Diseño de red de una organización Sanitaria

Ignacio Campos Marcé
Máster Universitario en Ingeniería de Telecomunicación
Telemática

Consultor: José López Vicario

03/01/2020

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño de red de una organización Sanitaria*
Nombre del autor:	*Ignacio Campos Marcé*
Nombre del consultor/a:	*Jose López Vicario*
Nombre del PRA:	*Jose López Vicario*
Fecha de entrega (mm/aaaa):	01/2020
Titulación:	*Máster Universitario en Ingeniería de Telecomunicación*
Área del Trabajo Final:	*TFM-Telemática*
Idioma del trabajo:	*Castellano*
Palabras clave:	*Diseño, Red, Sanidad*

Resumen del Trabajo:

La organización Ox, dispone de una red llamada Xenon, que interconecta los centros Hospitalarios, centros médicos, organizaciones gubernamentales y empresas externas de toda la Comunidad autónoma. Xenon es usada tanto para la comunicación entre los centros pertenecientes a la red, como para el servicio de aplicaciones al ciudadano y a los centros.

Esta red se caracteriza principalmente por la envergadura y cantidad de usuarios, el volumen de datos y la criticidad de los mismos. De este modo, la óptima gestión, arquitectura, seguridad y monitorización son las principales premisas que se han de tener en cuenta para obtener un diseño acorde con las características del servicio que se está ofreciendo.

De este modo, con el análisis de estos pilares fundamentales, se atenderán los principales factores que caracterizan la red para cada tipología de centro, resaltando los riesgos que implican y valorando con métricas basadas en los objetivos establecidos.

Así pues, se obtiene un diseño acorde para cada tipología de centro, que establece un balance óptimo entre las necesidades de la red y los riesgos, de modo que se concluye que es posible magnificar la gestión, seguridad y la monitorización, con costes mínimos, a través del correcto diseño de la arquitectura y adición de funcionalidades.

Abstract:

Ox organization has a network called Xenon which connects NHS centers, governmental organizations and external companies from the whole region. Xenon is used for communicating nodes from the network itself, as well as service provider to NHS centers and external citizens.

This network is distinguished by its size, big number of users, high amount of data and how critical they are. Considering these features, optimal management, architecture, security and monitoring are the main premises that we must accomplish to get a valid design for the service which is being offered.

Thus, with the analysis of these fundamentals, the main factors which describe the network for each sort of node wil be designed, standing out the risk components and evaluating them with metrics based on the goals agreed.

Therefore, a design for each sort of NHS center is obtained, which stablishes an optimal balance between the nekwork needs and risks. In conclusion, it is posible to increase the management, security and monitoring with minimal costs, through the correct architecture desgin and adding new features.

Índice

1. Introducción 1
   1.1. Contexto y justificación del Trabajo 1
   1.2. Objetivos del Trabajo 3
   1.3. Enfoque y método seguido 6
   1.4. Planificación del Trabajo 6
   1.5. Breve sumario de productos obtenidos 9
   1.6. Breve descripción de los otros capítulos de la memoria 9
2. Estado del arte 11
   2.1. Descripción de la Organización 11
   2.2. Tipos de sedes 13
   2.3. Acceso a la Información 14
      2.3.1. Accesos Inalámbricos 14
      2.3.2. Accesos Cableados 16
      2.3.3. Accesos Remotos 17
   2.4. Gestión del tráfico 18
   2.5. Tipos de arquitectura de red 20
      2.5.1. Redes convencionales 20
      2.5.2. Redes de nueva generación 22
   2.6. Monitorización y trazabilidad 24
   Resumen del capitulo 25
3. Análisis de la red 27
   3.1. Arquitectura de la red 27
      3.1.1. Red MacroLAN 27
      3.1.2. Redes de Área Local 29
      3.1.3. Análisis de monitorización y trazabilidad 34
   3.2. Análisis tecnológico 35
      3.2.1. Tecnología en Centro de Informática 35
      3.2.2. Tecnología en Hospitales 36
   3.3. Riesgos del modelo actual 37
      3.3.1. Riesgos sedes Tipo I 37
      3.3.2. Riesgos en Sedes tipo II y III 40
      3.3.3. Riesgos en monitorización 41
      3.3.4. Otros riesgos 41
   3.4. Resultados del Análisis de la red 42
   Resumen del capítulo 43
4. Diseño 45
   4.1. Diseño sedes Tipo I 45
      4.1.1. Centro de Informática 45
      4.1.2. Diseño Hospitales 54
   4.2. Diseños sedes Tipo II y III 63
   4.3. MacroLAN 69
   4.4. Diseño Monitorización y Trazabilidad 70
5. Resultados obtenidos y Viabilidad 72
6. Conclusiones 74
7. Glosario 76

8. Bibliografía 78
9. Anexos 80
9.1. Anexo I 80

Lista de figuras

Figura 1. Organización por bloques del Centro de Informática 11
Figura 2. Organización por bloques de Hospitales 13
Figura 3. Tipos redes inalámbricas 15
Figura 4. Tipos de accesos remotos 17
Figura 5. Representación gráfica de la Calidad de Servicio [4] 19
Figura 6. Arquitectura de tres capas 21
Figura 7. Reducción enlaces con Core compacto 22
Figura 8. Plano de control y de datos de arquitecturas convencionales [7] 23
Figura 9. Red overlay y underlay en SD-WAN 24
Figura 10. Tiempos de respuesta ante amenazas estudio Ponemon. [11] 25
Figura 11. Tipos de nodos que componen la red Xenon 29
Figura 12. Arquitectura de red Centro de Informática 31
Figura 13. Arquitectura de red Hospitales 33
Figura 14. Arquitectura de red en sedes tipo II y III 34
Figura 15. Diseño del Centro de Informática 46
Figura 16. Nuevo Bloque de Internet 47
Figura 17. Nuevo Bloque Externas 48
Figura 18. Nuevo Bloque CPD 51
Figura 19. Diseño Hospitales 55
Figura 20. Diseño lógico Hospitales 57
Figura 21. Diseño Hospitales físico bloque usuarios 58
Figura 22. Diseño de sedes tipo II 64
Figura 23. Diagrama de Gannt 80

