Procedimiento de Seguridad: Backup Automático de Estaciones de Trabajo con Google Drive

1. Propósito

Este procedimiento establece las directrices y medidas de seguridad para la implementación y gestión del backup automático de las estaciones de trabajo de los funcionarios utilizando la herramienta **Google Drive**. El objetivo es proteger la información crítica de **INFOTEP** almacenada en los equipos locales de los usuarios, facilitar su recuperación en caso de fallo del hardware o pérdida de datos, y asegurar la continuidad del negocio. El backup se realizará utilizando la cuenta institucional de Google Workspace asociada al correo electrónico de cada usuario.

2. Alcance

Este procedimiento aplica a todos los funcionarios, contratistas y personal autorizado que utilicen una estación de trabajo (computador de escritorio o portátil) propiedad de la institución y que cuenten con una licencia activa de Google Workspace. Cubre la configuración, el mantenimiento, la seguridad de la información y las responsabilidades del usuario y del personal de TI.

3. Definiciones

- **Estación de Trabajo:** Cualquier computador de escritorio o portátil utilizado para realizar funciones laborales.
- **Google Drive:** Servicio de almacenamiento en la nube de Google, vinculado a la cuenta corporativa del usuario.
- **Google Drive para escritorio:** La aplicación de software que se instala en la estación de trabajo para sincronizar carpetas y archivos entre el equipo local y la nube de Google Drive.
- **Backup Automático / Sincronización:** Proceso mediante el cual los archivos y carpetas locales designados se replican de forma continua en Google Drive. Es importante entender que es una **sincronización**: los cambios (modificaciones, eliminaciones) en el equipo local se reflejan en la nube y viceversa.
- **Autenticación en Dos Pasos (2SV):** El término de Google para la Autenticación Multifactor (MFA), un método de seguridad que requiere una segunda forma de verificación para acceder a una cuenta.

4. Responsabilidades

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Usuarios:**
  - Asegurar que la aplicación Google Drive para escritorio esté activa y con la sesión iniciada en su estación de trabajo.
  - Verificar periódicamente el estado de la sincronización y reportar cualquier error o anomalía al Departamento de TI.
  - Utilizar contraseñas seguras y únicas para su cuenta de Google Workspace y tener habilitada obligatoriamente la Autenticación en Dos Pasos (2SV).
  - Almacenar todos los archivos de trabajo dentro de las carpetas configuradas para la sincronización con Google Drive (principalmente Escritorio y Documentos).
  - No almacenar software ilegal, material personal no autorizado, o archivos que violen las políticas de la empresa en las carpetas sincronizadas.
  - Informar inmediatamente al Departamento de TI en caso de pérdida o robo del equipo, o si sospecha que su cuenta ha sido comprometida.
- **Departamento de TI / Seguridad de la Información:**
  - Asegurar que la aplicación Google Drive para escritorio esté instalada en todas las estaciones de trabajo nuevas.
  - Proveer guías claras y capacitación a los usuarios sobre cómo configurar y verificar la sincronización de carpetas.
  - Utilizar la Consola de Administración de Google Workspace para establecer y hacer cumplir las políticas de seguridad, como la obligatoriedad de la 2SV.
  - Asistir a los usuarios en la recuperación de archivos desde Google Drive cuando sea necesario.
  - Gestionar el acceso y la transferencia de datos de Google Drive de los empleados que dejan la organización.
  - Monitorear el uso del almacenamiento y la actividad sospechosa a través de la Consola de Administración.
  - Revisar y actualizar este procedimiento anualmente.

5. Procedimiento de Configuración del Backup Automático

- **5.1. Instalación e Inicio de Sesión:**
  1. El Departamento de TI se asegurará de que la última versión de **Google Drive para Escritorio** esté instalada en la estación de trabajo.
  2. El usuario deberá iniciar la aplicación e ingresar con su correo electrónico corporativo y su contraseña.
  3. El usuario deberá completar la verificación de Autenticación en Dos Pasos (2SV) si se le solicita.

- **5.2. Selección de Carpetas para Sincronización:**
  1. Una vez iniciada la sesión, el usuario debe hacer clic en el ícono de Google Drive en la barra de tareas (Windows) o en la barra de menús (macOS) y seleccionar el ícono de engranaje (⚙) para ir a **"Preferencias"**.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

2. En la sección **"Carpetas de mi ordenador"** o **"Mi PC"**, el usuario debe hacer clic en **"Añadir carpeta"**.
3. Se deben seleccionar y configurar para la sincronización las siguientes carpetas locales:
    - **Obligatorio:** `C:\Users\[TuUsuario]\Documents` (Documentos)
    - **Obligatorio:** `C:\Users\[TuUsuario]\Desktop` (Escritorio)
    - **Opcional:** `C:\Users\[TuUsuario]\Pictures` (Imágenes), `C:\Users\[TuUsuario]\Videos` (Videos), etc., si contienen información laboral relevante.
4. Asegurarse de que la opción **"Sincronizar con Google Drive"** esté seleccionada para cada carpeta añadida.
5. **Exclusiones:** No se deben sincronizar carpetas que contengan instalaciones de software (ej. Program Files), archivos de sistema operativo, archivos temporales, o grandes volúmenes de datos personales no relacionados con el trabajo.

