Si: Continúa con la actividad No 8. No: Continúa con la actividad No 6.			
6	Revisar y corregir Revisa y realiza las acciones necesarias para corregir la falla o error en el respaldo.		Técnico / Contratista / Profesional Universitario Oficina TIC	Informe mensual de gestión de riesgos
7	Ejecutar respaldo de forma Manual Ejecuta la tarea de respaldo de forma manual. Continúa con la actividad No 5. Nota: En caso de no poder solucionar la falla por factores externos o fuera del alcance de la Oficina TIC en ese momento, reporta la incidencia al jefe de la Oficina TIC y proceder a la actividad No. 8.		Técnico / Contratista / Profesional Oficina TIC	Informe mensual de gestión de riesgos
	¿El respaldo se ejecutó con éxito? Si: Continúa con la actividad No 8.			

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	No: Continúa con la actividad No 6.			
8	Realizar el informe mensual Realiza el informe mensual de la gestión de riesgos asociado con respaldos. Este informe deberá contener el grado de cumplimiento, las fallas más relevantes o críticas si las hubo y lecciones aprendidas cuando aplique.		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Informe mensual de gestión de riesgos
RESTAURACIÓN Y PRUEBAS				
1	Realizar selección de elementos a restaurar o probar <u>Para solicitud de restauración:</u> Selecciona, del listado de la herramienta de respaldo, el elemento a restaurar. En el caso de Office 365, seleccionar el usuario correspondiente. <u>Para pruebas:</u> Selecciona de acuerdo con el plan de trabajo elaborado en la actividad No. 1 de la		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Informe mensual de gestión

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	sección “RESPALDOS”.			
2	Comprobar Integridad Comprueba con las funciones de validación de la herramienta de respaldo (por ejemplo, Health Check) para verificar que el respaldo es íntegro y recuperable. Si la verificación falla, detiene el proceso y gestiona la incidencia. De no ser posible comprobar integridad, continúa con la siguiente actividad.		Administrador de infraestructura o encargado de la OTIC de la gestión de respaldos	Logs en la herramienta de respaldo
3	Realizar la restauración <u>Para solicitud de restauración:</u> Ejecuta la restauración desde la herramienta de respaldo, de acuerdo con los lineamientos de operación. <u>Para pruebas:</u> Restaura de acuerdo con el plan de trabajo en un ambiente controlado.	Lineamientos operativos	Administrador de infraestructura o encargado de la OTIC de la gestión de respaldos	Logs en la herramienta de respaldo
	¿Restauración exitosa?			

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	Si: Continúa con la actividad No. 4. No: Intente resolver según el tipo de fallo, restaure el punto de restauración inmediatamente anterior, ejecute nuevamente el respaldo. Si lo anterior no funciona, registra el incidente y notifica al jefe de la oficina TIC y finaliza el procedimiento. Nota: Se debe tomar el tiempo de restauración, desde el momento en que se accede a la herramienta hasta la finalización y configuraciones adicionales que requiera el elemento restaurado.			
4	Realizar la comprobación posterior Realiza una comprobación que el elemento restaurado funciona correctamente y que los datos son coherentes. En caso de fallo en la comprobación:	Herramienta de respaldos / Pruebas funcionales	Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Logs en la herramienta de respaldo o Informe mensual de gestión de riesgos

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	1) Documenta el error y conserva la evidencia (capturas, logs). 2) Selecciona y restaura el respaldo inmediatamente anterior que haya sido validado como íntegro. Nota 1: No aplica para datos de usuario final (office 365)			
5	Realizar Disposición Segura <u>Para solicitud de restauración:</u> La actividad no aplica, continua con la actividad 6. <u>Para pruebas:</u> Cuando aplique, realiza un borrado seguro o wipe del medio o partición donde se realizó la prueba.		Administrador de infraestructura o encargado OTIC de la gestión de respaldos	Informe mensual de gestión de riesgos
6	Realizar Informe Realiza o 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 mensual de gestión de riesgos
ENTREGA DE RESPALDOS A TERCEROS				

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	Realizar la solicitud Solicita al jefe de la Oficina TIC la copia de respaldo de la información objeto de interés.	Sistema de Gestión Documental Correo Electrónico	Líder de proceso o Terceros	Comunicación oficial
2	Realizar el análisis de aprobación Revisa la viabilidad de aprobación de la copia de respaldo y da la respuesta pertinente.	Sistema de Gestión Documental Correo Electrónico	Jefe de la Oficina TIC	Comunicación oficial
	¿aprueba la entrega de la copia de respaldo? No: Informa al peticionario las razones de la negación de la copia. Si: Informa al encargado de realizar las copias de seguridad y continúa con la actividad 3.			
3	Realizar Copia Realiza la copia solicitada, en el medio de almacenamiento dispuesto por la entidad o el solicitante y realiza un <i>Hash SHA256</i> para posterior verificación y garantizar la integridad de la información.		Técnico / Contratista / Profesional Oficina TIC.	Logs en la herramienta de respaldo

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
4	Entregar copia de respaldo Realiza la entrega al solicitante. Nota: En el memorando, correo electrónico o acta deberá constar el Hash generado.	Sistema de Gestión Documental Correo Electrónico	Jefe de la Oficina TIC	Comunicación oficial

Fuente: UAESP

7. CONTROL DE CAMBIOS:

TABLA 3 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	20/09/2022	Se incorporan lineamientos de operación para respaldos, pruebas de restauración y se amplía el procedimiento para estas pruebas.
04	11/09/2025	Se ajustan el objetivo, el alcance y las actividades de acuerdo con la política de backups, considerando

Versión	Fecha	Descripción de la modificación
		únicamente los respaldos de activos críticos. Se elimina el cronograma para integrarlo a un documento interno, debido a su carácter confidencial.

Fuente: UAESP

8. AUTORIZACIONES:

TABLA 4 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Wilson Manuel Rojas	Profesional universitario OTIC	
	Osbaldo Cortes Lozano	Profesional universitario OTIC	
Revisó	Jorge Alexis Rodriguez Meza	Jefe Oficina TIC	
	Luz Mary Palacios Castillo	Profesional Universitario Oficina Asesora de Planeación	
Aprobó	Marcela Toro Pascagaza	Jefe Oficina Asesora de Planeación	