Lista de tablas

Tabla 1. Resumen de la relación objetivos métricas. 6
Tabla 2. Planificación temporal de tareas 8
Tabla 3. Clasificación tipología de sedes según localización. 28
Tabla 4. Tabla de resultados del Análisis 43
Tabla 5. Resumen soluciones Centro Informática 54
Tabla 6. Relación de agrupación de switches y número fibras 58
Tabla 7. Resumen soluciones Hospitales 63
Tabla 8. Resumen soluciones sedes tipo II y III 69
Tabla 9. Resultados del Diseño 72
Tabla 10. Valoración objetivos 74

1. Introducción

En la actualidad las Tecnologías de la Información y Comunicación, se encuentran en un continuo crecimiento, avance y desarrollo. Esta revolución de gran importancia en la sociedad, tiene un amplio uso a día de hoy, tanto para el Marketing, dirección empresarial o incluso la gestión de centros Sanitarios, ofreciendo un sinfín de posibilidades adaptadas a las necesidades requeridas. El crecimiento del uso de este tipo de tecnologías, así como la evolución de las mismas, ha dejado atrás los modelos de diseño físico que sustentaban la red, incrementando los costes por mantenimiento, complejidad y sacrificando la seguridad de la información.

Las organizaciones requieren disponer de mecanismos de comunicación eficientes y seguras tanto a nivel interno, como entre diferentes puntos de presencia o sedes de la misma. Por ello, las redes de telecomunicaciones se han convertido en elementos indispensables que permiten la centralización de recursos, la compartición de datos y documentos, o capacidad de procesamiento de los mismos. El flujo de la información, así como la criticidad de la misma, pueden verse comprometidos si no se gestiona de manera eficiente y aplican las medidas de seguridad apropiadas. En redes de telecomunicaciones de organizaciones de gran tamaño, donde el número de recursos compartidos es elevado, así como el número de usuarios que hacen uso de ellos, la variedad de escenarios que pueden producirse requiere un estricto control y gestión del tráfico. En redes críticas, tales como las redes de datos de los centros sanitarios, la necesidad de disponer un servicio administrable, predecible y seguro requiere de un diseño de red que aplique mecanismos de control y de gestión del tráfico más estrictos que en redes convencionales. Por motivos de seguridad, los nombres e identificadores empleados en el presente proyecto han sido alterados por otros ficticios.

1.1. Contexto y justificación del Trabajo

La organización Ox, dispone de una red que interconecta los centros Hospitalarios, centros médicos, organizaciones gubernamentales y empresas externas de toda la Comunidad autónoma. Dicha red es usada tanto para la comunicación entre los centros pertenecientes a la red, como para el servicio de aplicaciones al ciudadano y a los centros. De ella dependen los más de 1000 centros de salud que pertenecen a esta agencia, existiendo aproximadamente 36.600 trabajadores que hacen un uso intensivo de la red, por no nombrar al resto de la ciudadanía. Durante el horario de trabajo los usuarios de cada centro hacen un uso continuo de las aplicaciones, generando flujos de datos que circulan dentro de la red e incluso en ocasiones dentro de la misma sede. Este tipo de tráfico puede ser corporativo, es decir tráfico generado por tareas de trabajo, o no corporativo. Además, cabe añadir, que la criticidad de los datos transmitidos puede variar según la aplicación empleada, pudiendo contener desde imágenes médicas hasta historiales de pacientes.

Cada sede Hospitalaria dispone de un centro de procesado de datos (CPD), que se interconecta con los nodos territoriales y estos a su vez al núcleo central de la red. La dependencia del funcionamiento óptimo de esta red es tal, que en caso de fallo podría ralentizar los servicios ofrecidos por los centros sanitarios, o incluso llegar a no ofrecer ciertas clases de servicios como la receta electrónica.

Actualmente, dado al gran número de usuarios de esta red, la generación de tráfico de datos es elevado, sobre todo en ciertas franjas horarias de trabajo. De igual modo, existe un continuo crecimiento de los servicios ofrecidos, integración entre los mismos y otras organizaciones. A su vez, también hay un aumento de la demanda que tiene la red, así como de los métodos de acceso a la misma, existiendo una tendencia en alza a la movilidad y al e-working. Todo ello provoca que en ocasiones se llegue a saturar la red, poniendo en riesgo los recursos disponibles de la misma.

Por otro lado, los múltiples ataques contra las vulnerabilidades de la red, como los ataques de Denegación de Servicio, o la propagación de malware dentro de la red, no son monitorizados ni controlados a tiempo, llegando a interrumpir la red durante 30 minutos, hasta iniciar una resolución de incidentes. Además, la facilidad de acceso a la red, como al uso de herramientas no corporativas para transmitir la información, como por ejemplo, envío de informes de pacientes, pone en serio compromiso la seguridad de la información, pudiendo haber fugas de información o ejecutar con facilidad ataques Man in the middle.

La solución aplicada al crecimiento de uso de la red, es la adición de nuevos equipamientos sin un criterio definido y sin aplicación de medidas de seguridad adecuadas. En cuanto a la tendencia hacia el e-working se ve obstaculizada por la infraestructura actual, permitiendo el acceso por Redes Privadas Virtuales (VPN), pero sin un control de accesos individualizado y que verifique la integridad del dispositivo. Por otro lado, el tratamiento dado a los distintos incidentes relacionados con la administración del flujo de tráfico, como la gestión del ancho de banda o el análisis de datos, es prácticamente nulo, haciendo uso de las herramientas estadísticas de los propios dispositivos.

