Diseño de red de una organización Sanitaria

Máster Universitario en Ingeniería de Telecomunicación
Especialidad Telemática

Autor: Ignacio Campos Marcé
Consultor: José López Vicario

Índice

Contexto y justificación

Organización Ox: Organización sanitaria que está compuesta por los centros sanitarios de la Comunidad Autónoma.

- 1292 centros.
- <36.600 profesionales sanitarios
- Gran volumen de datos
- Datos críticos
- Diferentes tipológicas de centros.

Red Xenon: Red que interconecta todas las sedes que componen la Organización Ox.

- Enlaza centros Sanitarios, organizaciones gubernamentales y empresas externas.
- Red vulnerable y expuesta.
- Falta de monitorización que dificulta la gestión.
- Sobredimensionamiento de recursos.
- No hay diseño definido por falta de tiempo.

Contexto y justificación

Características:

Deficiencias:

Diseño centrado en:

- Optimizar el uso de recursos.
- Administración
- Seguridad
- Escalable tipologías de centros
- Que mejore trazabilidad

Objetivos y requisitos

Objetivo principal: Análisis y diseño de un modelo de red de una organización de índole sanitario.

Objetivos específicos

- Comprender lógica negocio
- Analizar riesgos de la red
- Definir diseño de red según tipología de centros
- Mejorar administración red.
- Aumentar visibilidad de red
- Implementar medidas de seguridad

Requisitos

- Gestión óptima ancho banda
- Modelo para monitorización del tráfico
- Diseño claro y comprensible
- Segmentar tráfico corporativo del no corporativo
- Modelo base para resto centros
- Aprovechar máximo equipamiento
- Extender red Wifi a ciudadano
- Facilitar e-working

Clasificación sedes

- Clasificación sedes según número usuarios

Tipo Sede	Descripción	Localización	Numero
Tipo I	Principal y backup acceso de 10 Gbps fibra óptica	Hospitales de referencia, Centro de Informática (Sede central)	24
Tipo II	Principal de 1 Gbps fibra óptica, Backup acceso mediante ADSL	Hospitales y Centros de Especialidades. Centros de Salud y Centros administrativos. >20 usuarios	582
Tipo III	Principal de 1 Gbps fibra óptica, Backup acceso mediante ADSL	Centros de Salud y Centros administrativos. <20 usuarios	686

- Comunicación y relación entre nodos y sedes:
  - Nodo Troncal + Provincial = Tipo I
  - Nodo Enlace = Tipo II
  - Nodos de acceso (NA) =Tipo III

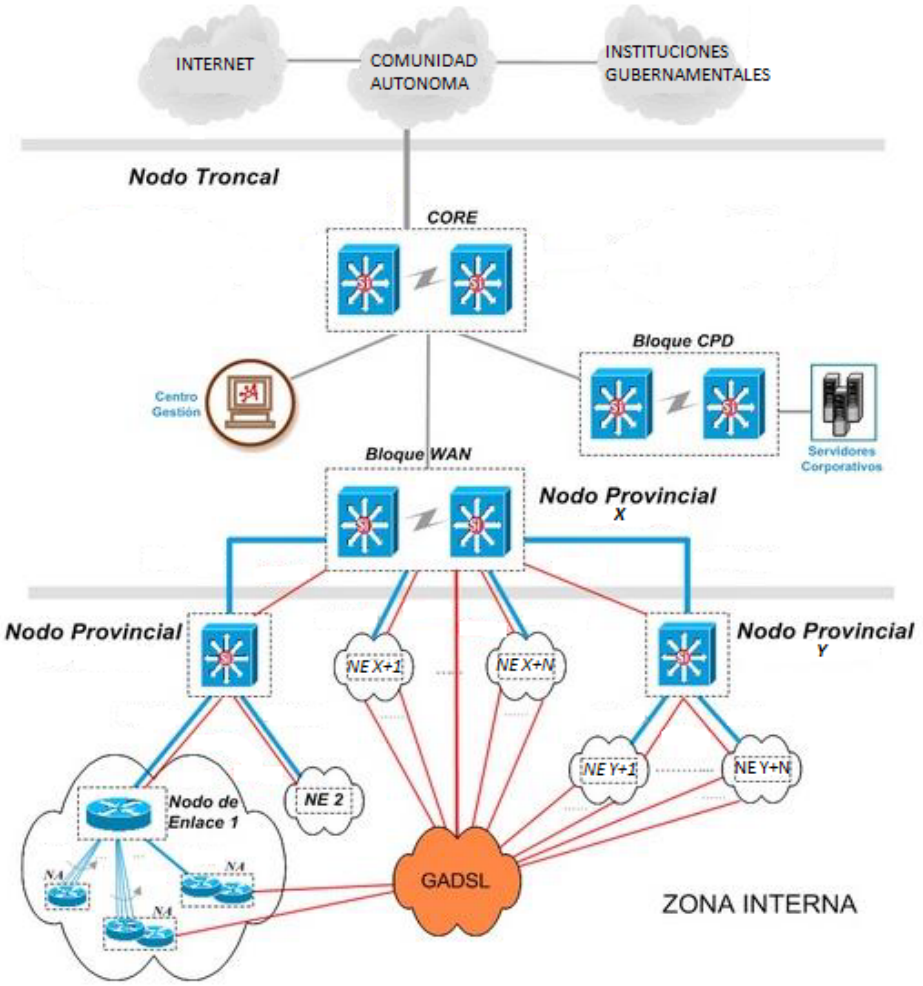
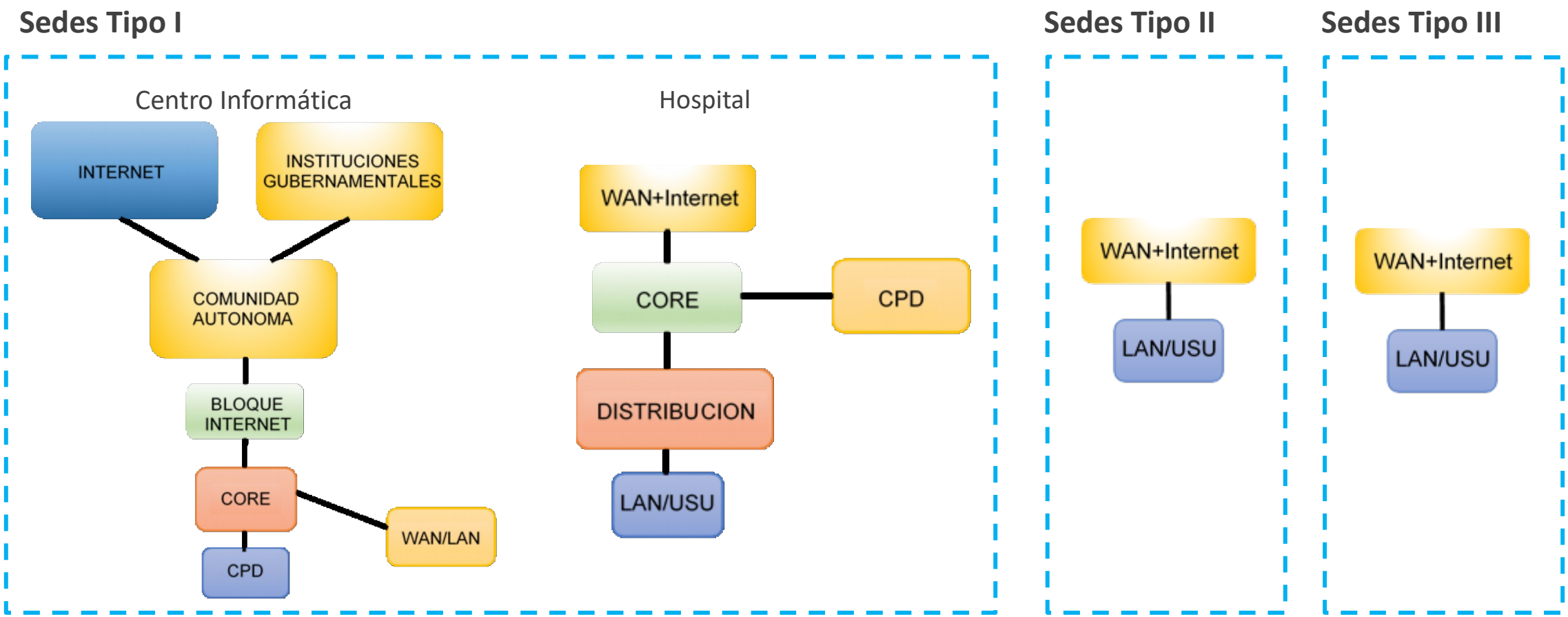


