

MEMORIA TÉCNICA

Interconexión Segura entre Dos Sedes VPN Site-to-Site (IPsec)

Proyecto: Interconexión Segura entre Dos Sedes (VPN Site-to-Site)
Sedes: Central (60 puestos) — Sucursal Remota · Fecha: Agosto 2026 · Versión: 1.1
Elaborado por: Enrique Calabozo Orea – Administrador de Sistemas TIC / Project Manager

ÍNDICE

1. Introducción
2. Objetivos del Proyecto
3. Antecedentes y Situación Actual
4. Descripción General del Proyecto
5. Solución Técnica Propuesta
6. Especificaciones Técnicas
7. Plan de Ejecución y Cronograma
8. Presupuesto Estimado
9. Gestión de Riesgos
10. Plan de Calidad y Pruebas
11. Documentación Para Entregar
12. Conclusiones
13. Anexos

1. Introducción

El presente documento constituye la Memoria Técnica del proyecto de interconexión segura entre la sede central de la organización (60 puestos de trabajo, ver proyecto de Implantación de Red Telemática) y una sucursal o tienda remota, mediante una VPN Site-to-Site basada en IPsec sobre Internet.

El objetivo principal es que ambas sedes operen como una única red corporativa lógica, con comunicación cifrada y autenticada entre ellas, sin necesidad de contratar una línea privada dedicada (MPLS o punto a punto), reduciendo costes de conectividad sin renunciar a la seguridad.

2. Objetivos del Proyecto

Objetivo General: Establecer una interconexión cifrada y estable entre la sede central y la sucursal remota mediante VPN IPsec Site-to-Site, con enlace de respaldo 4G/5G en la sucursal.

Objetivos Específicos:

- Desplegar firewalls/UTM de cabecera en ambas sedes con capacidad VPN IPsec.
- Configurar túnel IKEv2 con AES-256-GCM, PFS y DPD según el Anexo 5.
- Integrar el direccionamiento de la sucursal (10.20.x.0/24) con el de la sede central (10.10.x.0/24) sin solapes.
- Implementar y validar el failover automático a la línea 4G/5G de la sucursal.
- Aplicar reglas de firewall de mínimo privilegio entre las redes de interés del túnel.
- Superar las pruebas de aceptación formales (Anexo 9) y formalizar la recepción (Anexo 10).

3. Antecedentes y Situación Actual

- La sede central dispone de red telemática segmentada (proyecto de 60 puestos) con VLANs y direccionamiento 10.10.x.0/24.
- La sucursal remota no tiene interconexión segura con la central; el acceso a recursos corporativos es limitado o inexistente.
- No se dispone de línea privada (MPLS); se aprovecha Internet existente en ambas sedes para el túnel IPsec.

4. Descripción General del Proyecto

El proyecto contempla:

- Suministro e instalación de 2 firewalls/UTM de cabecera (uno por sede).
- Configuración del túnel IPsec Site-to-Site (IKEv2, AES-256-GCM, PFS).
- Módem/router 4G/5G de respaldo en la sucursal con failover automático.
- Switch de acceso en la sucursal y alineación de direccionamiento (Anexo 1).
- Reglas de firewall, NAT (si aplica) y documentación de operación.
- Pruebas de aceptación (Anexo 9) y Acta de recepción (Anexo 10).

5. Solución Técnica Propuesta

- Arquitectura: Túnel IPsec modo túnel entre los UTM de ambas sedes sobre Internet (ver Anexo 8).
- Cifrado: IKEv2, AES-256 (Fase 1), AES-256-GCM (Fase 2), PFS Grupo 14, DPD habilitado.
- Redes de interés: 10.10.10.0/24 y 10.10.60.0/24 (central) ↔ 10.20.10.0/24 y 10.20.30.0/24 (sucursal).

- Respaldo: Enlace 4G/5G en sucursal con conmutación automática ante caída de la WAN principal.
- Seguridad: Reglas de mínimo privilegio; sin exposición del endpoint VPN a Internet más allá de IKE/IPsec.