No obstante, pese a que se disponen de un gran número de recursos de elevado coste y calidad para una gestión optimizada y securizada, no se emplean como deberían o se destina cada dispositivo físico a un solo propósito, siendo soluciones contraproducentes que complican la gestión e incrementan los costes.
Debido a los numerosos problemas descritos anteriormente, en una red donde el menor fallo es crítico, se ha decidido realizar un proyecto de diseño y securización de la red de una organización sanitaria. A consecuencia del elevado caudal de trabajo diario, la resolución de incidentes donde el 50% son provenientes de dicha gestión, el 20% es por la falta de trazabilidad para detectar los incidentes de seguridad y los proyectos puestos en marcha, los empleados técnicos responsables del

funcionamiento óptimo de la red, no disponen del tiempo suficiente para realizar el presente proyecto de replanteo.

Este proyecto trata de diseñar un modelo de red para las diferentes tipologías de centros, para optimizar el uso de recursos, la administración y la seguridad de los mismos, siendo un modelo escalable y que permita la trazabilidad de la información, minimizando las tareas de mantenimiento y gestión, así como incremente la experiencia de usuario sin descuidar la securización de acceso del mismo. Además, se tendrán en cuenta aspectos como la criticidad de la información o del entorno, que influirán directamente en el diseño del modelo, aplicando las medidas que sean necesarias para garantizar la seguridad y la disponibilidad de la información.

1.2. Objetivos del Trabajo

El objetivo principal del presente proyecto consiste en el análisis y diseño de un modelo de red de una organización de índole sanitario. De este modo, se pretende establecer las pautas a tener en cuenta para la implementación de una red sanitaria, en cumplimiento con la criticidad de la información y mejora de la experiencia de administración y de usuario. Para ello se procede al análisis y diseño del modelo con los siguientes objetivos generales:

- **Definir las características de la red.** Existen diferentes tipos de tráfico circulando en una red sanitaria, así como tipologías de centros y comunicaciones, cuyas criticidades varían según la lógica de negocio o contenido de la información, por lo que es necesaria su identificación y definición de requisitos.
- **Definir un modelo óptimo y escalable.** De este modo poder simplificar la administración y, al mismo tiempo, ofrecer una mejor experiencia de usuario.
- **Establecer mecanismos que permitan la trazabilidad.** Así poder tener una visión completa de los flujos de tráficos, incrementando el conocimiento de la organización, permitiendo proactividad ante anomalías e incidentes.

Por lo tanto, los objetivos específicos a cumplir a lo largo del proyecto son detallados a continuación:

O1. Comprender la lógica de negocio. Revisión de la lógica de negocio para entender su organización, objetivo y función.
O2. Analizar los riesgos de la red actual. Identificar y definir los riesgos que supone el diseño de red actual.
O3. Definir diseño de red según tipología de centros. Según los tipos de centros existentes dentro de la organización, definir un modelo de red que cumpla con los requisitos establecidos.
O4. Mejorar la administración de la red. Minimizar la carga de trabajo, así como facilitar la resolución de incidencias y minimizar tiempos de respuesta.

O5. Aumentar la visibilidad de la red. Mejorar la monitorización y la trazabilidad del tráfico de la red.

O6. Implementar medidas de seguridad en la red. Establecer las medidas de seguridad oportunas en la red para minimizar los incidentes de seguridad tales como, accesos no autorizados, propagación de amenazas, ciberataque, etc.

Por otro lado, el cliente ha especificado una serie de requisitos que debe cumplir el modelo a diseñar.

R1. El diseño tiene que servir para la gestión optima del ancho de banda de la red.

R2. El modelo debe de estar estructurado de manera que sirva a su vez para la monitorización del tráfico de la red.

R3. La estructura debe ser clara y comprensible.

R4. Se debe segmentar el tráfico corporativo del no corporativo.

R5. Tiene que ser un modelo base para su implantación en los demás centros de la Organización Ox.

R6. Se deben aprovechar el máximo equipamiento posible.

R7. Extender la red WiFi al ciudadano en todos los centros.

R8. Facilitar mecanismos para el e-working del personal interno.

Para valorar el grado de cumplimiento de los objetivos se han definido las siguientes métricas:

M1. Comprender la lógica de negocio. En qué grado se ajusta el diseño a la lógica de negocio, respondiendo a las preguntas ¿Qué nivel de mejora existe en la gestión del tráfico?¿En qué medida se respeta la criticidad de los servicios?.

M2. Analizar los riesgos de la red actual. Análisis del grado de identificación y valoración de riesgos del diseño actual, respondiendo a las preguntas ¿Cuántos riesgos se han identificado?¿Que estimación de riesgos se han identificado?¿El diseño cubre todos los riesgos identificados?

M3. Definir diseño de red según tipología de centros. Medida del diseño planteado de red según el tipo de centro, respondiendo a las preguntas ¿Cuántos diseños se han implementado?¿Se han respetado las buenas prácticas de diseño?¿En qué grado se ajusta el diseño a la tipología de centro?

M4. Mejorar la administración de la red. En qué grado el diseño facilita la administración de la red, respondiendo a las preguntas ¿Qué nivel de mejora se estima que se ha producido en la administración de la red?¿En qué grado se estima la variación de número de incidencias?¿En cuánto se estima que varíe el tiempo de respuesta ante peticiones, cambios e incidencias?

M5. Aumentar la visibilidad de la red. Análisis del grado en el que aumenta la visibilidad de la red, respondiendo a las preguntas ¿En qué medida mejora la visibilidad de la red?¿Qué grado de visión de la red se alcanza?

M6. Implementar medidas de seguridad en la red. En qué medida se ha mejorado la seguridad de la red con el diseño implementado, respondiendo a las preguntas ¿En cuánto se estima la reducción de amenazas?¿En qué grado se estima la mejora en protección ante amenazas?¿Cuánto se estima la mejora en protección ante intrusiones?¿En qué medida se reduce la propagación?¿En qué grado se estima la posibilidad de detección de amenazas?

M7. Cumplimiento de requisitos. En qué grado se cumplen los requisitos del cliente, respondiendo a la pregunta ¿Se han respetado cada uno de los requisitos?