Diagrama bloques actual



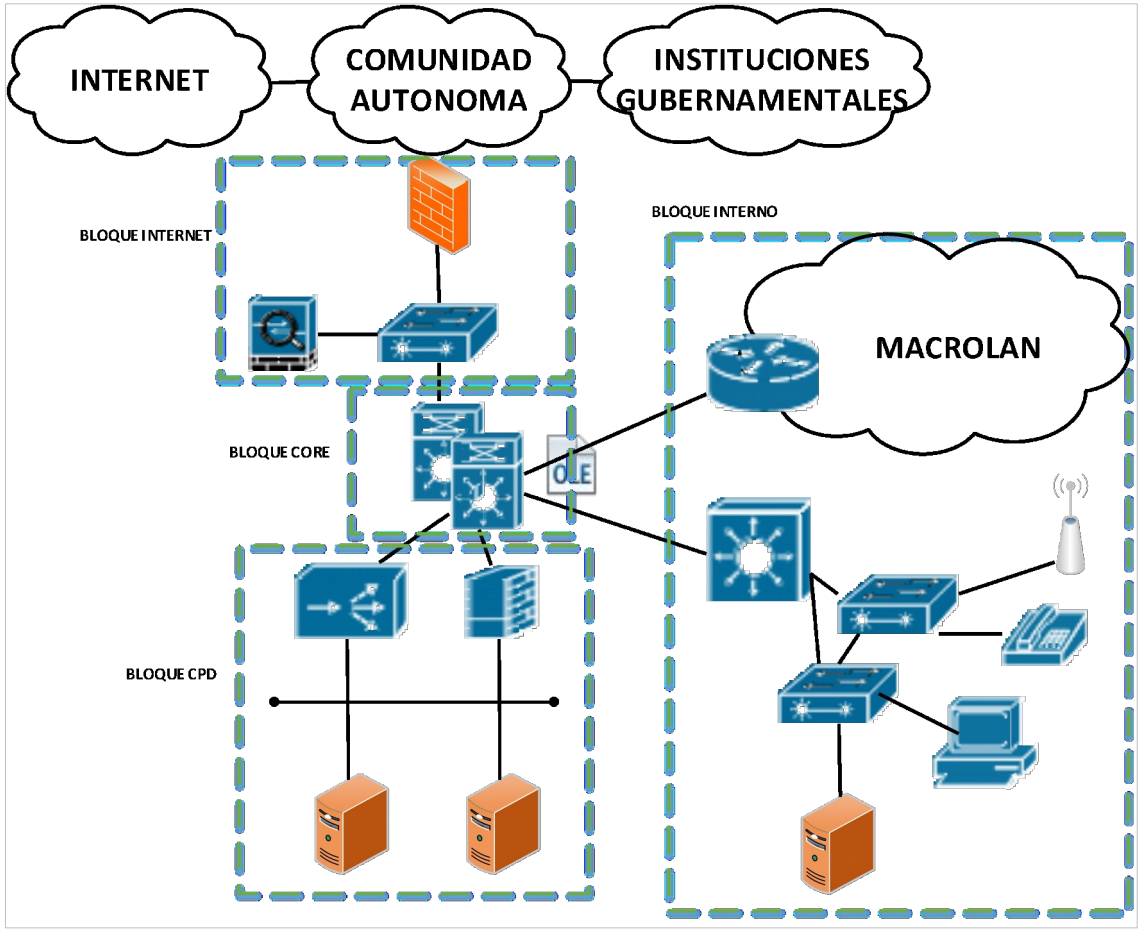
Análisis – Tipo I

Características Centro Informática:

- **Separación bloques:** Internet, Core, CPD, Interno.
- **Peculiaridades:** Accesos remotos, Publicación servicios a ciudadano y a profesionales, Proxy, NAC, LDAP.
- **Equipamiento:** Firewalls 2 fabricantes, Balanceadores, Proxy, DNS, Wifi, Concentrador y múltiples herramientas monitorización.

