**PLAN DE RESPALDO – PIXEL STORE**

**1. Objetivo**

El objetivo del presente Plan de Respaldo es establecer las políticas, procedimientos y herramientas necesarias para garantizar la protección, integridad, disponibilidad y recuperación de la información crítica de la plataforma Pixel Store, desarrollada por QuantumLeap. Este plan busca prevenir la pérdida de datos y asegurar la continuidad operativa del sistema ante fallas técnicas, errores humanos, ataques cibernéticos o cualquier evento que afecte los activos digitales del proyecto.

**2. Alcance**

Este plan aplica a todos los componentes tecnológicos involucrados en el desarrollo, implementación y operación del sistema Pixel Store. Incluye los siguientes elementos clave:

* Base de datos principal del sistema (MySQL).
* Aplicación backend desarrollada en Python (Flask).
* Aplicación frontend desarrollada en React.
* Imágenes y recursos multimedia almacenados en Cloudinary.
* Archivos de configuración, documentación técnica y scripts de mantenimiento.
* Repositorios de código (GitHub).

**3. Estrategias de Respaldo**

Para salvaguardar los activos digitales del sistema, se utilizarán varias estrategias combinadas de respaldo. Estas incluyen respaldos completos, incrementales y diferenciales, respaldos locales y en la nube, y automatización de tareas críticas.

**3.1 Tipos de Respaldo**

| **Tipo de respaldo** | **Descripción** |
| --- | --- |
| Completo | Copia íntegra de todos los archivos y bases de datos. |
| Incremental | Copia únicamente los datos que han cambiado desde el último respaldo. |
| Diferencial | Copia los datos que han cambiado desde el último respaldo completo. |

**3.2 Frecuencia y Ubicación**

| **Elemento** | **Frecuencia** | **Método** | **Ubicación** |
| --- | --- | --- | --- |
| Base de datos | Diario | Script automático cron | Google Drive + disco local seguro |
| Backend (Flask) | Semanal | Compresión .zip | Servidor externo + USB encriptado |
| Frontend (React) | Semanal | GitHub + copia .zip | Repositorio + carpeta sincronizada |
| Imágenes (Cloudinary) | Automático | Backup automático nativo | Cuenta Cloudinary + backup semanal |
| Documentación técnica | Mensual | Compresión y cifrado | Google Drive + Dropbox compartido |

**4. Herramientas Utilizadas**

* **Cron + bash**: Para programar tareas automáticas de respaldo en el servidor.
* **Google Drive API**: Para subir automáticamente respaldos comprimidos y cifrados.
* **Cloudinary**: Para gestión automatizada de imágenes con respaldo propio.
* **Git/GitHub**: Control de versiones con respaldo remoto constante.
* **WinRAR/7-Zip**: Compresión y encriptado de archivos para respaldo local.
* **MySQLDump / pg\_dump**: Herramientas para exportar bases de datos completas.

**5. Procedimiento de Respaldo**

1. **Respaldo Diario (Base de datos):**
   * Hora: 3:00 AM
   * Script ejecuta mysqldump/pg\_dump
   * El archivo se comprime y sube automáticamente a Google Drive.
2. **Respaldo Semanal (Código fuente):**
   * Se genera un archivo comprimido (.zip) del backend y frontend.
   * Se almacena en un disco duro externo y se sube una copia a la nube.
3. **Respaldo Automático de Imágenes:**
   * Cloudinary realiza copias internas de forma automática.
   * Se descarga manualmente un backup completo una vez al mes.
4. **Verificación de integridad:**
   * Todos los respaldos se validan mediante hash SHA256.
   * Se registra cada respaldo en un archivo log de respaldo.

**6. Recuperación de Información**

En caso de pérdida de información, el procedimiento de recuperación es el siguiente:

* **Nivel 1 – Fallo menor:** Recuperación local desde el disco de respaldo.
* **Nivel 2 – Fallo total:** Recuperación desde Google Drive o Dropbox.
* **Nivel 3 – Catástrofe total:** Se reinstala el servidor base, se clona el repositorio desde GitHub y se importa la base de datos.

Tiempo estimado de recuperación total: **3 a 6 horas**.

**7. Políticas de Seguridad**

* Los respaldos estarán en carpetas cifradas con contraseña segura.
* Se realizará auditoría mensual del cumplimiento del plan de respaldo.
* Solo los administradores tendrán acceso a las copias almacenadas.
* Se utilizará autenticación en dos pasos para acceso a la nube.

**8. Registro de Respaldo**

Cada respaldo generado se documentará en un archivo de log con la siguiente información:

| **Fecha** | **Elemento respaldado** | **Tipo de respaldo** | **Ubicación** | **Hash de verificación** | **Responsable** |
| --- | --- | --- | --- | --- | --- |
| 20/05/2025 | Base de datos | Completo | Google Drive | SHA256-xxxx | Diego R. |

**9. Responsables**

* **Administrador de sistemas:** Diego Guerra – Ian Rodríguez. Responsables de la ejecución y monitoreo de respaldos.
* **Desarrolladores:** Diego Guerra. Encargados de mantener actualizado el código en GitHub.
* **Líder de proyecto:** Ian Rodríguez Valida la correcta aplicación del plan y coordina tareas de recuperación.