A continuación, se recoge en la Tabla 1, una tabla resumen los objetivos con las métricas aplicadas:

	Métricas	**Valoración métricas**	**Valoración objetivos**
O1	**M1.a.** ¿Qué nivel de mejora existe en la gestión del tráfico?		
	M1.b. ¿En qué medida se respeta la criticidad de los servicios?.		
O2	**M2.a.** ¿Cuántos riesgos se han identificado?		
	M2.b. ¿Qué estimación de riesgos se han identificado?		
	M2.c. ¿El diseño cubre todos los riesgos identificados?		
O3	**M3.a.** ¿Cuántos diseños se han implementado?		
	M3.b. ¿Se han respetado las buenas prácticas de diseño?		
	M3.c. ¿En qué grado se ajusta el diseño a la tipología de centro?		
O4	**M4.a.** ¿Qué nivel de mejora se estima que se ha producido en la administración de la red?		
	M4.b. ¿En qué grado se estima la variación de número de incidencias?		
	M4.c ¿En cuánto se estima que varíe el tiempo de respuesta ante peticiones, cambios e incidencias?		
O5	**M5.a.** ¿En qué medida mejora la visibilidad de la red?		
	M5.b. ¿Qué grado de visión de la red se alcanza?		
O6	**M6.a.** ¿En cuánto se estima la reducción de amenazas?		
	M6.b. ¿En qué grado se estima la mejora en protección ante amenazas?		
	M6.c. ¿Cuánto se estima la mejora en protección ante intrusiones?		
	M6.d. ¿En qué medida se reduce la propagación?		
	M6.e. ¿En qué grado se estima la posibilidad de detección de amenazas?		
R1	**M7.** ¿Se han respetado cada uno de los requisitos?		
R2			
R3			

R4			
R5			
R6			
R7			
R8			

Tabla 1. Resumen de la relación objetivos métricas.

1.3. Enfoque y método seguido

El método seguido a lo largo del proyecto es un método analítico seguido de un diseño teórico de la solución propuesta. Esto se consigue en base a un análisis de riesgos que se han de mitigar y la alineación con los objetivos y requisitos del proyecto. De este modo, se toma como referencia el diseño origen del modelo para mejorarlo.

1.4. Planificación del Trabajo

A lo largo del siguiente punto se describen las tareas de trabajo y la metodología empleada para abordar cada una de las etapas para alcanzar los objetivos especificados teniendo en cuenta la metodología general:

T1. Definición del proyecto. En esta primera etapa, será definida la tipología y localización del proyecto, para ello se hará uso de las motivaciones propias para una selección entre las competencias posibles. De este modo, y mediante una investigación para identificar el ámbito del trabajo, será posible establecer de manera global la base del proyecto.

T2. Definición de objetivos y planificación temporal. Para dotar de una estructura, una envergadura y unas directrices orientativas, es necesario, una vez definido el proyecto, establecer unos objetivos. Estos, vendrán dados tanto por el tipo de organización que planteará el problema a resolver, como por el propio desarrollo proyecto que impondrá requisitos con fines didácticos adicionales. Por otro lado, se realizará una línea temporal para la realización de dicho trabajo.

T3. Estado del arte. Es importante la adquisición de los conocimientos necesarios previamente a la iniciación del proyecto. De esta manera, mediante la búsqueda de información, posibilita la formación de manera global en las necesidades, problemáticas y posibles soluciones de los distintos aspectos que se puedan presentar a lo largo del trabajo, así como, elegir la metodología idónea para la elaboración general del proyecto. Este proceso resulta de gran utilidad para comprender la lógica de negocio de una organización sanitaria, la circulación y tipología del tráfico de la red y la criticidad del mismo, así como los tipos de accesos, diseños actualmente existentes y soluciones tecnológicas para llevarlo a cabo.

T4. Anteproyecto y documentación. Ya definida la totalidad del proyecto, se procede al desarrollo de un Anteproyecto para su posterior aprobación. En caso de no ser aprobado, se redefinirán los objetivos, tiempo o presupuesto, acorde con las necesidades del mismo. Tras su

aprobación, se cumplimentará la documentación necesaria para su puesta en marcha.

T5. Escritura de proyecto. La generación de la documentación pertinente, será necesaria como diario de trabajo y para una futura presentación del proyecto realizado. Por estos motivos, el comienzo de este, tendrá lugar al mismo tiempo que el estudio preliminar y finalización en su entrega.

T6. Desarrollo. En este, serán planteados los problemas de implementación existentes y una serie de soluciones. Para aplicar las soluciones, se implementará el diseño óptimo del modelo según la tipología de centro, especificando las soluciones tecnológicas empleadas y los mecanismos empleados para garantizar la seguridad y trazabilidad de la información.

T7. Conclusiones. Para finalizar, se definen las conclusiones generales obtenidas, realizando una comparación con modelos convencionales, para visualizar si los resultados son los esperados y de qué manera ha afectado la mejora implementada. Dicha tarea concluirá con una perspectiva futura de uso del presente proyecto.

Así pues, con las tareas y objetivos marcados, se procede a la definición de la planificación temporal que se recoge en la Tabla 2. En el Anexo I se puede observar el diagrama de Gannt de dicha planificación.