Riesgos Centro Informática:

- Mismo tratamiento tráfico corporativo del no corporativo
- Falta protección de servicios públicos
- Proxy cuello de botella
- Falta de seguridad en accesos internos y remotos
- No hay segmentación ni de entornos ni de usuarios
- Desaprovechamiento recursos firewalls y balanceadores.
- Falta monitorización.



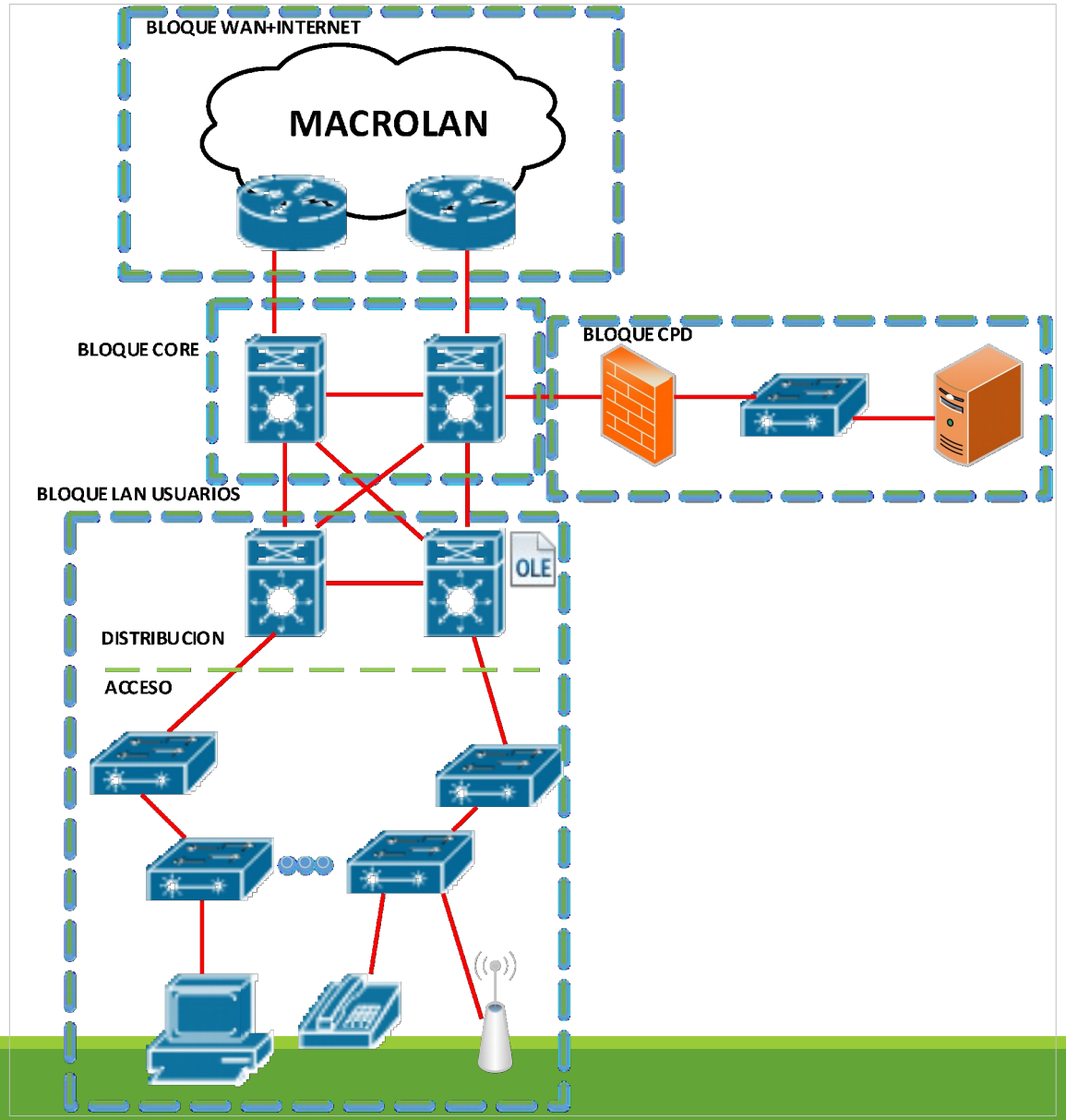
Análisis – Tipo I

Características Hospitales:

- **Separación bloques:** WAN/Internet, Core, CPD, Usuarios.
- **Peculiaridades:** Arquitectura 3 capas, MacroLan administrada por proveedor, Firewalls en CPD.
- **Equipamiento:** Firewalls 2 fabricantes, switches, Wifi.

Riesgos Hospitales:

- Falta protección perimetral.
- No hay segmentación de entornos
- Visión nula bloque usuarios
- No hay diseño definido
- Falta de granularidad en roles de usuarios
- Red expuesta
- Desaprovechamiento recursos firewalls y balanceadores



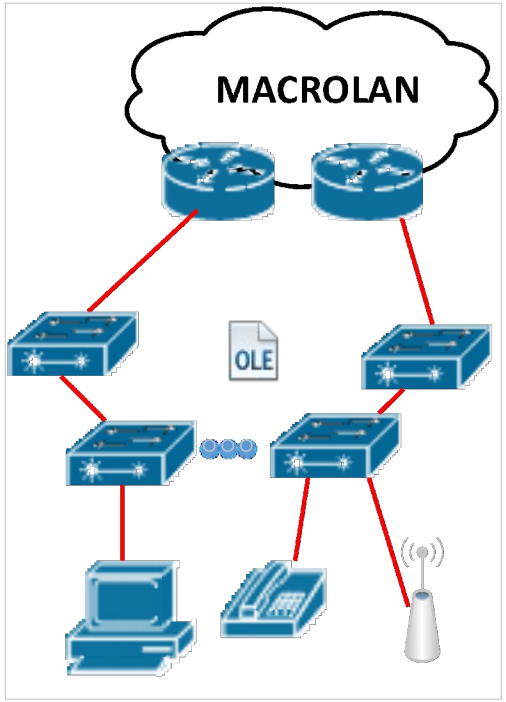
Análisis Tipo II y Tipo III

Características Sedes:

- **Separación bloques:** WAN/Internet y Usuarios.
- **Peculiaridades:** Core compacto, N3 en router, MacroLan administrada por proveedor.
- **Equipamiento:** Switches, Wifi.

