ANEXO 9

Plan de Pruebas de Aceptación (UAT) — VPN Site-to-Site

Proyecto: Interconexión Segura entre Dos Sedes (VPN Site-to-Site)
Fecha: Agosto 2026 · Versión: 1.0
Elaborado por: Enrique Calabozo Orea – Administrador de Sistemas TIC / Project Manager

Casos de prueba y criterios de aceptación cuantificados que deben superarse antes de la recepción provisional del túnel VPN. Cada caso se registra con resultado y evidencia. Coherente con el apartado 10 de la Memoria Técnica.

1. Establecimiento y estabilidad del túnel

ID	Prueba	Procedimiento	Criterio de aceptación	Resultado
P-V01	Establecimiento del túnel IPsec	Verificar que el túnel IKEv2 se establece correctamente entre ambos peers tras el arranque.	Túnel UP en ambos extremos; SA de Fase 1 y Fase 2 activas; sin errores en logs	[Pendiente]
P-V02	Rekey / lifetime	Forzar o esperar la renegociación de SA según lifetime configurado (Fase 1 y Fase 2).	Rekey exitoso sin caída del túnel; tráfico interrumpido < 2 s	[Pendiente]
P-V03	Dead Peer Detection (DPD)	Simular caída del peer (apagar interfaz WAN remota) y verificar detección por DPD.	DPD detecta la caída en ≤ 30 s; túnel marcado DOWN; al recuperar, se restablece automáticamente	[Pendiente]
P-V04	Estabilidad 24 h	Mantener el túnel activo durante al menos 24 h con tráfico de prueba periódico.	Sin caídas no planificadas; logs sin errores críticos de IKE/IPsec	[Pendiente]

2. Conectividad y rendimiento

ID	Prueba	Procedimiento	Criterio de aceptación	Resultado
P-V05	Ping entre redes de interés	Hacer ping desde host en 10.10.10.0/24 hacia host en 10.20.10.0/24 y viceversa.	Respuesta OK; pérdida de paquetes < 0,5 %; RTT medio < 80 ms (línea fija)	[Pendiente]
P-V06	Throughput cifrado	Medir throughput TCP/UDP a través del túnel (iperf o similar) en ambas direcciones.	≥ 70 % de la capacidad nominal de la línea más lenta (p. ej. ≥ 70 Mbps si línea 100 Mbps)	[Pendiente]
P-V07	Acceso a servidores centrales	Desde la sucursal, acceder a recursos en 10.10.60.0/24 (file server, intranet, etc.).	Acceso correcto según reglas de firewall; latencia aceptable para aplicaciones de negocio	[Pendiente]
P-V08	Split-tunnel / política de enrutamiento	Verificar que el tráfico a Internet de cada sede sale por su WAN local (si aplica split-tunnel).	Tráfico Internet no atraviesa el túnel; solo redes de interés usan el IPsec	[Pendiente]

3. Seguridad y firewall

ID	Prueba	Procedimiento	Criterio de aceptación	Resultado
P-V09	Reglas de mínimo privilegio	Intentar tráfico no autorizado entre redes (p. ej. desde sucursal a segmento no permitido).	Tráfico bloqueado por firewall; evento registrado en logs	[Pendiente]
P-V10	Sin acceso desde Internet al túnel	Desde Internet, intentar conexión al endpoint VPN con parámetros incorrectos o sin autenticación.	Conexión rechazada; no se establece SA; intentos registrados	[Pendiente]
P-V11	Integridad de cifrado	Verificar con captura (si es viable en lab) o con herramientas del fabricante que el tráfico del túnel va cifrado.	Tráfico entre peers aparece cifrado (ESP); no se observa payload en claro	[Pendiente]

4. Failover y respaldo 4G/5G

ID	Prueba	Procedimiento	Criterio de aceptación	Resultado
P-V12	Conmutación a 4G/5G	Simular caída de la WAN principal de la sucursal y verificar conmutación al módem 4G/5G.	Failover en ≤ 60 s; túnel se restablece por la ruta 4G/5G; conectividad recuperada	[Pendiente]
P-V13	Retorno a WAN principal	Restaurar la WAN principal y verificar failback al enlace preferente.	Failback automático o controlado; túnel estable de nuevo sobre la línea fija	[Pendiente]
P-V14	Rendimiento por 4G/5G	Medir latencia y throughput del túnel cuando opera sobre el enlace 4G/5G.	Conectividad funcional; latencia y throughput documentados (pueden ser inferiores a la línea fija)	[Pendiente]

5. Notas de ejecución

- Las pruebas de failover (P-V12, P-V13) requieren coordinación para no afectar usuarios en producción si se hacen en horario laboral.
- Se requiere que el 100 % de los casos críticos (P-V01 a P-V13) resulten PASS para la recepción provisional (Anexo 10).
- Evidencias: capturas de estado del túnel, resultados de ping/iperf, logs de firewall y fotografías se adjuntan a este plan.