# Fase 2: Documento de Diseño y Prototipado

Implantación de un Sistema de Virtualización y Copias de Seguridad en una Empresa Informática

| | | | |
|---|---|---|---|
| **Microproyecto:** | Organizar servicios TI con copias de seguridad automáticas y seguras | **Centro Educativo:** | IES Ana Luisa Benítez |
| **Ciclo / Curso:** | Sistemas Microinformáticos y Redes (SMR) - 2º Curso | **Caso de Referencia:** | Worten Canarias |
| **Fecha de Inicio:** | 01/05/2026 | **Fecha de Fin:** | 07/06/2026 |

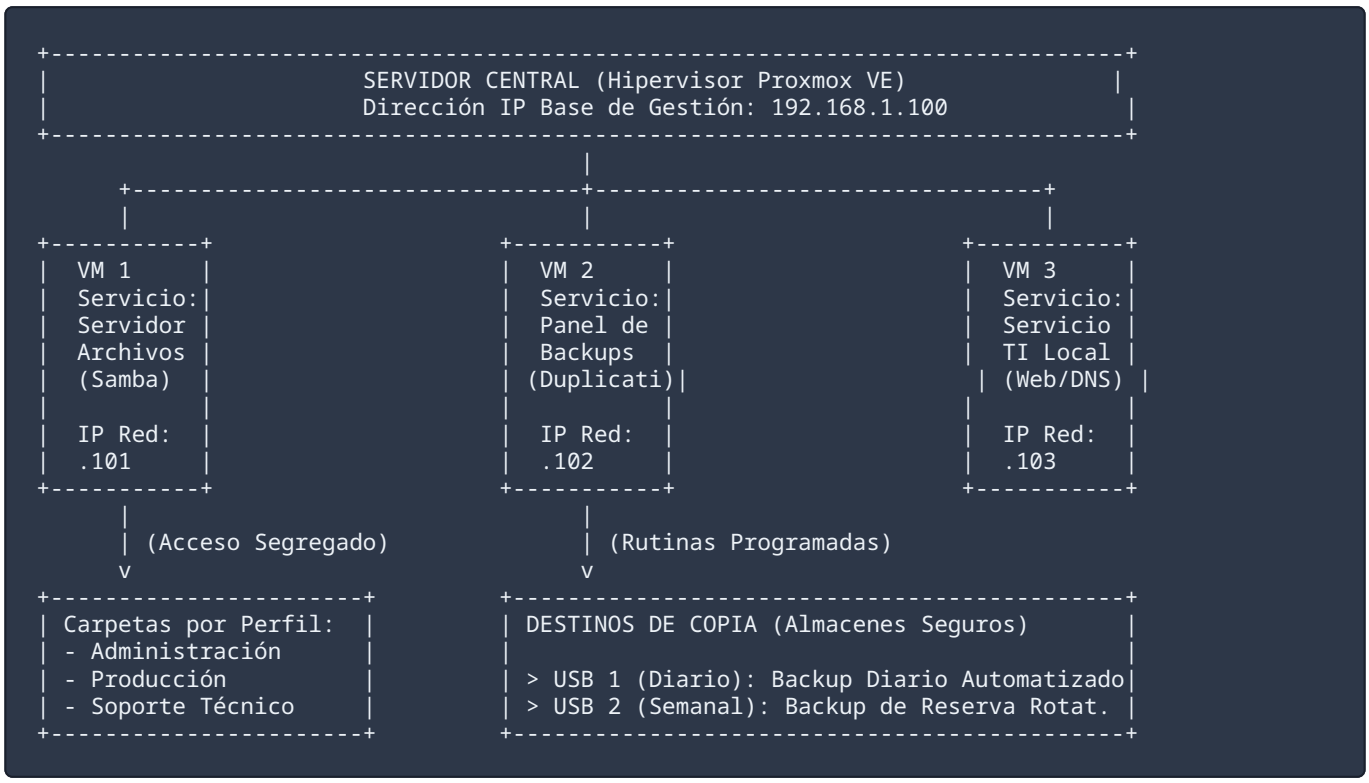
## 1. Justificación y Planteamiento de la Solución

Tras evaluar las brechas detectadas en la infraestructura informática de la empresa de referencia, caracterizada por la preocupante dispersión de servicios esenciales y datos en múltiples equipos de forma independiente, se ha diseñado una infraestructura centralizada y segura. La falta de consistencia actual eleva sustancialmente el riesgo ante incidentes de hardware, ataques de malware o borrados fortuitos.

Para solventar esta situación de forma definitiva, se plantea la creación de un prototipo técnico que unifique los servicios críticos sobre un entorno controlado que asegure la continuidad de las operaciones del personal administrativo, técnico y de producción mediante copias de seguridad programadas.