Riesgos Hospitales:

- Falta protección perimetral
- Visión nula bloque usuarios
- No hay diseño definido
- Falta de granularidad en roles de usuarios
- Red expuesta



Análisis - Resultados

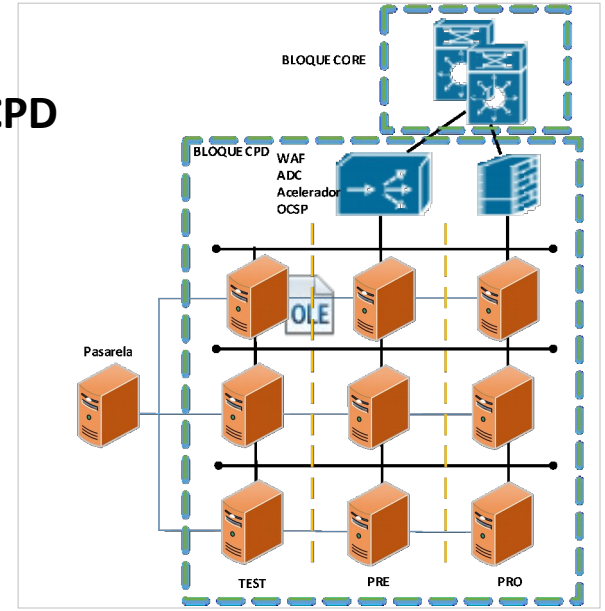
	Métricas	Valoración métricas	Valoración objetivos
O1	M1.a. ¿Qué nivel de mejora existe en la gestión del tráfico?	70%	N.A.
	M1.b. ¿En qué medida se respeta la criticidad de los servicios?.	20%	
O2	M2.a. ¿Cuántos riesgos se han identificado?	N.A.	N.A.
	M2.b. ¿Qué estimación de riesgos se han identificado?	N.A.	
	M2.c. ¿El diseño cubre todos los riesgos identificados?	N.A.	
O3	M3.a. ¿Cuántos diseños es encuentran implementados?	2	N.A.
	M3.b. ¿Se han respetado las buenas prácticas de diseño?	NO	
	M3.c. ¿En qué grado se ajusta el diseño a la tipología de centro?	30%	
O4	M4.a. ¿Qué nivel de mejora se estima que existe en la administración de la red?	80%	N.A.
	M4.b. ¿Qué número de incidencias mensuales se estima que existe a consecuencia del diseño?	210	
	M4.c ¿En cuánto se estima el tiempo de respuesta ante peticiones, cambios e incidencias prioritarias?	30 min	

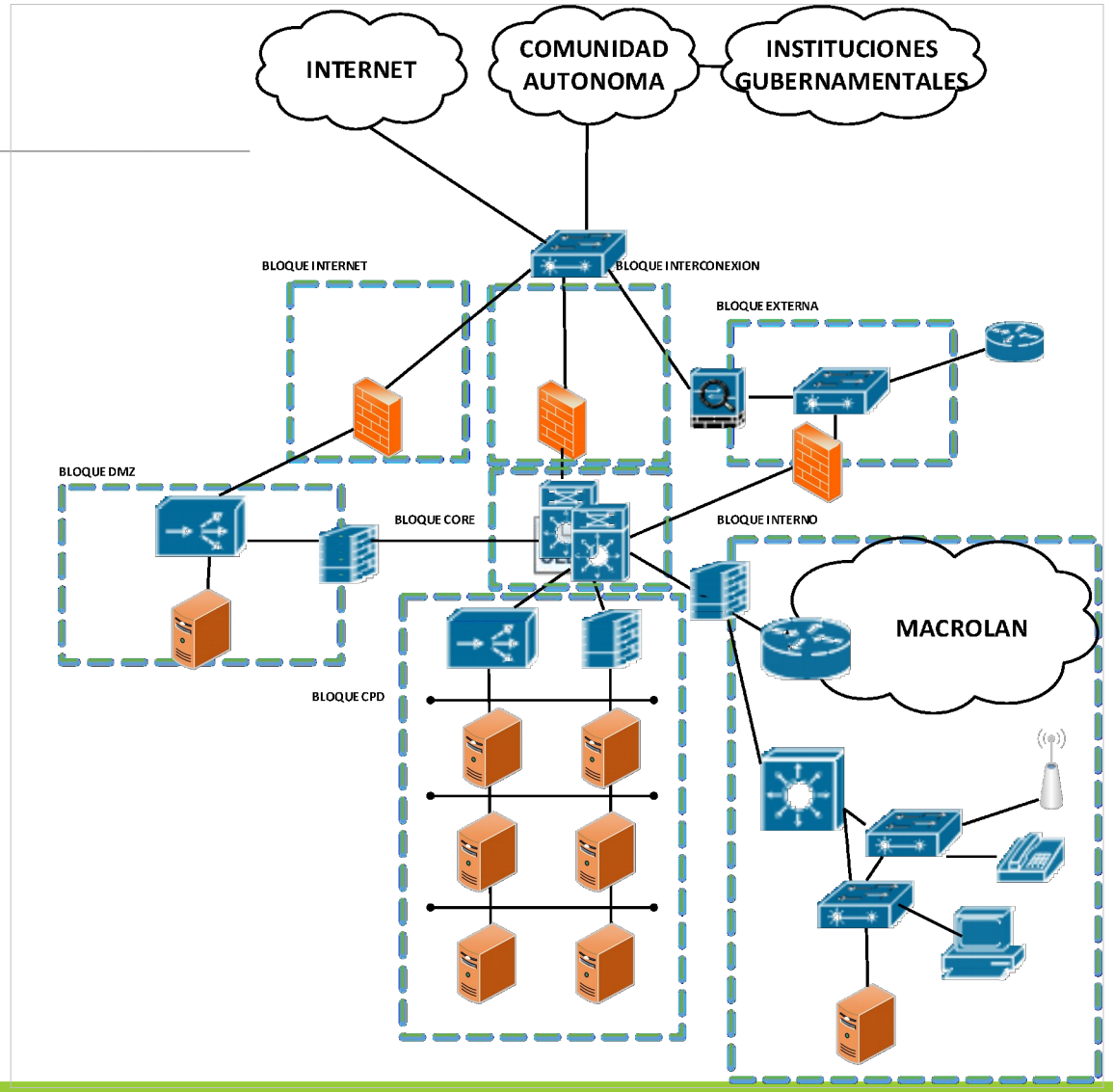
	Métricas	Valoración métricas	Valoración objetivos
O5	**M5.a.** ¿Qué medida de mejora de la visibilidad de la red hay?	90%	N.A.
	M5.b. ¿Qué grado de visión de la red se alcanza?	10%	
O6	**M6.a.** ¿En cuánto se estima el nivel de amenazas?	40%	N.A.
	M6.b. ¿En qué grado se estima la protección ante amenazas?	20%	
	M6.c. ¿Cuánto se estima la protección ante intrusiones?	10%	
	M6.d. ¿En qué grado existe protección ante la propagación?	10%	
	M6.e. ¿En qué grado se estima la posibilidad de detección de amenazas?	20%	
R1	**M7.** ¿Se han respetado cada uno de los requisitos?	N.A.	N.A.
R2		N.A.	
R3		N.A.	
R4		N.A.	
R5		N.A.	
R6		N.A.	
R7		N.A.	
R8		N.A.	

