

*GERO Y NATIS*

*Plan de Respaldo*

*Daniel Felipe Bermeo Torres*

*Deisy Caterine Gonzalez Bueno*

*Jennifer Vanessa Mateus Farfan*

*ADSO – 2900602*

1. Tabla de contenido

[1. Introducción 3](#_heading=h.sjhc5iu7fye4)

[2. Objetivos 3](#_heading=h.w22mgmz7laow)

[3. Componentes Críticos del Sistema 3](#_heading=h.fn50p3sdsyoj)

[4. Frecuencia de los Respaldos 4](#_heading=h.rkvcra2byv0d)

[5. Métodos y Medios de Almacenamiento 4](#_heading=h.t6bxo3dzaqaj)

[5.1 Medios de Almacenamiento Recomendados 4](#_heading=h.woibgl8sijrr)

[5.2 Formatos de Respaldos 4](#_heading=h.2m6o1vau4yju)

[6. Validación de los Respaldos 4](#_heading=h.ujw0cax0desd)

[6.1 Pruebas Periódicas 5](#_heading=h.y7yp7aa6q0s7)

[6.2 Retención de Versiones 5](#_heading=h.smm2l4ox8qtj)

[7. Responsables del Plan de Respaldo 5](#_heading=h.6lvfaus5n7n7)

[8. Seguridad del Plan de Respaldo 5](#_heading=h.q66x1jjcplro)

[9. Procedimiento para Realizar un Respaldo 5](#_heading=h.dyosq7fu4b0w)

[10. Actualización del Plan de Respaldo 7](#_heading=h.7z89pmhzq6p8)

[11. Anexos Recomendados 8](#_heading=h.2gudcy97g5ac)

# 1. Introducción

El presente Plan de Respaldo tiene como finalidad establecer estrategias claras y procedimientos técnicos para salvaguardar los componentes críticos del sistema web [NOMBRE DEL SISTEMA], garantizando su disponibilidad, integridad y posibilidad de recuperación ante fallos técnicos, errores humanos o amenazas externas.

Este documento está diseñado como complemento al Plan de Restauración y busca prevenir la pérdida de información, minimizar tiempos de inactividad y asegurar la continuidad operativa del sistema.

## 2. Objetivos

* Establecer un proceso estandarizado para realizar copias de seguridad (backups) del sistema.
* Identificar los elementos clave del sistema que deben incluirse en cada respaldo.
* Definir frecuencias adecuadas de respaldo según la criticidad de los componentes.
* Garantizar la integridad y accesibilidad de los respaldos mediante validaciones periódicas.
* Promover la seguridad y confidencialidad de los archivos respaldados.
* Asignar responsables y roles específicos dentro del plan.
* Documentar todas las acciones realizadas durante el proceso de respaldo.

## 3. Componentes Críticos del Sistema

Para un respaldo completo del sistema, se identifican los siguientes elementos:

| **Componentes** | **Descripción** |
| --- | --- |
| Archivos del código fuente | Páginas HTML, CSS, PHP, JavaScript, Bootstrap y demás recursos front-end y back-end. |
| Base de datos | Estructura y datos almacenados en [TIPO DE BASE DE DATOS]. |
| Configuraciones del servidor | Archivos **.env**, ajustes de [SERVIDOR WEB], permisos y variables de entorno. |
| Archivos multimedia | Imágenes, logos, documentos cargados por usuarios. |
| Documentación del sistema | Manual de usuario, guías técnicas, políticas de seguridad. |

## 4. Frecuencia de los Respaldos

Se define una periodicidad acorde a la criticidad de cada componente:

| **Componente** | **Frecuencia recomendada** | **Observaciones** |
| --- | --- | --- |
| Bases de datos | Diaria | Hasta que se implemente un sistema automatizado. |
| Archivos del proyecto | Semanal + antes de actualizaciones importantes | Incluye código fuente y recursos estáticos. |
| Configuraciones del servidor | Mensual o tras cambios significativos | Solo cuando haya modificaciones relevantes. |
| Archivos multimedia | Semanal | Si hay carga constante de nuevos archivos. |
| Documentación del sistema | Trimestral o tras actualización | Si se generan nuevos manuales o políticas. |