6. Especificaciones Técnicas

- Protocolo: IPsec ESP modo túnel. IKE: versión 2. Cifrado: AES-256 / AES-256-GCM. Hash: SHA-256.
- Grupo DH: 14 (2048 bits) mínimo. Lifetime Fase 1: 8 h. Lifetime Fase 2: 1 h. PFS: habilitado.
- DPD: intervalo 10 s, 3 reintentos. Autenticación: PSK $\geq$ 20 caracteres o certificados digitales.
- Garantía equipos: 3 años (UTM), 2 años (módem 4G/5G). Licencias UTM/VPN: 1 año renovable.

7. Plan de Ejecución y Cronograma

(Anexo 3 — duración estimada: 8 semanas, agosto-septiembre 2026).

- Fase 1 — Análisis de requisitos (1 sem).
- Fase 2 — Diseño de direccionamiento y perfiles IPsec (1 sem).
- Fase 3 — Adquisición e instalación de equipos (2 sem).
- Fase 4 — Configuración del túnel IPsec (1 sem).
- Fase 5 — Configuración de seguridad, NAT y failover 4G (1 sem).
- Fase 6 — Pruebas de aceptación UAT (Anexo 9) (1 sem).
- Fase 7 — Puesta en producción, documentación y Acta de Recepción (Anexo 10) (1 sem).

8. Presupuesto Estimado

Se adjunta desglose detallado en el Anexo 2 — Presupuesto Detallado. Incluye 2x UTM, módem 4G/5G, switch, licencias, instalación, configuración y gestión de proyecto.

9. Gestión de Riesgos

Se detalla en el Anexo 4 — Matriz de Riesgos (versión 1.1). Riesgos principales: retraso de equipos (R-01), disponibilidad de la línea de Internet en sucursal (R-02) y fallo del failover 4G (R-04).

10. Plan de Calidad y Pruebas

El plan de pruebas se formaliza en el Anexo 9 — Plan de Pruebas de Aceptación (UAT), con 14 casos cuantificados (P-V01 a P-V14):

- Establecimiento y estabilidad del túnel: UP, rekey, DPD $\leq$ 30 s, estabilidad 24 h.
- Conectividad y rendimiento: ping entre redes, throughput cifrado $\geq$ 70 % de la línea, acceso a servidores.
- Seguridad: reglas de mínimo privilegio, rechazo de conexiones no autorizadas, tráfico cifrado.
- Failover 4G/5G: conmutación $\leq$ 60 s, fallback y rendimiento documentado sobre móvil.

Se requiere el 100 % de casos críticos en PASS para la recepción provisional (Anexo 10).

11. Documentación a Entregar

- Esquema de direccionamiento IP (Anexo 1).
- Presupuesto detallado (Anexo 2).
- Cronograma (Anexo 3).
- Matriz de riesgos (Anexo 4).
- Configuración IPsec y reglas de firewall (Anexo 5).
- Manual de operación y mantenimiento (Anexo 6).
- Inventario detallado de equipos (Anexo 7).
- Diagrama de arquitectura (Anexo 8).
- Plan de pruebas de aceptación cumplimentado (Anexo 9).
- Acta de recepción provisional firmada (Anexo 10).

12. Conclusiones

La interconexión VPN Site-to-Site permitirá a la organización operar la sede central y la sucursal como una única red corporativa lógica, con comunicación cifrada, reglas de seguridad controladas y un enlace de respaldo 4G/5G que minimiza el impacto de caídas de la línea principal. El proyecto se alinea con el direccionamiento y la segmentación de la Red Telemática de la sede central (60 puestos).

13. Anexos

- Anexo 1: Direccionamiento IP / VPN
- Anexo 2: Presupuesto detallado
- Anexo 3: Cronograma
- Anexo 4: Matriz de riesgos
- Anexo 5: Configuración IPsec y reglas de firewall
- Anexo 6: Manual de operación y mantenimiento
- Anexo 7: Inventario detallado de equipos

- Anexo 8: Diagrama de arquitectura
- Anexo 9: Plan de pruebas de aceptación (UAT)
- Anexo 10: Acta de recepción provisional

Versión 1.1 — Anexos numerados de forma correlativa (1-10). Incluye Arquitectura (8), UAT (9) y Acta (10). Alineada con el proyecto de Red Telemática (60 puestos).