Diseño – Tipo I

Centro de Informática

CPD





Diseño – Tipo I

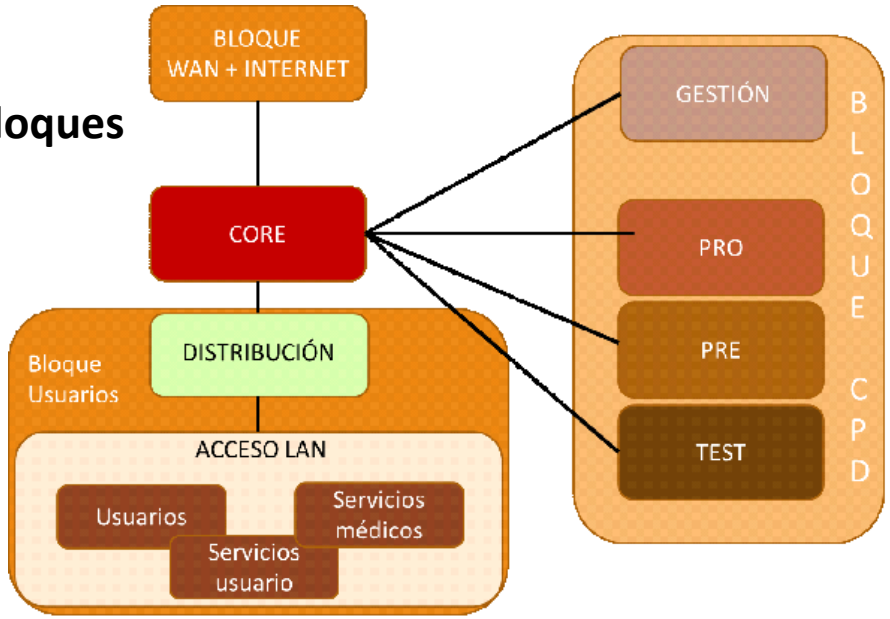
Tipo Sede	Sede	Bloque	Área	Solución
I	Centro de Informática	General	Gestión	Separación bloques, separación zonas, definición propósito bloques, Gestor log centralizado, perfilado CA Spectrum
			Visibilidad	
			Seguridad	
		Internet	Gestión	Eliminación proxy
			Visibilidad	
			Seguridad	Restricción URLs, Filtrado capa 7, IPS
		Interconexión	Gestión	
			Visibilidad	
			Seguridad	Políticas Antivirus
		Externa	Gestión	Sustitución P2P por VRF, integración LDAP, OCSP, APN
			Visibilidad	Usuarios individualizados
			Seguridad	Concentrador VPN antes firewall, SSO, Integración LDAP, políticas base usuario, eliminación usuarios locales, user login certificado, OCSP, plataforma salto, IPS Antivirus, Inspección SSL.
		DMZ	Gestión	Aceleración, wildcard
			Visibilidad	
			Seguridad	WAF, reverse proxy, aislamiento servidores públicos, firewall entre DMZ y Core, doble barrera fabricante.