Nombre Tarea	**Duración**	**Comienzo**	**Fin**	**Pred.**
Diseño de modelo de red de entornos sanitarios	**84 días**	**mié 18/09/19**	**lun 13/01/20**	
Definición del Proyecto	**5 días**	**mié 18/09/19**	**mar 24/09/19**	
Definición del Trabajo a Realizar	2 días	mié 18/09/19	jue 19/09/19	
Investigación sobre la organización	3 días	vie 20/09/19	mar 24/09/19	2
Go-No Go	0 días	mar 24/09/19	mar 24/09/19	3
Definición de Objetivos y tiempo	**6 días**	**mié 25/09/19**	**mié 02/10/19**	
Definición de etapas del proyecto	3 días	mié 25/09/19	vie 27/09/19	4
Definición de objetivos a alcanzar	2 días	lun 30/09/19	mar 01/10/19	6
Estimación Escala de Tiempos	1 día	mié 02/10/19	mié 02/10/19	7
Go-No Go	0 días	mié 02/10/19	mié 02/10/19	8
AnteProyecto y Documentación	**8 días**	**mié 25/09/19**	**vie 04/10/19**	
Documentación necesaria	1 día	mié 25/09/19	mié 25/09/19	3
Formalización documentación	1 día	mié 02/10/19	mié 02/10/19	11;7
Entrega	1 día	jue 03/10/19	jue 03/10/19	12
Aceptación	1 día	vie 04/10/19	vie 04/10/19	13
Go-No Go	0 días	vie 04/10/19	vie 04/10/19	14
Escritura de Proyecto	39 días	lun 07/10/19	jue 28/11/19	15

Estudio Preliminar	**18 días**	**lun 07/10/19**	**mié 30/10/19**	
Lógica de Negocio	**8 días**	**lun 07/10/19**	**mié 16/10/19**	
Tipologías de centros	3 días	lun 07/10/19	mié 09/10/19	15
Flujo de trafico	3 días	jue 10/10/19	lun 14/10/19	19
Métodos de acceso a la red	3 días	jue 10/10/19	lun 14/10/19	19
Criticidad de datos	2 días	mar 15/10/19	mié 16/10/19	21;20
Metodología	1 día	jue 17/10/19	jue 17/10/19	22
Modelos de diseños	5 días	jue 17/10/19	mié 23/10/19	22
Soluciones tecnológicas	5 días	jue 24/10/19	mié 30/10/19	24
Go-No Go	0 días	mié 30/10/19	mié 30/10/19	25
Desarrollo	**14 días**	**jue 31/10/19**	**mar 19/11/19**	
Descripción del modelo	**6 días**	**jue 31/10/19**	**jue 07/11/19**	
Diseño según tipología sede	6 días	jue 31/10/19	jue 07/11/19	26
Diseño según tipo de acceso	6 días	jue 31/10/19	jue 07/11/19	26
Medidas de Seguridad implementadas	3 días	vie 08/11/19	mar 12/11/19	30
Medidas de trazabilidad	2 días	mié 13/11/19	jue 14/11/19	31
Herramientas implementadas	3 días	vie 15/11/19	mar 19/11/19	32
Go-No Go	0 días	mar 19/11/19	mar 19/11/19	33
Conclusiones	**7 días**	**mié 20/11/19**	**jue 28/11/19**	
Conclusiones Generales	3 días	mié 20/11/19	vie 22/11/19	34
Viabilidad del proyecto	3 días	lun 25/11/19	mié 27/11/19	36
Trabajo Futuro	1 día	jue 28/11/19	jue 28/11/19	37
Go-No Go	0 días	jue 28/11/19	jue 28/11/19	38
Exposición	1 día	lun 13/01/20	lun 13/01/20	

Tabla 2. Planificación temporal de tareas

A continuación, se muestra el seguimiento de la planificación previamente establecida, así como los costes temporales asociados y las medidas aplicadas.

Primera entrega de Trabajo:

- No hay anomalías en la planificación del trabajo.
- Se sigue el calendario establecido.

Segunda entrega de Trabajo:

- Existen correcciones en la Definición del Trabajo y Definición de objetivos, los cuales se han de redefinir y ajustar a los requisitos del proyecto.
    - Coste temporal: Se prevé un retraso temporal de 3 días sobre el proyecto.
    - Medidas: No se aplican medidas correctivas.
- A fecha de entrega [13/11/2019] Se alcanza el inicio de Medidas de Seguridad implementadas.

Tercera entrega de Trabajo:

- Existen correcciones en la tarea de Escritura de Proyecto y en las Fases de Estudio Preliminar y Diseño. Se proponen mejoras en estructura del proyecto.

    - Coste temporal: Se prevé un retraso temporal de 15 días sobre el proyecto.
    - Medidas:
        - Se dedica más tiempo al proyecto.
        - Se resta tiempo a la tarea de Escritura de Proyecto.
            - Se replanifica esta tarea con fecha finalización 24/12/2019.
        - Se modifica el orden de las tareas, se antepone Viabilidad a Conclusiones.
- A fecha de entrega [18/12/2019] Se alcanza la tarea de Viabilidad del proyecto.

Cuarta entrega de Trabajo:

- Con el nuevo plan establecido se sigue correctamente.

1.5. Breve sumario de productos obtenidos

No aplica ya que no han sido necesario obtener recursos para realizar el diseño, dado que se trata de un diseño teórico.

1.6. Breve descripción de los otros capítulos de la memoria

En este apartado se describe la estructuración de los capítulos que está compuesto el proyecto.

- **Capítulo 1.** Este capítulo se realiza una introducción al proyecto para así establecer el contexto y justificación. Además, se detallan los objetivos propuestos y la metodología optada para la realización del trabajo. De igual manera, se detallan las etapas o fases de las que consta el proyecto, realizando una breve descripción de cada una, así como el método de elaboración.
- **Capítulo 2.** A lo largo de este capítulo se realizará una primera aproximación para incrementar la comprensión de los temas que va abordar el proyecto. Para ello se realiza una breve descripción de la las características típicas de una red perteneciente al sector de Salud. Se pretende dar una visión general de los aspectos que componen la base del proyecto, definiendo y analizando los diferentes diseños, protocolos, las tipologías de centros y métodos de acceso a la información.
- **Capítulo 3.** Basándose en el anterior capítulo, se realiza un análisis de las características típicas de red y como se ajustan las soluciones existentes, como trabajo previo al diseño. Este análisis contemplará la arquitectura de la red, como la base de cada tipología de sede. De igual modo, se detallarán las soluciones tecnológicas a utilizar. Una vez analizadas las partes técnicas de la red, el capítulo prosigue con el análisis de la estructura implementada y del tráfico de la red.
- **Capítulo 4.** En el siguiente capítulo se refleja la aportación propia. En él se detallará el diseño final sobre clasificaciones tipológicas que se han

definido previamente, exponiendo los motivos asociados a esa elección de diseño, protocolos y equipamiento. Para finalizar, se dará una visión de los mecanismos empleados que implementan la seguridad y trazabilidad deseada.