## 

## 5. Métodos y Medios de Almacenamiento

### 5.1 Medios de Almacenamiento Recomendados

* **Local**: Discos duros externos o USB cifrados
* **En la nube**: Plataformas como Google Drive, Dropbox, OneDrive o Amazon S3
* **Control de versiones**: Repositorios Git (GitHub, GitLab) exclusivamente para código fuente, sin contener datos sensibles ni credenciales

### 5.2 Formatos de Respaldos

* **Base de Datos**: Archivo **.sql** comprimido con **mysqldump** (o herramienta equivalente)
* **Archivos del sistema**: Paquetes comprimidos en formato **.zip** o **.tar.gz**
* **Configuraciones**: Archivos **.txt**, **.json**, **.php** según corresponda
* **Documentación**: PDF o DOCX organizados por versión

## 6. Validación de los Respaldos

Es fundamental verificar que los respaldos sean útiles y puedan restaurarse correctamente:

### 6.1 Pruebas Periódicas

* Realizar una prueba mensual de restauración en un entorno de desarrollo o prueba
* Verificar que la base de datos pueda importarse sin errores
* Confirmar que los archivos comprimidos no estén corruptos
* Probar funcionalidades básicas del sistema tras la restauración

### 6.2 Retención de Versiones

* Mantener al menos tres (3) versiones anteriores de cada tipo de respaldo:
  + Base de datos
  + Archivos del proyecto
  + Configuraciones del servidor
* Cada archivo debe tener un nombre claro que indique la fecha y propósito del respaldo (ej.: [nombre\_sistema]\_db\_20250612.sql)

## 7. Responsables del Plan de Respaldo

| **Tarea** | **Responsable** |
| --- | --- |
| Ejecutar respaldos diarios/semanales | Daniel Bermeo |
| Validar respaldos y probar restauración | Deisy Gonzalez |
| Gestionar medios de almacenamiento local y en nube | Vanessa Mateus |
| Supervisar y coordinar actividades | Equipo completo |

## 8. Seguridad del Plan de Respaldo

Para proteger los respaldos contra accesos no autorizados o corrupción:

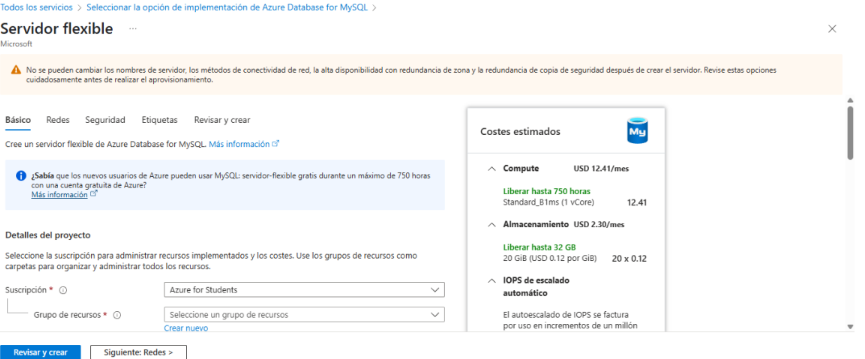
* Cifrado obligatorio en todos los medios de almacenamiento locales
* Acceso restringido solo a personal autorizado
* Registro de actividades relacionadas con la creación, acceso y modificación de respaldos
* Políticas de contraseñas seguras aplicadas a todos los repositorios y cuentas usadas