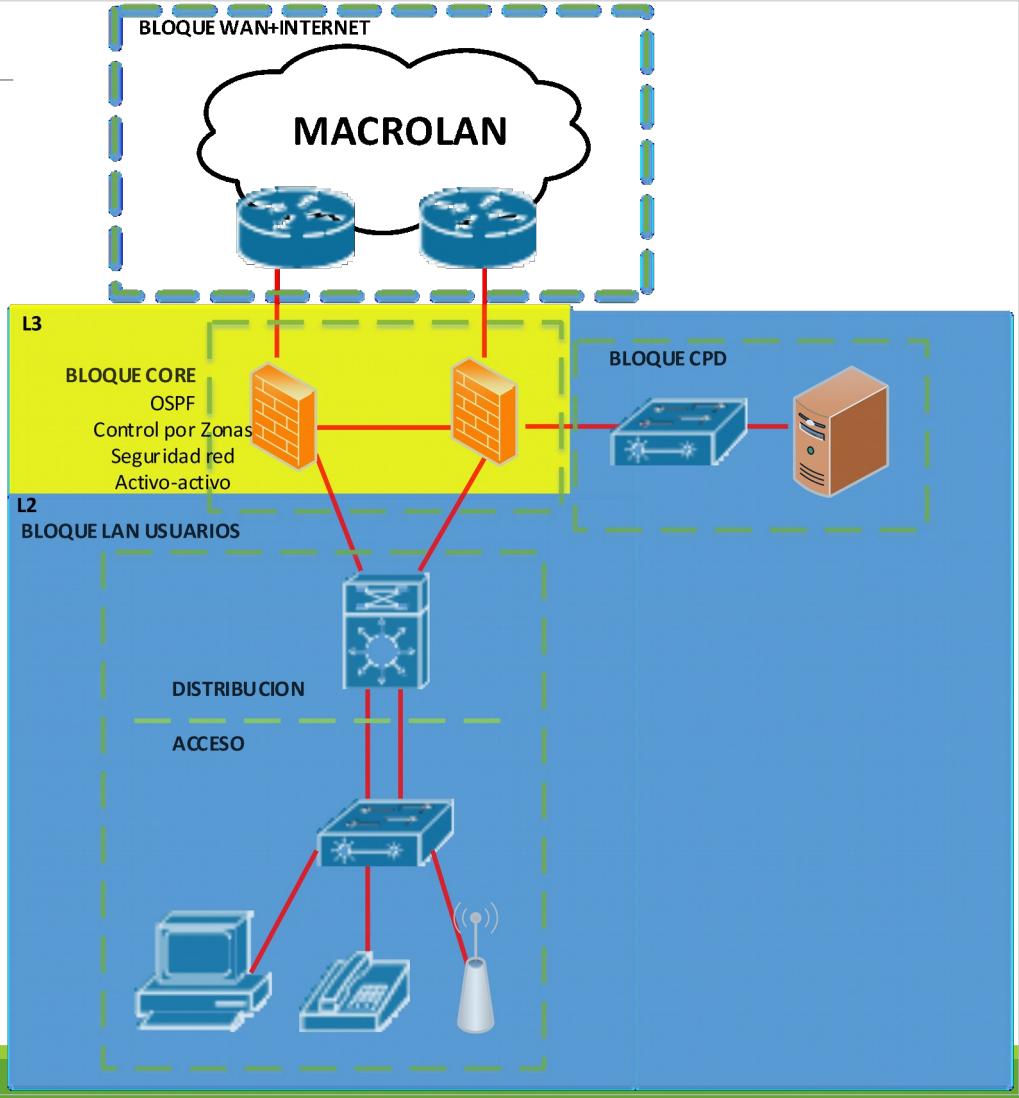
Tipo Sede	Sede	Bloque	Área	Solución
I	Centro de Informática	Core	Gestión	OSPF
			Visibilidad	
			Seguridad	
		CPD	Gestión	Zonas por nivel funcional, separación gestión de servicio, Unificar cableado a fibra, Frontales en ADC, acelerador contenidos, OCSP
			Visibilidad	Zonas por nivel funcional
			Seguridad	WAF, segmentación zonas, pasarela para gestión, aislamiento gestión, OCSP, segmentación servidores, conexión entre servidores, Unificación servicios en ADC.
		Interno	Gestión	Segmentación redes por rol, separación direccionamiento Inalambrico-cableado, Invitados portal cautivo autogestionado, NAC Server, Automatización procesos
			Visibilidad	Segmentación, separación direccionamiento Inalambrico-cableado, NAC Server, Integración firewall-NAC.
			Seguridad	Adición firewall, IPS, Antivirus, Quitar VLAN1 default, Asignar VLAN98 default, shutdown puertos, segmentación redes, separación direccionamiento Inalambrico-cableado, 802.1X, Validación LDAP, NAC Server, Integración firewall-NAC, detección temprana,

