

INTERCONEXIÓN SEGURA ENTRE DOS SEDES

VPN Site-to-Site (IPsec)

Sede Central (60 puestos) ⇄ Sucursal Remota — túnel cifrado IKEv2 / AES-256-GCM

Objetivos del Proyecto

Que ambas sedes operen como una única red corporativa lógica, cifrada y controlada.

1

Routers/firewalls de cabecera

Un equipo UTM con soporte VPN IPsec en cada sede.

2

Túnel IPsec Site-to-Site

IKEv2, AES-256-GCM, con reconexión automática.

3

Direccionamiento sin solapes

Subredes disjuntas entre sede central y sucursal.

4

Reglas de seguridad en whitelist

Solo el tráfico necesario cruza entre sedes.

Antecedentes y Situación Actual

Situación de partida

- La sucursal opera aislada de la sede central
- Accesos puntuales no cifrados / expuestos a Internet
- Necesidad de acceso a ficheros, ERP e impresión en red
- Sin política homogénea de direccionamiento IP
- Sin reglas de acceso controladas entre sedes

2

sedes a interconectar

100%

del tráfico entre sedes, cifrado

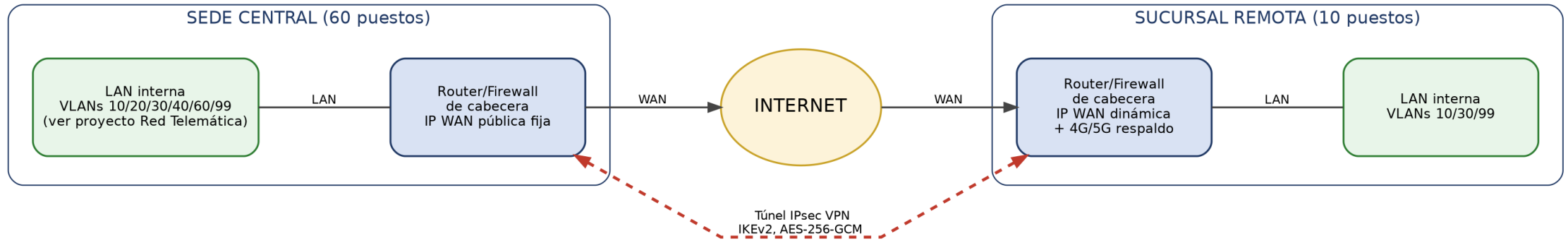
8

semanas de despliegue

Solución Técnica

- Fase 1 (IKE): IKEv2, AES-256, SHA-256, grupo DH 14+
- Fase 2 (IPsec/ESP): AES-256-GCM, PFS, modo túnel
- Dead Peer Detection (DPD) y reconexión automática
- Línea de respaldo 4G/5G en la sucursal con conmutación automática
- Reglas de firewall en whitelist (deny-by-default)

Topología de la Interconexión



- Sede central: IP WAN pública fija · Sucursal: IP WAN dinámica + respaldo 4G/5G
- Túnel IPsec Site-to-Site entre ambos routers/firewalls de cabecera, sobre Internet
- Cada sede conserva su LAN interna y sus propias VLANs de gestión local

Direccionamiento IP

Sede	Subred	¿Cruza el túnel?
Sede Central — Datos (VLAN 10)	10.10.10.0/24	Sí
Sede Central — Servidores (VLAN 60)	10.10.60.0/24	Sí
Sucursal — Datos (VLAN 10)	10.20.10.0/24	Sí
Sucursal — Wi-Fi Corp (VLAN 30)	10.20.30.0/24	Sí

Únicamente Datos y Servidores de la sede central, y Datos y Wi-Fi Corp de la sucursal, cruzan el túnel (mínimo privilegio).

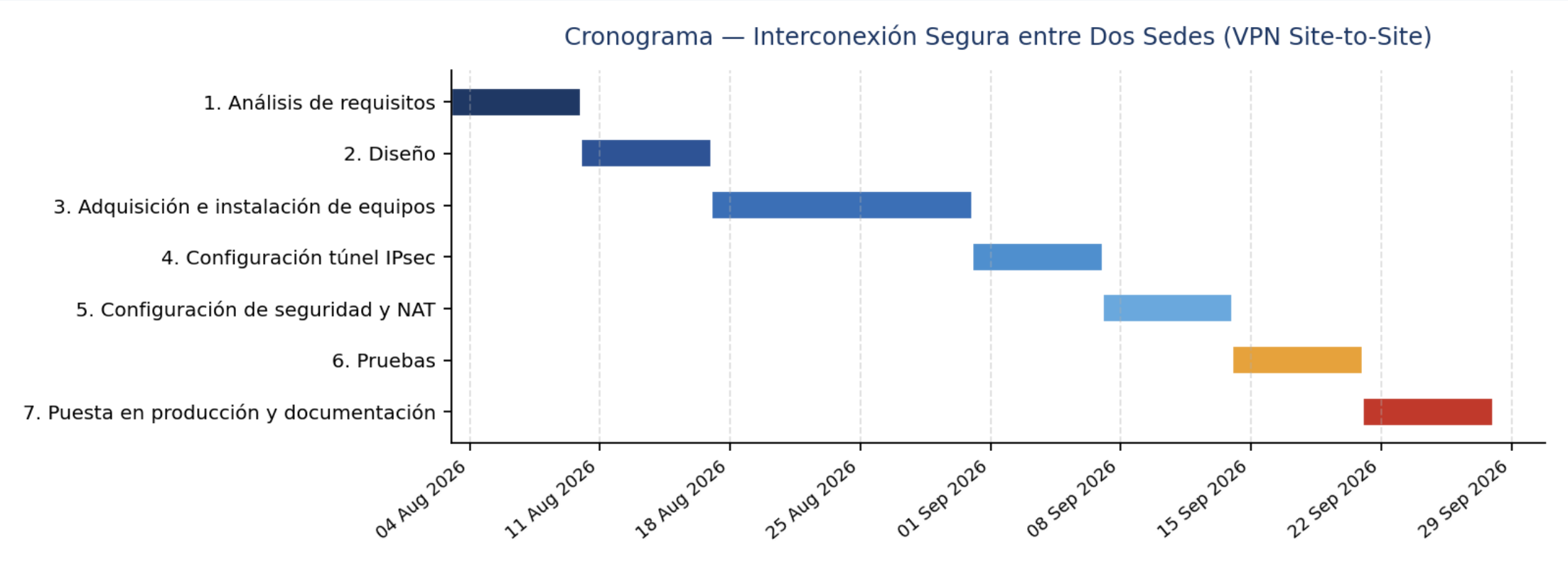
Reglas de Firewall (Whitelist)

