



Instituto Tecnológico Superior del Occidente del Estado de Hidalgo  
Soporte Técnico

# GUÍA DE CONSERVACIÓN Y RESGUARDO DE LA INFORMACIÓN DIGITAL INSTITUCIONAL PARA EL TECNOLÓGICO SUPERIOR DEL OCCIDENTE DEL ESTADO DE HIDALGO.

Página 1 de 5

Mayo, 2025



**2025**  
Año de  
**La Mujer  
Indígena**

Carretera Mixquiahuala-Tula km. 2.5, Paseo del Agrarismo No. 2000,  
Mixquiahuala de Juárez, Hgo., C. P. 42700 Tel.: 738 735 4000 |  
[www.itsoeh.edu.mx](http://www.itsoeh.edu.mx)





## GUÍA PARA RESPALDO DE INFORMACIÓN DEL PERSONAL DOCENTE Y ADMINISTRATIVO

### Objetivo

Garantizar la protección de la información institucional generada y almacenada por el personal docente y administrativo mediante respaldos periódicos, que permitan su recuperación ante pérdidas, fallos o daños.

### Alcance

Personal Directivo, Docente y Administrativo del Instituto que haga uso de equipos institucionales (de escritorio o portátiles) cuyas funciones requieran almacenar información sensible o relevante.

### Responsables

- Usuarios Finales: Deben resguardar su información en las carpetas indicadas y evitar almacenar en lugares no respaldados y poco confiables.

### Frecuencia de Respaldo

Con el fin de garantizar la disponibilidad y recuperación de la información ante cualquier eventualidad, se establece la siguiente frecuencia de respaldo en función del perfil del usuario y la criticidad de los datos que maneja:

- Directores: respaldo diario, al finalizar la jornada laboral. Por el uso de documentos que se actualizan constantemente y bases de datos con información muy sensible y oficial, para evitar pérdidas críticas.
- Docentes: respaldo semanal, ya que generan menor volumen de información y la actualización es moderada.





- Administrativos: respaldo diario, al finalizar la jornada laboral. Por el uso de documentos que se actualizan constantemente y bases de datos con información muy sensible y oficial, para evitar pérdidas críticas.

### Medios y Ubicación de Respaldo

Las copias de seguridad se deben almacenar en medios seguro, confiables y accesibles, con el objetivo de garantizar la recuperación de la información en caso de pérdida, daño al equipo de cómputo (de escritorio o portátil), o algún otro incidente.

- Servicios en la nube (Google Drive), se utilizarán plataformas oficiales Institucionales vinculadas a las cuentas de las Áreas y del personal Directivo, Docente y Administrativo para un acceso remoto de múltiples dispositivos. Será responsabilidad del usuario almacenar los archivos relevantes en carpetas sincronizadas con la nube.
- En caso de contar con discos duros externos como medio de respaldo limitado (en casos especiales) como falta de acceso a la red, actividades fuera del Instituto.

Esto asegura que haya una o más copias de la información en lugares seguros y accesibles.

***Nota: Queda estrictamente prohibido el uso de cuentas personales para fines institucionales, así como el almacenamiento de información sensible en plataformas no autorizadas.***

Con el fin de asegurar que la información sea incluida correctamente en los respaldos automáticos o manuales, los usuarios deberán evitar almacenar archivos en carpetas o ubicaciones no monitoreadas como carpetas personales, memorias USB como almacenamiento permanente ya que representan un riesgo alto de pérdida.

Los usuarios son responsables de verificar que sus archivos se encuentren en las rutas de respaldo que asignen y en su caso de reportar cualquier anomalía detectada en su equipo que pueda afectar el proceso. Así mismo deberá ejecutar y/o revisar que el respaldo se haya hecho de forma correcta y registrarlo en la bitácora que el respaldo fue exitoso.

### Retención de la Información

Para asegurar la trazabilidad de los datos y permitir la recuperación de versiones anteriores de archivos, se sugiere los siguientes periodos de retención para las copias de seguridad, según su frecuencia:





- Respaldos diarios: 15 días.
- Respaldos semanales: 3 meses.
- Respaldos mensuales: 1 año.

Esto ayuda a recuperar versiones antiguas de archivos y optimiza el uso del almacenamiento. La correcta gestión del ciclo de vida de los respaldos permite optimizar el uso del almacenamiento, reducir riesgos de acumulación innecesaria de datos y asegurar el cumplimiento de normas internas y externas de protección de información.

### Seguridad y Confidencialidad

Con la finalidad de proteger la información Institucional almacenada, asegura que toda la información respaldada esté protegida contra accesos no autorizados mediante:

- Acceso restringido solo al personal autorizado.
- Monitoreo constante de la integridad de los archivos respaldados.

### Anexos

Se incluyen documentos complementarios como:

- Formatos de bitácora para registrar respaldos.





Instituto Tecnológico Superior del Occidente del Estado de Hidalgo  
Soporte Técnico



BITÁCORA DE RESPALDOS DE INFORMACIÓN

Área: \_\_\_\_\_

Fecha de respaldo	Cargos y documentos respaldados	Medio de respaldo utilizado

Responsable: \_\_\_\_\_  
Nombre y Firma



### Conclusion

La implementación de una guía para la realización de respaldos permite asegurar que la información generada por el personal docente y administrativo se mantenga protegida, disponible y recuperable ante cualquier eventualidad. Seguir estas indicaciones facilita la continuidad de las actividades institucionales y minimiza el riesgo de pérdida de datos importantes.

ELABORÓ

ING. IVAN RODRIGUEZ HERNANDEZ  
ENCARGADO DEL ÁREA DE SOPORTE  
TÉCNICO

VO. BO.

MTRO. ÁNGEL HERNÁNDEZ CABRERA  
DIRECTOR DE PLANEACIÓN Y  
VINCULACIÓN



