

# Política de Copias de Seguridad

## 1. Frecuencia de Copias de Seguridad:

- Se realizarán copias de seguridad de forma regular, al menos una vez al día.
- La copia de seguridad principal se realizará en la versión actual del trabajo en curso, mientras que la segunda copia se actualizará solo cuando se suba al repositorio remoto una versión estable con cambios notables.

## 2. Ubicaciones de Copias de Seguridad:

### - Repositorio Remoto en GitHub:

- Una copia de seguridad se almacenará de forma automática en un repositorio remoto de GitHub. Esto garantiza una copia fuera del entorno local y proporciona una capa adicional de seguridad y colaboración.
- Esta copia de seguridad en GitHub servirá como una versión estable y se actualizará cuando se realicen cambios notables y se haya probado la estabilidad.

### - Dispositivo de Trabajo:

- La copia principal se mantendrá en el dispositivo de trabajo, donde se están realizando las modificaciones. Esto proporciona accesibilidad rápida y facilita el desarrollo continuo.
- Se recomienda realizar copias de seguridad incrementales para evitar la pérdida de datos en caso de un fallo del sistema o pérdida de archivos importantes.

### - Segundo Dispositivo:

- Una segunda copia de seguridad se almacenará en un dispositivo diferente, preferiblemente ubicado en un lugar físico separado del dispositivo principal. Esto actúa como una capa adicional de protección contra pérdidas de datos debido a desastres naturales, robos, o fallas de hardware en el dispositivo de trabajo principal.

## 3. Proceso de Actualización:

- La copia de seguridad en GitHub se actualizará manualmente o automáticamente cuando se haya alcanzado una versión estable con cambios notables.
- Antes de actualizar la copia en GitHub, se realizarán pruebas exhaustivas para garantizar la estabilidad y la integridad de la versión actualizada.

## 4. Procedimientos de Recuperación:

- Se establecerán procedimientos claros y detallados para la recuperación de datos en caso de pérdida o corrupción.
- Se realizarán simulacros periódicos de recuperación para garantizar la eficacia de los procedimientos establecidos.

## **5. Monitoreo y Mantenimiento:**

- Se implementará un sistema de monitoreo para verificar la integridad de las copias de seguridad.
- Se realizarán revisiones periódicas de la política de copias de seguridad para adaptarse a cambios en el entorno tecnológico o en los requisitos del proyecto.

## **6. Seguridad:**

- Todas las copias de seguridad estarán protegidas mediante medidas de seguridad, como cifrado, para garantizar la confidencialidad de los datos.

Esta política integral de copias de seguridad asegura la protección de los datos en todas las etapas del proceso, desde el trabajo diario hasta la preservación de versiones estables en repositorios remotos y dispositivos adicionales.