Política de denegación por defecto: solo se permite explícitamente el tráfico de la tabla.

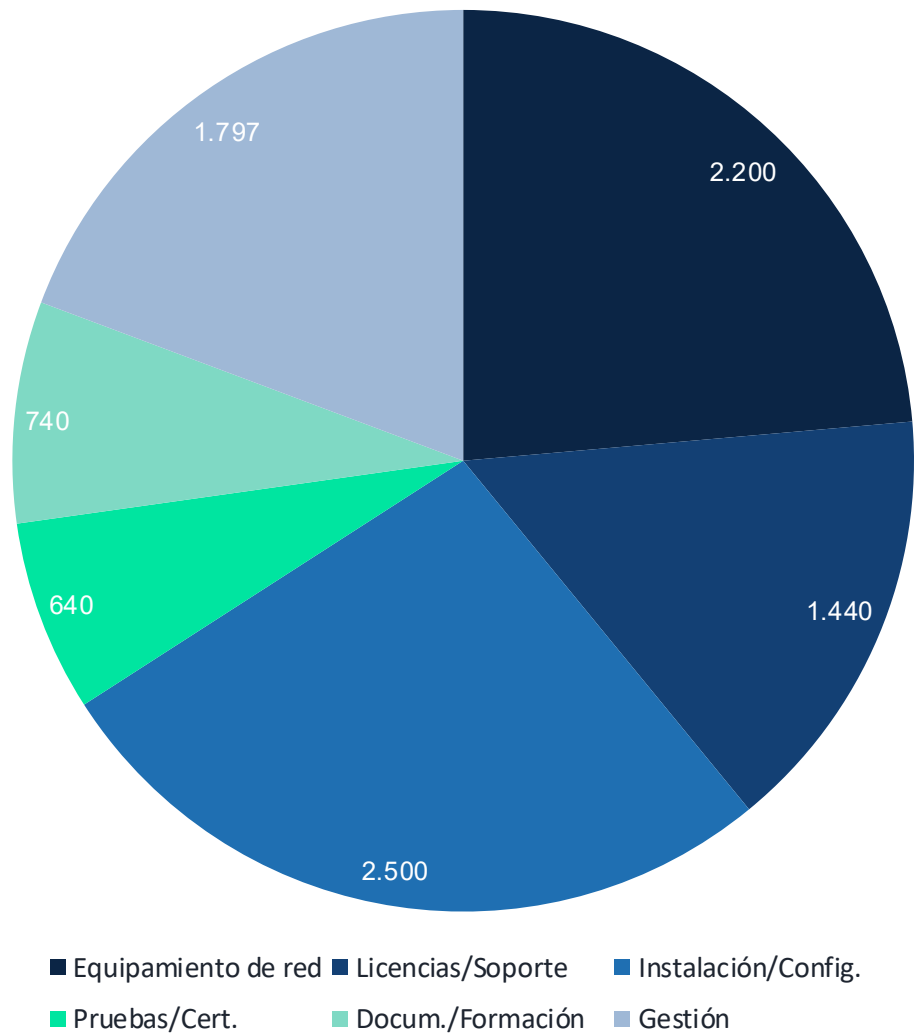
Origen	Destino	Servicio	Acción
Datos-Sucursal	Servidores (Central)	SMB / BD ERP	Permitir
Datos-Sucursal	Datos (Central)	HTTP/HTTPS	Permitir
WiFi-Corp-Sucursal	Servidores (Central)	HTTPS (ERP web)	Permitir
Cualquiera	Cualquiera	Resto de tráfico	Denegar

Cronograma del Proyecto

8 semanas — del 3 de agosto al 28 de septiembre de 2026



Presupuesto



9.317 €

Total sin IVA · 11.273,57 € con IVA

No incluye el coste recurrente de las líneas de Internet (principal ni de respaldo 4G/5G).

Gestión de Riesgos

Alto

Caída de línea de Internet

Línea de respaldo 4G/5G con conmutación automática

Alto

Reglas de firewall mal configuradas

Diseño en whitelist + revisión por segunda persona

Alto

Intentos de intrusión sobre el túnel

Autenticación robusta, límite de intentos y monitorización

Medio

Solapamiento de rangos IP

Verificación del esquema de direccionamiento antes de implementar

Una red corporativa, dos sedes, un solo perímetro de seguridad

Conectividad cifrada, controlada y resiliente entre la sede central y la sucursal remota, a una fracción del coste de una línea dedicada.