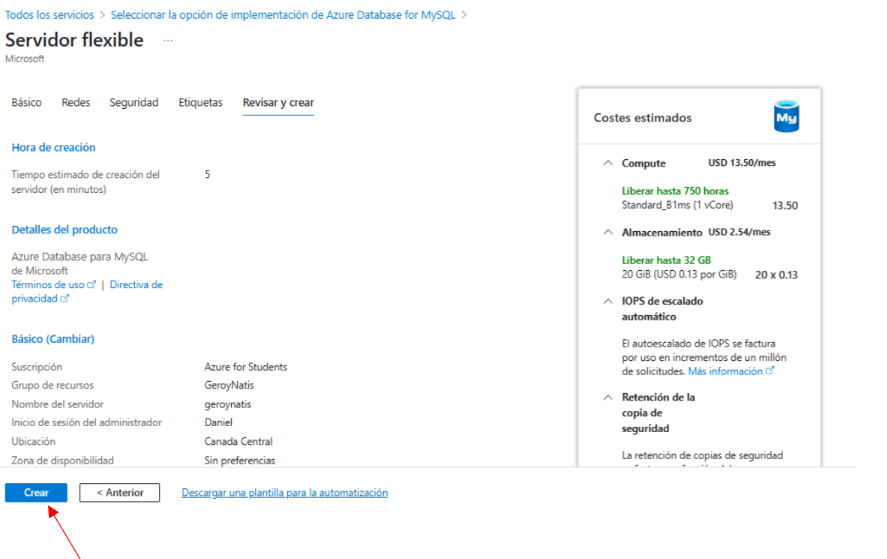
## 9. Procedimiento para Realizar un Respaldo

* **Paso 1: Preparación**
* Revisar qué componentes deben incluirse esta vez
* Verificar espacio disponible en dispositivos de almacenamiento
* Notificar al equipo sobre la realización del respaldo

**Paso 2: Generación de Respaldo**

* Exportar la base de datos usando la herramienta correspondiente
* Comprimir los archivos del proyecto y recursos multimedia
* Guardar configuraciones del servidor y archivos **.env**
* Subir respaldo a nube y/o guardar en disco seguro



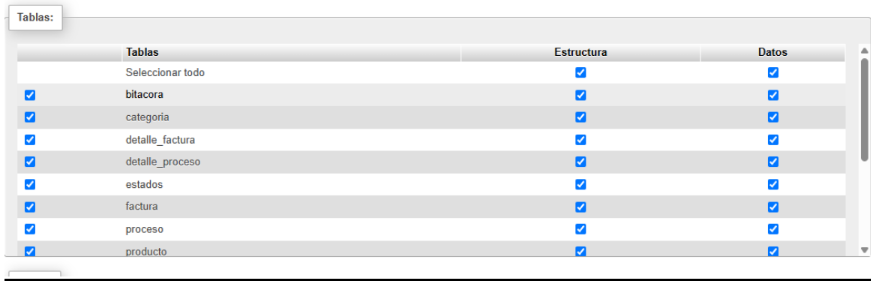


**Paso 3: Validación**

* Descomprimir y revisar los archivos
* Importar la base de datos en un entorno de prueba
* Verificar funcionamiento básico del sistema

**Paso 4: Registro**

* Anotar en la bitácora de respaldos:
  + Fecha y hora
  + Responsable



## 10. Actualización del Plan de Respaldo

El presente plan será revisado y actualizado cada 3 meses o cuando ocurra alguno de los siguientes eventos:

* Cambios significativos en la arquitectura del sistema
* Modificaciones en el equipo de desarrollo o roles
* Incorporación de nuevas funcionalidades críticas
* Actualización de políticas de seguridad o cumplimiento normativo

Cada nueva versión del plan debe incluir:

* Registro de los cambios realizados
* Versión actualizada del documento
* Notificación formal al equipo

## 11. Anexos Recomendados

1. Guía básica de uso de repositorios Git
2. Checklist de validación post-respaldo
3. Políticas de seguridad y control de accesos
4. Lista de contactos clave del equipo