TaskMaster Pro

Plan de respaldo

Versión: 0100

Fecha: 03/07/2025

HOJA DE CONTROL

Organismo	SENA		
Proyecto	TaskMaster Pro		
Entregable	Plan de respaldo		
Autor	Johan Felipe Garcia Salazar Andres Julian Garzón Perea		
Aprobado por		**Fecha Aprobación**	
		Nº Total de Páginas	10

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Versión inicial	Johan Felipe Garcia Salazar	03/07/2025

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Johan Felipe Garcia Salazar
Andres Julian Garzón Perea
Nikole Camila Bernal Avila
Erika Daniela Triana Bustos

Objetivo.

Asegurar la continuidad de la empresa, garantizando la disponibilidad, integridad y recuperación de los datos y sistemas críticos ante posibles incidentes, como fallos técnicos, errores humanos o pérdida de datos. Esto por medio de una estrategia integral y confiable que se redactará en la continuidad de este documento.

1. Componentes a respaldar:

- Base de datos: task_master tipo SQL la cual está dentro del repositorio en GitHub.
- Archivos del sistema: Carpeta como tal del proyecto Backend y Frontend dentro del repositorio en GitHub.

2. Frecuencia de respaldo:

- Base de datos: Diaria dentro del repositorio.
- Código fuente: Es automático con cada commit/push usando Git/GitHub.

3. Estrategia de almacenamiento:

- Ubicaciones seguras y redundantes como GitHub privado para código fuente.
- Cifrado aplicado a los respaldos de compresión cifrada como zip -o 7zip.
- Nomenclatura estándar para los archivos de respaldo, usando un formato claro y consistente (ejemplo: (**(task_master)_03_2025_07_DD.backup**).

4. Procedimientos de respaldo:

Respaldo de la base de datos MySQL

Para garantizar la integridad y recuperación del sistema en caso de pérdida o corrupción de datos, es necesario realizar respaldos periódicos de la base de datos.

Requisitos previos

- Tener XAMPP correctamente instalado y en ejecución.
- Asegurarse de que los módulos Apache y MySQL estén activos.
- Verificar que la base de datos del sistema esté creada y funcional.
- Tener instalada la utilidad de línea de comandos mysqldump (incluida en XAMPP).

Comando de respaldo

- Desde la terminal o símbolo del sistema, ejecutar el siguiente comando:

  mysqldump -u root -p task_master > respaldo_taskmaster.sql

- Nota: Sustituir task_master por el nombre real de tu base de datos, por ejemplo, taskmasterdb.
- El sistema pedirá la contraseña del usuario MySQL (por defecto suele estar vacía en XAMPP).

Ejemplo práctico

- Mysqldump -u root taskmasterdb > D:\TaskMasterPro\db\backups\respaldo_2025-07-03.sql

Verificación del respaldo

- Ubicación esperada del archivo:
- D:\TaskMasterPro\db\backups\respaldo_YYYY-MM-DD.sql

Verificaciones para realizar:

- Confirmar que el archivo fue creado exitosamente en la ruta indicada.
- Validar que el archivo tenga tamaño mayor a 0 KB.
- Comprobar la fecha de creación/modificación para verificar que corresponde al respaldo reciente.

Respaldo del Código Fuente:

- Directamente en el repositorio ubicado en el siguiente enlace https://github.com/FGFERNAN/TaskMasterPro.git siempre encontraremos una copia del proyecto actualizada, en el paso a paso solo tendríamos que clonar y sincronizar el repositorio en el equipo.

5. Restauración y pruebas:

Restauración y Pruebas

Con el fin de garantizar la efectividad de los mecanismos de respaldo y la capacidad de recuperación ante incidentes, se establece la siguiente metodología para la restauración periódica del sistema:

Restauración de la base de datos MySQL

Periodicidad

- Mensualmente, el equipo técnico debe realizar una restauración completa de la base de datos en un entorno de prueba o sandbox.

Metodología de restauración

Crear una base de datos vacía en el entorno de prueba (por ejemplo, taskmasterdb_test) desde phpMyAdmin o usando terminal:

sql
CopiarEditar
CREATE DATABASE taskmasterdb_test;

1. Restaurar el respaldo más reciente con el siguiente comando:

   bash
   CopiarEditar
   mysql -u root -p taskmasterdb_test < respaldo_YYYY-MM-DD.sql

2. Asegurarse de cambiar el nombre del archivo .sql por el correspondiente.

3. Verificar que la base se haya restaurado correctamente:
   - Ingresar a phpMyAdmin y revisar que las tablas estén presentes.
   - Comprobar que los datos estén accesibles (usuarios, proyectos, tareas, etc.).
   - Correr consultas básicas para validar integridad.

Criterios de validación

- Todas las tablas deben existir.
- El número de registros debe coincidir con la base original.
- Se debe poder iniciar sesión desde el frontend conectado al entorno de prueba.

2. Restauración del código fuente

Periodicidad

- Mensualmente, se debe probar que los respaldos comprimidos del código fuente sean funcionales y estén íntegros.

Metodología de verificación

Seleccionar el respaldo comprimido más reciente, por ejemplo:

python
CopiarEditar
respaldo_codigo_taskmaster_2025-07-03.zip

1. Extraer el archivo comprimido en un entorno de prueba:
    - Verificar que se descompriman correctamente las carpetas backend_web, frontend_web, db, uploads, etc.
2. Ejecutar el sistema de forma local o en sandbox:
    - Instalar dependencias con npm install en backend_web y frontend_web.
    - Iniciar ambos servidores (npm start o el comando correspondiente).
    - Conectar el sistema al entorno de prueba con la base de datos restaurada.