Diseño – Tipo I

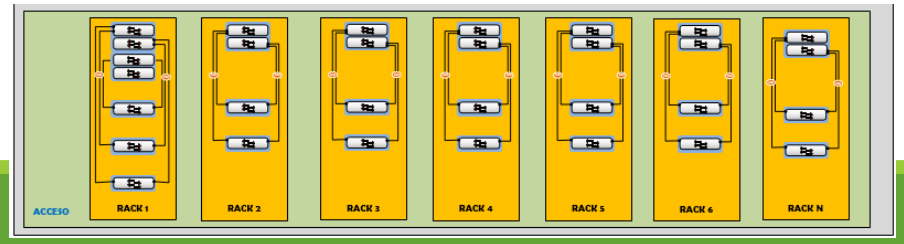
Hospitales

Diagrama bloques





Stack

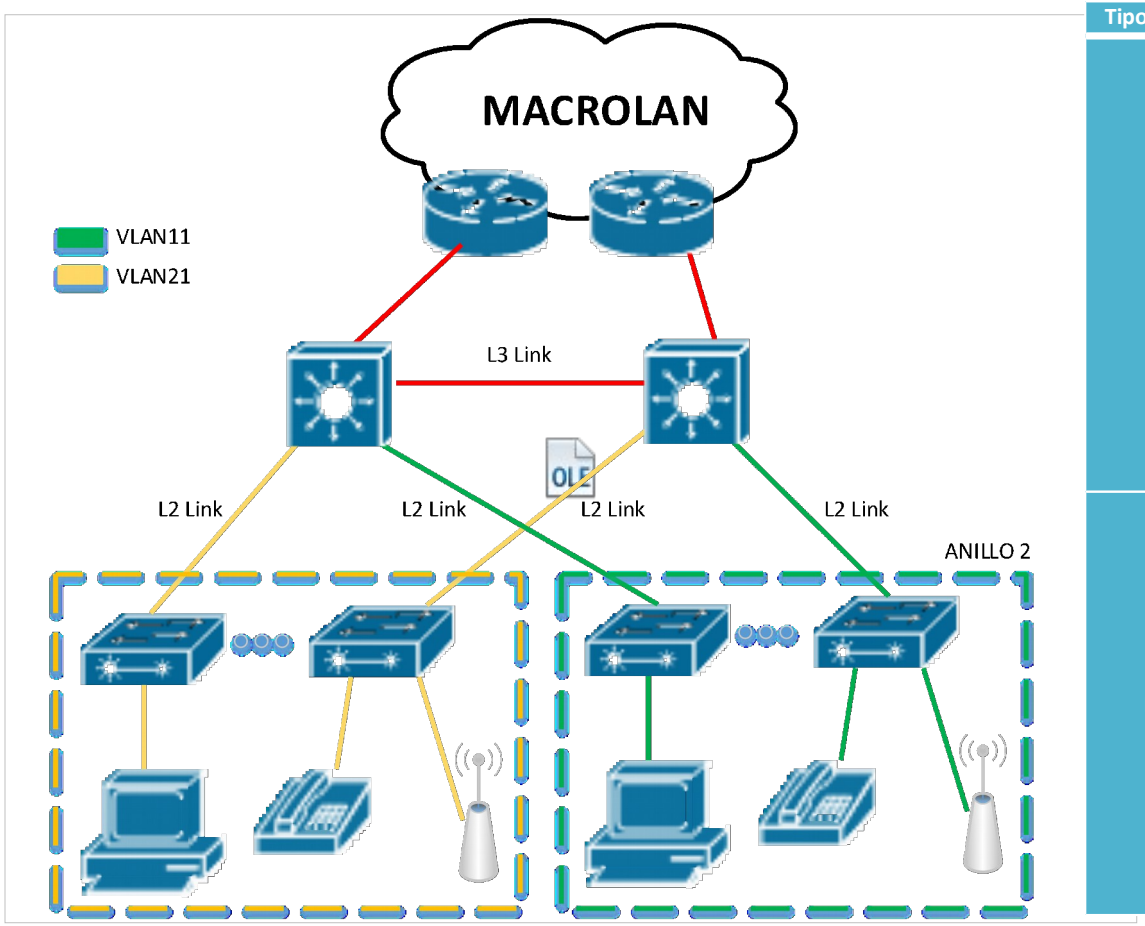


Diseño – Tipo I

Tipo Sede	Sede	Bloque	Área	Solución
I	Hospitales	General	Gestión	Hibrido arquitectura 3 capas y Core Compacto, Gestor log centralizado, perfilado CA Spectrum
			Visibilidad	
			Seguridad	
		CORE	Gestión	OSPF, eliminación ACLs, activo-activo, separación Zonas.
			Visibilidad	Nivel 3 Firewall
			Seguridad	Firewall Gestiona todo tráfico, Separación Zonas
		Internet	Gestión	SD-WAN con proveedor, QoS, OSPF
			Visibilidad	Monitorización SD-WAN.
			Seguridad	Firewall en perímetro, reglas capa 7, Filtrado URL, IPS, Antivirus. Túneles IPSec entre sedes
		CPD	Gestión	Zonas por nivel funcional, separación gestión de servicio, Unificar cableado a fibra, stack switchs, redundancia servidores, eliminación STP
			Visibilidad	Zonas por nivel funcional
			Seguridad	segmentación zonas, pasarela para gestión, aislamiento gestión, segmentación servidores, conexión entre servidores

Tipo Sede	Sede	Bloque	Área	Solución
		Usuarios	Gestión	Falsos distribución, stack, definición protocolo de conexión, eliminación STP, aumento caudal, topología libre bucles, segmentación redes por rol, separación direccionamiento Inalambrico-cableado, Invitados portal cautivo autogestionado, NAC Server, Automatización procesos
			Visibilidad	Segmentación, separación direccionamiento Inalambrico-cableado, NAC Server, Integración firewall-NAC, Wifi centralizada
			Seguridad	Adición firewall, IPS, Antivirus, Quitar VLAN1 default, Asignar VLAN98 default, shutdown puertos, segmentación redes, separación direccionamiento Inalambrico-cableado, 802.1X, WPA2-PSK-AES Validación LDAP, NAC Server, Integración firewall-NAC, detección temprana, Wifi Ciudadano separada de la red.