- **Capítulo 5.** Se realiza un estudio sobre la viabilidad del proyecto. Para ello, se muestra, una organización y estimación temporal del proyecto.
- **Capítulo 6.** Se exponen las conclusiones obtenidas del trabajo desarrollado. Posteriormente serán comentados los costes temporales. También se discute el cumplimiento de los objetivos, realizando un análisis comparativo de los resultados obtenidos, con los previos. El capítulo concluye proponiendo las líneas de trabajo futura que derivan del proyecto realizado

2. Estado del arte

2.1. Descripción de la Organización

La Organización Ox dispone de una red de datos de área extensa llamada Xenon. Es una red multiservicio IP de banda ancha, diseñada para gestionar servicios de voz, datos e imagen. Incorpora, entre otras, el potencial para aplicar técnicas de calidad de servicio, optimización de ancho de banda y de seguridad. Ofrece acceso a internet, así como acceso remoto a la red, y dispone de un Centro de Gestión de red desde donde se realiza una gestión integral y centralizada permitiendo administrar sus funcionalidades. En la actualidad da cobertura a 1292 Centros Sanitarios y Administrativos en la Comunidad Autónoma, además de integrar servicios con otras organizaciones.

De igual modo, la Organización Ox forma parte de una red más extensa que está compuesta por el resto de organizaciones de la Comunidad Autónoma y a su vez, por los organismos que componen el ministerio y resto de Comunidades, que será llamada red "Interministerial", tal y como queda reflejado en la Figura 1.

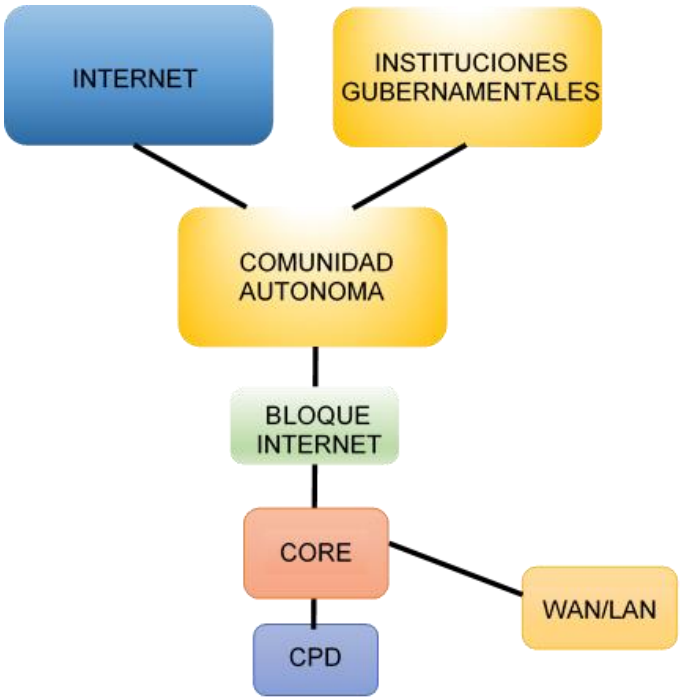

Figura 1. Organización por bloques del Centro de Informática

La evolución de la red Xenon en los últimos años ha estado marcada por las crecientes demandas de los proyectos incluidos en el "Plan de Sistemas de Información (2009-2011)" de la Ox, cuyos objetivos fundamentales han sido poder realizar una autentica gestión sanitaria integral y conseguir el acercamiento al ciudadano.

La puesta en marcha de aplicaciones corporativas, en base a un modelo de arquitectura centralizada donde la red se convierte en un factor crítico, ha exigido realizar un especial esfuerzo en mejorar las infraestructuras de comunicaciones existentes en todos los centros de la Ox, con los objetivos de alcanzar la conectividad de todos los puestos de trabajo, optimizar el rendimiento y asegurar su disponibilidad.

Por otra parte, la utilización de aplicaciones multimedia, que en el entorno sanitario se suelen agrupar bajo el concepto de telemedicina, ha obligado a buscar mecanismos de gestión de tráfico, de manera que se puedan clasificar los paquetes de información en origen, para posteriormente aplicar tratamientos diferenciados de reservas de ancho de banda y establecer prioridades.

De acuerdo con el programa actual de modernización de los sistemas de información, está previsto continuar con la implantación de nuevos servicios, todos ellos desarrollados bajo el criterio de integración. El objetivo de lograr la completa integración, requiere que la Red no solo sea capaz de transportar datos, imagen y voz, sino que además debe ofrecer la máxima calidad, ya que se convierten en servicios esenciales de la gestión sanitaria actual y futura.

Para mantener de manera eficaz todas las funcionalidades, así como garantizar la continuidad del servicio se hace indispensable disponer de una gestión integral y centralizada que incremente la calidad y los niveles de disponibilidad de las redes, mediante la realización de tareas de soporte, administración y mantenimiento de las infraestructuras y equipamiento de comunicaciones que la componen.

Las redes de los diversos Hospitales de la Ox se han ido creando a medida que surgían las necesidades en cada uno de ellos. Por lo tanto, se diseñó un “Modelo de Red” ideal, en semejanza con el núcleo de la red ubicado en el Centro de Informática, que atendía a los parámetros de disponibilidad, escalabilidad y rendimiento, que se detallarán en el Capítulo 3.