Criterios de validación

- La descompresión debe finalizar sin errores.

- La estructura del código debe estar intacta.
- El sistema debe funcionar sin fallos en el entorno de prueba.
- El frontend y backend deben comunicarse correctamente.

6. Políticas de retención:

Con el fin de optimizar el uso de los recursos de almacenamiento y garantizar la disponibilidad de versiones históricas confiables para la recuperación de datos, se establecen las siguientes políticas de retención según el tipo de respaldo:

Tipo de Respaldo	Periodo de Retención	Uso Típico
Diario	7 días	Recuperación rápida de errores recientes.
Semanal	1 mes	Balance entre espacio y flexibilidad.
Mensual	6 meses o más	Cumplimiento legal o auditorías.

7. Responsable del respaldo:

El responsable deberá coordinar las tareas de respaldo, monitorear el cumplimiento de las políticas de retención, mantener actualizada la documentación técnica del proceso y realizar pruebas periódicas de restauración para garantizar la efectividad del plan.

Principal:

Nombre del Responsable:	Andres Julian Garzón Perea
Rol en el Proyecto	Administrador del Sistema
Correo Electrónico	ajgarzon662@soy.sena.edu.co
Teléfono de Contacto	+57 324 3850896

Alterno:

Nombre del Responsable:	Johan Felipe Garcia Salazar
Rol en el Proyecto	Administrador del Sistema
Correo Electrónico	jfgarcia463@soy.sena.edu.co
Teléfono de Contacto	+57 310 7847573

Conclusión:

El proceso de respaldo debe ser realizado exclusivamente por los usuarios que cuenten con privilegios administrativos y acceso autorizado a información sensible del sistema, garantizando así la confidencialidad y la seguridad de los datos críticos. Que en este caso serían:

- Administradores de sistemas/BD (para datos críticos)

- Personal de TI/Soporte (con credenciales de backup validadas).

La frecuencia y horario del respaldo se elige en este momento, en base al tráfico de datos que afronta el sistema actualmente, al ser un tráfico leve o suave, no es necesario hacer un backup diario, por ende la la frecuencia que se elige es **semanal** y el horario será todos los lunes a las 5 AM, previo a inicio de operaciones en el SENA. Este proceso se realizará de manera automatizada y supervisada por el responsable designado. Esta frecuencia permite mantener una copia reciente del sistema, minimizando el riesgo de pérdida de información y asegurando la continuidad operativa ante cualquier eventualidad

Preguntas

Para garantizar que el plan de respaldo se implemente correctamente, es crucial resolver cualquier duda sobre:

1. Términos Técnicos o Conceptos

¿Cómo se diferencia un respaldo incremental de uno completo?

R/: Un respaldo completo copia todos los datos seleccionados, sin importar si han cambiado o no desde el último respaldo. Un respaldo incremental, en cambio, solo guarda los archivos que han cambiado desde el último respaldo, lo cual ahorra espacio y tiempo de ejecución.

¿Qué herramientas usaremos para automatizar los backups?

R/: Dependiendo del entorno, se puede usar software como mysqldump (para bases de datos MySQL), rsync, cron jobs, o servicios en la nube como Google Cloud Backup, AWS Backup, o herramientas específicas del entorno de desarrollo.

¿Qué es una política de retención y cómo afecta al espacio de almacenamiento?

R/: Es la norma que define cuánto tiempo se conservan los respaldos antes de eliminarlos. Afecta el espacio de almacenamiento porque determina la cantidad de respaldos que se acumulan. Una buena política equilibra la disponibilidad de versiones históricas y el uso eficiente del espacio.

¿Qué se entiende por integridad de los datos en el contexto del respaldo?

R/: La integridad se refiere a que los datos respaldados no estén corruptos ni incompletos y que puedan ser restaurados en su estado original. Esto se asegura con verificaciones automáticas o pruebas de restauración.

2. Instrucciones o Procedimientos

¿El horario de respaldo semanal (Lunes 5:00 AM) aplica también en días festivos?

R/: Depende, si el proceso ya se encuentra completamente automatizado, entonces si. En caso de que no, se realizará el proceso el siguiente día hábil. Lo ideal es automatizar el proceso y solo notificar en caso de que falle.

¿Qué debo hacer si el sistema notifica un fallo durante el respaldo automático?

R/: Lo primero es que se deben verificar los logs, luego notificar al responsable de TI y ejecutar un respaldo manual en caso de que sea algo crítico.

¿Dónde están ubicados los respaldos una vez que se generan?

R/: Generalmente se almacenan en servidores dedicados o en unidades externas en rutas previamente definidas por el administrador del sistema. Por ejemplo: `/backups/`

3. Roles y Responsabilidades

Si el responsable principal no está disponible, ¿quién es el siguiente en la cadena de soporte?

R/: El responsable alterno debe tomar el control. Sus datos están en la sección "Responsable del Respaldo".

¿Quién debe validar que los respaldos se están haciendo según la frecuencia establecida?

R/: El responsable del respaldo, quien debe verificar periódicamente que los respaldos se generen según lo establecido en el cronograma y que los archivos estén íntegros.

¿Un desarrollador puede acceder a los respaldos o solo el administrador del sistema?

R/: Por razones de seguridad, el acceso a los respaldos debe ser restringido al administrador del sistema o a personal con permisos explícitos. Los desarrolladores no deben tener acceso directo a la información sensible respaldada.