Diseño – Tipo II y Tipo III

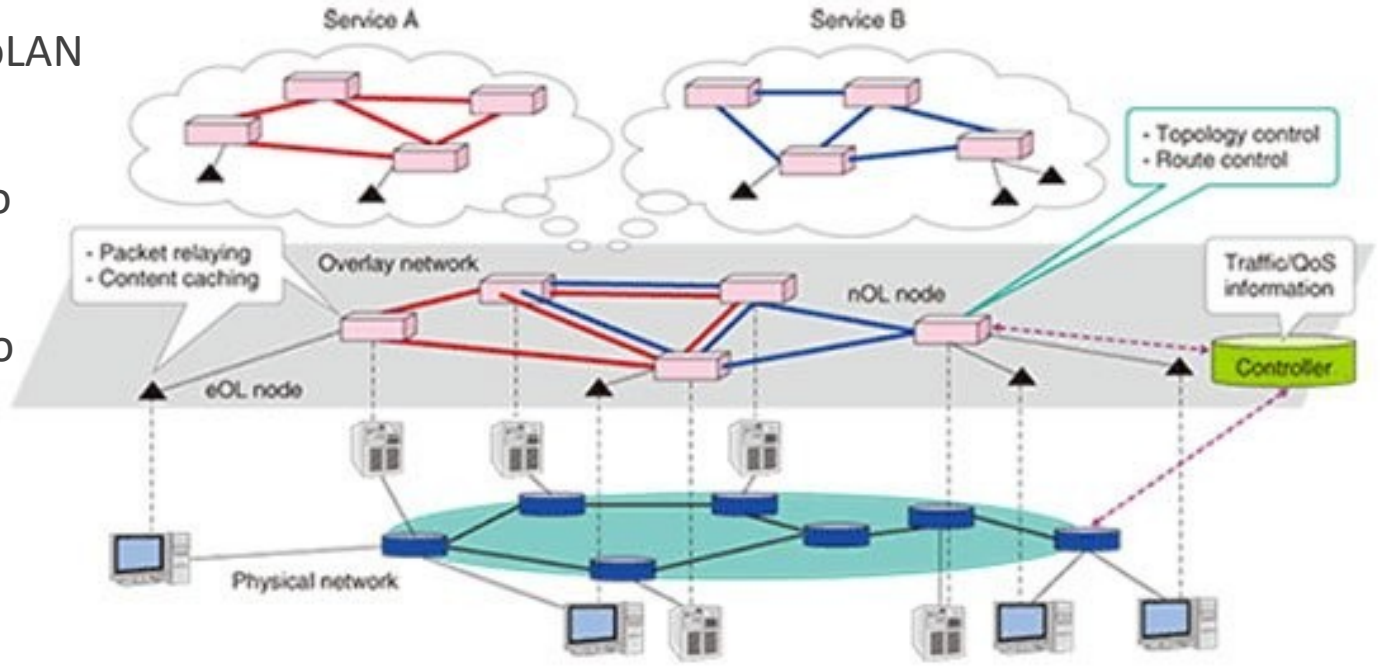


Tipo Sede	Sede	Bloque	Área	Solución
II	Hospitales y Centros de Especialidades. Centros de Salud y Centros administrativos. >20 usuarios	General	Gestión	Core compacto, definición protocolo de conexión, eliminación STP, aumento caudal, topología libre bucles, segmentación redes por rol, separación direccionamiento Inalambrico-cableado, Invitados portal cautivo autogestionado, NAC Server, Automatización procesos, SD-WAN con proveedor, QoS, OSPF
			Visibilidad	Segmentación, separación direccionamiento Inalambrico-cableado, NAC Server, Integración firewall-NAC, Wifi centralizada, monitorización SD-WAN, Nivel III en core, Gestor log centralizado, perfilado CA Spectrum
			Seguridad	Quitar VLAN1 default, Asignar VLAN98 default, shutdown puertos, segmentación redes, separación direccionamiento Inalambrico-cableado, 802.1X, WPA2-PSK-AES Validación LDAP, NAC Server, Integración firewall-NAC, detección temprana, Wifi Ciudadano separada de la red, túneles IPSec entre sedes
III	Centros de Salud y Centros administrativos. <20 usuarios	General	Gestión	Definición protocolo de conexión, eliminación STP, aumento caudal, topología libre bucles, segmentación redes por rol, separación direccionamiento Inalambrico-cableado, Invitados portal cautivo autogestionado, NAC Server, Automatización procesos, SD-WAN con proveedor, QoS, OSPF
			Visibilidad	Segmentación, separación direccionamiento Inalambrico-cableado, NAC Server, Integración firewall-NAC, Wifi centralizada, monitorización SD-WAN, perfilado CA Spectrum
			Seguridad	Quitar VLAN1 default, Asignar VLAN98 default, shutdown puertos, segmentación redes, separación direccionamiento Inalambrico-cableado, 802.1X, WPA2-PSK-AES Validación LDAP, NAC Server, Integración firewall-NAC, detección temprana, Wifi Ciudadano separada de la red, túneles IPSec entre sedes

Diseño - MacroLAN

Cambio de contratación de servicio a **SD-WAN,** aportando las **siguientes ventajas:**

- SD-WAN
- Posibilita tener mayor visión de la red MacroLAN
- Dota inteligencia a la red
- Infraestructura construida en base al servicio
- QoS basado en servicio
- OSPF área 0 – BRs routers sedes optimizando gestión y tráfico.
- QoE
- Túneles entre sedes, securizando el camino



Diseño - Monitorización

Se trata del **punto débil para resolver peticiones e incidencias** y es el principal causante de la **detección tardía de amenazas**.

Tras ajuste del diseño, se realizan las siguientes modificaciones en la monitorización:

- Se mantiene CA Spectrum, pero se perfila del siguiente modo:
  - Se añaden thresholds para aumentar proactividad
  - Se habilitan backups de configuraciones y gestión de versiones y cambios.
- Se cambia Cacti por ELK Stack, por mayor adaptación al negocio:
  - Permite disponer de servidores altamente distribuidos
  - Almacena y representa logs de dispositivos
  - Pollings SNMP a interfaces para almacenar tráfico.
  - Eventos de Seguridad capturados de los firewalls
- No se monitorizan las sedes Tipo III ya que decrementa considerablemente la gestión.

Resultados

	Métricas	Valoraciones métricas	Valoración objetivos
O1	M1.a. ¿Qué nivel de mejora futura existe en la gestión del tráfico?	20%	80%
	M1.b. ¿En qué medida se respeta la criticidad de los servicios?.	80%	
O2	M2.a. ¿Cuántos riesgos se han identificado?	+40	85%
	M2.b. ¿Qué estimación de riesgos se han identificado?	85%	
	M2.c. ¿El diseño cubre todos los riesgos identificados?	SI	
O3	M3.a. ¿Cuántos diseños se han implementado?	4	95%
	M3.b. ¿Se han respetado las buenas prácticas de diseño?	SI	
	M3.c. ¿En qué grado se ajusta el diseño a la tipología de centro?	90%	
O4	M4.a. ¿Qué nivel de mejora se estima que se ha producido en la administración de la red?	70%	75%
	M4.b. ¿En qué grado se estima la variación de número de incidencias?	75%	
	M4.c ¿En cuánto se estima que varíe el tiempo de respuesta ante peticiones, cambios e incidencias?	15 min	

	Métricas	Valoración métricas	Valoración objetivos
O5	**M5.a.** ¿En qué medida mejora la visibilidad de la red?	80%	85%
	M5.b. ¿Qué grado de visión de la red se alcanza?	90%	
O6	**M6.a.** ¿En cuánto se estima la reducción de amenazas?	80%	85%
	M6.b. ¿En qué grado se estima la mejora en protección ante amenazas?	85%	
	M6.c. ¿Cuánto se estima la mejora en protección ante intrusiones?	90%	
	M6.d. ¿En qué medida se reduce la propagación?	75%	
	M6.e. ¿En qué grado se estima la posibilidad de detección de amenazas?	80%	
R1	**M7.** ¿Se han respetado cada uno de los requisitos?	90%	95%
R2		100%	
R3		90%	
R4		100%	
R5		100%	
R6		100%	
R7		75%	
R8		90%	

Conclusiones

Envergadura del proyecto obliga a enfatizar el diseño en las sedes de mayor relevancia.

Se deben de implementar mecanismos de automatización para mejorar la gestión

- En caso de no existir automatización se tendría que optar por modelos de mayor riesgos.

La solución de diseño cumple con los objetivos y requisitos marcados.

- Se alcanza un equilibrio entre los objetivos.

	O1	O2	O3	O4	O5	O6
Valoración Objetivos	80%	85%	95%	75%	85%	85%

Se ha tenido que modificar la planificación para adaptarse a los contratiempos sufridos, mediante reordenación de tareas.

Las líneas de trabajo futuro se pueden centrar en:

- Implementación red con SDN
- Focalizar diseño en sedes tipo II y tipo III
- Focalizar diseño en CPDs
- Implementar y estudiar el nivel de ajuste de este modelo en una organización de otro ámbito.