- **Disponibilidad:** Para que la red tenga alta disponibilidad se ha diseñado de tal forma que gran parte del equipamiento de red, así como los enlaces que unen dicho equipamiento, este redundado. Además, el diseño divide la red en bloques funcionales de manera que fallos producidos en un bloque no se propaguen al resto de bloques. Esto también facilita la gestión de cambios, ya que un cambio realizado sobre un bloque funcional no afecta al resto de bloques.
- **Escalabilidad:** Para que las ampliaciones de red o la puesta en marcha de nuevos servicios se pueda realizar de forma sencilla mediante la adición de nuevo equipamiento, sin tener que modificar la arquitectura de red ya existente.
- **Capacidad:** que la red tenga un ancho de banda suficiente para que por ella circule el tráfico de los sistemas de información corporativa actual y los venideros a medio plazo.

El resultado fue el esquema del modelo de Hospital de la Figura 2.

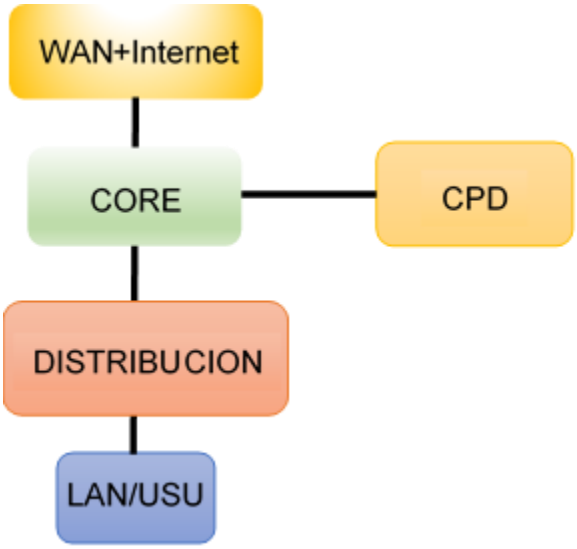

Figura 2. Organización por bloques de Hospitales

2.2. Tipos de sedes

Las organizaciones sanitarias están compuestas por diferentes tipos de sedes, que van destinados a dar unos servicios determinados. La tipología de cada sede, va en función de su tamaño, al número de ciudadanos que va dirigido, el servicio prestado o la época del año. Cabe anotar, que la organización Ox, dispone de una clasificación en 3 tipos de sedes que se verá en el apartado “3.1.1 Red MacroLAN”.

Así pues, es posible encontrar Hospitales, que son emplazamientos de grandes dimensiones, donde se dan servicios de asistencia sanitaria por parte de facultativos. Esta asistencia puede ser especializada o primaria, según el grado de atención requerido, que a su vez puede ser cotidiana o de urgencia. En general, los Hospitales disponen de todo tipo de instalaciones y servicios, teniendo zona de Urgencias, Consultas externas, mostradores, administración, etc. Con lo que se encuentran servicios de Radiografía y Mamografía o centralitas de telefonía.

Una variante de los Hospitales son los Hospitales o Centros de Atención para pacientes crónicos de Larga Estancia (HACLEs). Estos Hospitales, generalmente de menores dimensiones que los anteriores y por lo tanto con menor número de servicios y trabajadores, van destinados a un determinado número de pacientes. Estos pacientes necesitan cuidados paliativos y su estancia en el Hospital es de mayor duración, como, por ejemplo, convalecientes postquirúrgicos, con daños cerebrales, etc.

Por otro lado están los Centros de Salud, donde se realiza atención principalmente primaria y por tanto el número de facultativos y, por ende, el número de pacientes se reduce considerablemente, con lo que el número

de servicios ofrecidos se reducen a los básicos. No obstante, también se ofrecen servicios de urgencias, en los cuales se da una atención primaria para su posterior derivación al Hospital de referencia. Este tipo de centros, van dirigidos a una región determinada, como un distrito de una gran ciudad o un municipio con gran número de habitantes.

En cambio, la atención especializada, se delega en otro tipo de centros muy similares en cuanto a tamaño, llamados Centros de Especialidades, los cuales disponen de servicios especializados similares a los que dispone un Hospital.

En cuanto a los centros de menor tamaño se encuentran los Consultorios Auxiliares. Los consultorios auxiliares, son centros de atención primaria localizados en pueblos de pocos habitantes o pedanías. Los servicios de atención primaria de estos centros, van destinados a un conjunto reducido, llegando en ocasiones a realizar agrupaciones de pueblos a los que ofrecer sus servicios. La mayor parte de facultativos proviene del Centro de Salud de referencia y la atención al usuario viene determinada a unas pocas horas y días determinados.

Por último, es posible encontrar los centros cuyas funciones se alejan de la atención primaria y especializada. Así pues, se encuentran los centros de Salud Pública, cuyo fín va a la investigación, promoción y control sanitario. Estos centros, se engloban dentro de los Hospitales y determinados Centros de Salud. Por el contrario, los Centros de Transfusiones, cuyo objetivo es promoción y provisión de un punto de donación, transferencia y abastecimiento de sangre, son centros independientes y regionales. Del mismo modo, se disponen de los nodos territoriales, los cuales se encargan de tareas administrativas y de gestión del territorio.

2.3. Acceso a la Información

Para acceder a la información o a los datos de una organización, es necesario que los usuarios se conecten a la red. Para ello, existen varios mecanismos para proveer de este acceso, pudiendo agrupar según el método en el que acceden a la red. Así pues, es posible diferenciar si se producen vía Inalámbrica, Cableada o Remota.

La securización de los accesos que se producen a la red es de vital importancia ya que son la puerta que permite acceder a la información que, dependiendo del entorno, puede ser crítica. Ataques como Man-in-the-Middle, MAC Spoofing o ARP Spoofing, se aprovechan de la falta de securización en estos accesos.

2.3.1. Accesos Inalámbricos

Este tipo de accesos han ido cogiendo notoriedad con el paso del tiempo, ya que permite la movilidad de los usuarios dentro de una infraestructura

determinada. Entre las tecnologías que proveen de este mecanismo, se encuentran NFC (Near Field Communication), RFID (Radio Frecuency Identification), Bluetooth y WiFi (Wireless Fidelity) entre otros, tal y como refleja la Figura 3. NFC, RFID y Bluetooth suelen ser empleados en entornos sanitarios para logística, geolocalización de equipamiento, transferencia de información a corto alcance, etc. y generalmente, tienen sus propias estaciones base con las que se comunican. Por otro lado, la tecnología WiFi, cada vez más extendida, ofrece la posibilidad de tener puestos de usuarios e incluso estaciones de trabajo móviles.