- **5.3. Verificación de la Sincronización:**
    - El usuario debe verificar que el ícono de Google Drive no muestre errores. Un ícono estático y sin alertas indica que la sincronización está completa y activa.
    - Se recomienda al usuario acceder a Google Drive desde un navegador web (drive.google.com) y comprobar que existe una sección llamada **"Ordenadores"** o **"Computers"** donde puede ver y acceder a los archivos de su estación de trabajo.

6. Medidas de Seguridad

- **6.1. Seguridad de la Cuenta:**
    - **Contraseñas Robustas:** Todos los usuarios deben cumplir la política de contraseñas de la institución.
    - **Autenticación en Dos Pasos (2SV):** Su uso es **obligatorio**. El Departamento de TI forzará esta política desde la Consola de Administración de Google Workspace.
    - **Concienciación sobre Phishing:** Los usuarios deben estar capacitados para no caer en correos fraudulentos que busquen robar sus credenciales de Google Workspace.
- **6.2. Seguridad de los Datos:**
    - **Cifrado:** Google Drive cifra automáticamente todos los datos en tránsito y en reposo. No se requiere ninguna acción del usuario.
    - **Uso Compartido de Archivos:** Los usuarios deben adherirse estrictamente a la política de compartición de datos. Se debe evitar compartir archivos con la opción "Cualquier persona con el enlace" para información sensible. El acceso debe limitarse a usuarios específicos.
    - **Papelera e Historial de Versiones:** Los usuarios deben saber que los archivos eliminados van a la Papelera de Google Drive, donde permanecen por 30 días antes de ser eliminados permanentemente. Google Drive también guarda un

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

historial de versiones de los archivos, lo que permite restaurar una versión anterior en caso de modificación no deseada o corrupción.

- **6.3. Seguridad de la Estación de Trabajo:**
  - Mantener el sistema operativo y el software antivirus actualizados.
  - Bloquear la sesión del equipo cuando el usuario se ausente.
  - No instalar software de fuentes no confiables.

7. Procedimiento de Recuperación de Datos

- **7.1. Auto-servicio por el Usuario:**
  - **Archivos Eliminados:** El usuario puede restaurar archivos desde la "Papelera" en la interfaz web de Google Drive.
  - **Versiones Anteriores:** Para restaurar una versión previa de un archivo, el usuario puede hacer clic derecho sobre el archivo en Google Drive (web) y seleccionar "Gestionar versiones" o "Historial de versiones".
- **7.2. Asistencia del Departamento de TI:**
  - En casos de eliminación permanente (tras vaciar la papelera) o pérdida de datos complejos, el usuario debe contactar al Departamento de TI inmediatamente.
  - El administrador de Google Workspace tiene un periodo limitado (aproximadamente 25 días desde la eliminación permanente) para intentar restaurar datos eliminados de la cuenta de un usuario a través de la Consola de Administración.
- **7.3. Limitaciones Importantes (Riesgo de Sincronización):**
  - Se debe entender que Google Drive es una herramienta de **sincronización**, no un backup tradicional aislado. Si un archivo es dañado o cifrado por ransomware en la estación de trabajo, la versión dañada se sincronizará con la nube. La principal defensa en este caso es el **historial de versiones** y una rápida respuesta para evitar la propagación.

8. Proceso de Incorporación y salida de Usuarios

- **8.1. Incorporación:**
  - El Departamento de TI instalará y guiará al nuevo usuario en la configuración de Google Drive para escritorio según este procedimiento.
  - Se proporcionará la capacitación necesaria sobre su uso y las políticas de seguridad.

- **8.2. Salida de colaboradores:**
  - Al notificarse la salida de un funcionario o contratista, el Departamento de TI seguirá un protocolo estricto:
  2. Cambiar la contraseña de la cuenta del usuario para revocar su acceso inmediatamente.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

3. Utilizar la Consola de Administración para transferir la propiedad de todos los archivos y carpetas del usuario a su supervisor o a una cuenta de archivo designada.
4. Una vez asegurados los datos, la cuenta del usuario será suspendida y posteriormente eliminada de acuerdo con la política de retención de datos de la institución.

9. Monitoreo y Auditoría

- El Departamento de TI utilizará los informes y registros de auditoría de la Consola de Administración de Google Workspace para supervisar el uso del almacenamiento, la actividad de inicio de sesión y los eventos de compartición de archivos para detectar comportamientos anómalos o incumplimientos de la política.

10. Revisión del Procedimiento

Este documento será revisado anualmente, o antes si ocurren cambios significativos en la tecnología de Google Workspace o en las políticas de seguridad del INFOTEP.

Versión: 1.0 **Fecha de Entrada en Vigor:** 24 de junio de 2025 **Próxima Revisión:** 24 de junio de 2026 **responsable:** Departamento de TI / Seguridad de la Información

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai