

**Centro de Enseñanza Técnica Industrial**

**Desarrollo de Software**

**Administración de la infraestructura y plataforma**

**Jesús Alberto Aréchiga Carrillo**

**22310439 6N**

**Profesor**

**José Francisco Pérez Reyes**

**Mayo 2025**

**Guadalajara, Jalisco**

## Objetivo

Establecer un proceso estructurado para realizar respaldos periódicos y recuperar datos de manera eficiente, garantizando la disponibilidad y continuidad del servicio ante fallos, errores humanos o incidentes de seguridad.

### Este procedimiento aplica a:

* Configuraciones personalizadas de usuarios (vínculo con dispositivos rutinas, automatizaciones).
* Tokens de autenticación (según marcas integradas).
* Base de datos de usuarios y preferencias.
* Backend/API (microservicios y configuración del sistema).
* Archivos de logs críticos (seguridad y errores).

|  |  |  |
| --- | --- | --- |
| Tipos de datos | Frecuencia | Tipo de respaldo |
| Base de datos de usuarios | Diario (00:00 hrs) | Completo |
| Configutraciones de dispositivos | Diario | Incremental |
| Backups de la app y servicios API | Semanal | Completo |
| Logs críticos | Diario | Incremental |

### Medio y Ubicación del Respaldo

* **Primario:** Almacenamiento cifrado en la nube (AWS S3 / Azure Blob Storage).
* **Secundario:** Almacenamiento local cifrado (servidor de respaldo interno).
* **Redundancia geográfica:** Copia duplicada en otra región de la nube.

### Seguridad en el respaldo

* Cifrado AES-256 en tránsito y en reposo.
* Acceso restringido mediante roles y autenticación multifactor (MFA).
* Registro de auditoría de cada operación de respaldo/restauración.
* Verificación de integridad del backup (hash SHA-256).

### Procedimiento de Recuperación

Recuperación Parcial (ej. usuario pierde su configuración)

1. Usuario solicita restauración desde la app.
2. Se accede al último respaldo disponible.
3. Se restauran configuraciones y tokens relacionados a su perfil.
4. Confirmación al usuario.

Recuperación Total (fallo del sistema o incidente mayor)

1. Se declara el incidente y se activa el plan de recuperación.
2. Se identifican respaldos más recientes no afectados. }
3. Se restauran bases de datos, configuraciones y servicios en entorno secundario.
4. Se valida la integridad del sistema.
5. Se reanuda el servicio (RTO objetivo: 1 hora / RPO objetivo: 24 horas).

### Pruebas y validaciones

* Prueba de restauración completa **mensual**.
* Restauraciones parciales de muestra **semanalmente**.
* Registro de tiempos de recuperación y revisión de errores.

### Registro y Documentación

Todos los respaldos y restauraciones deben registrarse con:

* + Fecha y hora
  + Tipo de datos respaldados/restaurados
  + Responsable
  + Resultado (éxito o falla)

### Herramientas

* **Base de datos:** PostgreSQL / MongoDB con pg\_dump o mongodump.
* **Automatización:** Cron Jobs, AWS Lambda o GitHub Actions.
* **Monitoreo:** Prometheus + Grafana / AWS CloudWatch / Sentry para errores.
* **Almacenamiento:** AWS S3 con políticas de ciclo de vida / Azure Vault.