## 2. Diseño Lógico de la Arquitectura de Red

La solución se estructura mediante la consolidación de la infraestructura física del aula de SMR usando virtualización moderna. A continuación, se expone el esquema conceptual del entorno planteado:




# 3. Especificaciones del Prototipo Técnico

## 3.1. Dimensionamiento del Entorno Virtualizado

Se despliega un nodo central de virtualización con Proxmox VE que aloja tres máquinas virtuales (VMs) diferenciadas e independientes, dando pleno cumplimiento a los requerimientos técnicos fijados en los objetivos generales de la guía docente:

- **VM 1 (Servidor de Archivos Compartidos):** Basado en una distribución Linux estable con el servicio Samba activo. Su función principal consiste en centralizar la documentación de las áreas críticas del negocio.
- **VM 2 (Servidor de Backups):** Nodo orquestador encargado de las automatizaciones y auditorías del estado de las copias.
- **VM 3 (Servidor de Servicios Auxiliares de Red):** Instancia adicional configurada para balancear la carga de infraestructura de red interna (servicio web/intranet o resolución de nombres local).

## 3.2. Estructura de Directorios y Control de Accesos

Para solventar el problema de archivos desperdigados en escritorios individuales, la VM 1 cuenta con restricciones basadas en perfiles específicos con accesos autenticados obligatorios:

- `/srv/smb/administracion`: Permisos exclusivos para el personal de contabilidad y administración.
- `/srv/smb/produccion`: Acceso restringido para el desarrollo técnico de proyectos.
- `/srv/smb/soporte`: Directorio asignado al equipo técnico y soporte al cliente.

## 4. Estrategia y Planificación de Copias de Seguridad

La política operativa de salvaguarda de información se articula bajo un esquema dual que balancea automatización y almacenamiento offline seguro:

| Tipo de Copia | Frecuencia | Destino Físico | Objetivo / Retención |
|---|---|---|---|
| **Automatizada Diaria** | Cada noche de forma desasistida | Unidad USB Externa 1 (`USB_DIARIO`) conectada permanentemente al nodo central. | Histórico incremental de 7 días. Garantiza recuperación operativa rápida. Registro de estado diario. |
| **Automatizada Semanal** | Cada viernes al cierre de jornada | Unidad USB de Reserva 2 (`USB_SEMANAL`) con intercambio físico manual. | Copia completa del entorno. Resguardo fuera de línea en el armario de seguridad / secretaría del centro. |

### 4.1. Medidas de Seguridad Mínimas Obligatorias

1. **Separación de Cuentas:** Las credenciales de administración del hipervisor y servidores son totalmente ajenas a las credenciales de uso diario.
2. **Fortaleza de Accesos:** Uso de políticas de contraseñas robustas complejas para todos los perfiles de usuario de red.
3. **Registro Activo:** Activación sistemática del log del sistema de copias para auditoría de incidencias.

## 5. Guía de Operación y Plan de Contingencia en 4 Pasos

Para asegurar un correcto desempeño de la solución, el personal operativo de la empresa seguirá la siguiente secuencia metodológica:

1. **Almacenamiento Centralizado:** Almacenar cualquier archivo de trabajo obligatoriamente dentro del recurso compartido de red asignado según su perfil, evitando el uso del almacenamiento del equipo de sobremesa local.
2. **Verificación Diaria:** Al iniciar el turno de trabajo diario, el operador responsable inspeccionará el registro del panel central de backups para verificar el estado de la tarea nocturna (**OK** / **ERROR**).
3. **Acción ante Fallos (Contingencia):** Si el log reporta un estado de **ERROR**, se procederá a pulsar el botón o script de **"Copia Manual"** y se notificará por canal urgente al administrador TI del centro.
4. **Rotación Semanal:** Al finalizar la última jornada lectiva de la semana, se desconectará el dispositivo USB de copias semanales y se sustituirá por la unidad de reserva, archivando el disco saliente de forma física en el armario protegido.

## 6. Métricas de Control y Criterios de Aceptación (KPIs)

**KPI de Continuidad Operativa:** Demostración de restauración completa verificada ante desastres. La infraestructura debe restaurar una VM caída o un lote completo de archivos en **menos de 30 minutos** (y menos de 15 minutos en tareas de archivos planos).

**KPI de Fiabilidad del Backup:** En un ciclo de monitorización continua de 10 días lectivos, las copias automatizadas diarias deben certificar un umbral mínimo del **95% de estados correctos ("OK")** en los registros del servidor.

**KPI de Eficiencia Energética (ODS 12):** Centralización de servicios en un único hardware con apagado automático en periodos de inactividad, proyectando una reducción del **20% en el consumo energético (kWh)** frente a servidores físicos dispersos.