Figura 3. Tipos redes inalámbricas

Con frecuencias de operación en las bandas de 5GHz (Banda a) y de los 2,4GHz (Banda b/g/n), la tecnología WiFi permite actualmente tasas de transferencias de 300Mbps en un medio broadcast, con un límite teórico de hasta 600Mbps. No obstante, estas cifras son ideales, puesto que se ve muy influenciado por el medio, es decir, reflexiones, materiales, etc.

Para el acceso vía WiFi, es necesario un punto de Acceso o AP, que haga como receptor de las señales y sea el nexo de unión con una controladora WiFi, que bien puede estar incorporada en el mismo dispositivo o puede encontrarse centralizada, permitiendo un diseño compuesto por varios AP que dan cobertura a toda la infraestructura.

2.3.1.1. Seguridad en accesos inalámbricos.

A la hora de securizar los accesos vía WiFi, se ha de tener en cuenta dos factores, la autenticación del usuario y la securización del canal. En cuanto a la autenticación del usuario, esta puede ser abierta, por 802.1x, empleado también en accesos inalambricos y que se basa en una autenticación cliente servidor los cuales intercambian la información requerida para dar acceso al puerto o Preshared Key (PSK), una contraseña preestablecida y compartida. Así pues, aunque 802.1x es considerado el método más robusto, no todos los clientes lo soportan. Es por ello, que en estos casos se requiere la implementación de PSK y para complementarlo, y dotar de mayor robustez, se lleva a cabo un control por el Control de Accesos al Medio (MAC).

En cuanto a la securización del canal, se realiza mediante cifrado del mismo. Este cifrado puede ser mediante Wired Equivalent Privacy (WEP) que es el estándar más antiguo definido en el IEEE 802.11 y menos seguro, Wireless Protected Access (WPA) o su segunda versión WPA2,

que son las evoluciones del WEP. Se ha visto que es más seguro WPA2, ya que soporta bloques de encriptación mucho mayores que WPA cuyos bloques son de 256 bits, haciendo uso de encriptaciones Advanced Encryption Standard (AES), mientras que WPA usa Temporal Key Integrity Protocol (TKIP).

Cabe anotar que la seguridad en redes inalámbricas son más bajas que la seguridad en redes cableadas y supone un riesgo muy grande de seguridad [14]. Esto es debido al nivel de exposición que sufren este tipo de redes.

2.3.2. Accesos Cableados

Es el acceso más común y requiere de una conectividad física en la red para poder acceder a la información. Generalmente, estas conexiones se realizan a través de un adaptador RJ45 y cable de cobre, pero es cada vez más habitual que las estaciones de trabajo, servidores, etc, tengan posibilidad de conectarse a través de fibra óptica, delegando las conexiones de cobre a equipos como PCs de usuario, Telefonía VoIP, Impresoras, etc.

El acceso de estos dispositivos es por conexión directa a la red a través de los switches de acceso, que pueden tener comunicaciones a full-duplex o a half-duplex, dependiendo de si la comunicación es bidireccional de manera simultánea o secuencial. Así pues, la velocidad de transmisión varía según las capacidades de la tarjeta de red o también del cableado a emplear, siendo común el uso de cables de categoría 5e y 6, siendo este último el estándar actual, que puede alcanzar hasta 1Gbps con un ancho de banda de 200MHz que beneficia las aplicaciones tipo streaming.

2.3.2.1. Seguridad en accesos cableados

Antiguamente se tenía como creencia generalizada que las amenazas proveían del exterior y el enfoque de seguridad consistía en la protección del perímetro de la red, confiando ciegamente en la red interna. No obstante, con el paso del tiempo esta confianza en la propia red se ha ido perdiendo a consecuencia del creciente BYOD (Bring your own device) [6], tendencia que consiste en que los empleados tengan acceso directo a los recursos de la red con sus propios equipos personales, creciendo la necesidad de implementar seguridad en el acceso físico. De igual modo, estos accesos en muchas ocasiones son los más descuidados, dado que se confía en la propia vigilancia y ética de los usuarios. Es por ello, que se hacen uso de mecanismos como 802.1X o control de MACs, para evitar el acceso no autorizado mediante el medio físico.

Además, al igual que se puede aplicar en la WiFi, es recomendable la restricción de los propios accesos a tener una visión más restringida de la red mediante la segmentación con Virtual Local Area Networks (VLANs). Si

se requiere mayor nivel de securización, se puede dotar de un NAC (Network Access Control) Server, los cuales son capaces de combinar varias técnicas para permitir el acceso. Por ejemplo, pueden comparar la huella o fingerprinting DHCP, con la MAC y el certificado y tomar acciones al respecto, como aislar de la red o asignar una determinada VLAN.

2.3.3. Accesos Remotos

Con el fin de comunicar las diferentes sedes que disponía una empresa, surgieron las comunicaciones con líneas dedicadas y las comunicaciones a través de internet tal y como se muestra en la Figura 4. El potencial de este tipo de accesos era tal, que el propósito inicial de comunicación entre las sedes de una misma organización evolucionó hasta llegar a ser un método de acceso más a la red desde una ubicación ajena a la organización.

Así pues, con las líneas dedicadas surgieron las llamadas líneas Punto a Punto o P2P, que serían empleadas para la comunicación entre empresas, generalmente para soporte remoto. Estas comunicaciones son soluciones que actualmente se encuentran en desuso, puesto que requería de equipamiento dedicado y de contratación de una línea con un Proveedor de Servicios de Internet (ISP), con lo que los costes eran elevados en comparación con otras soluciones existentes.

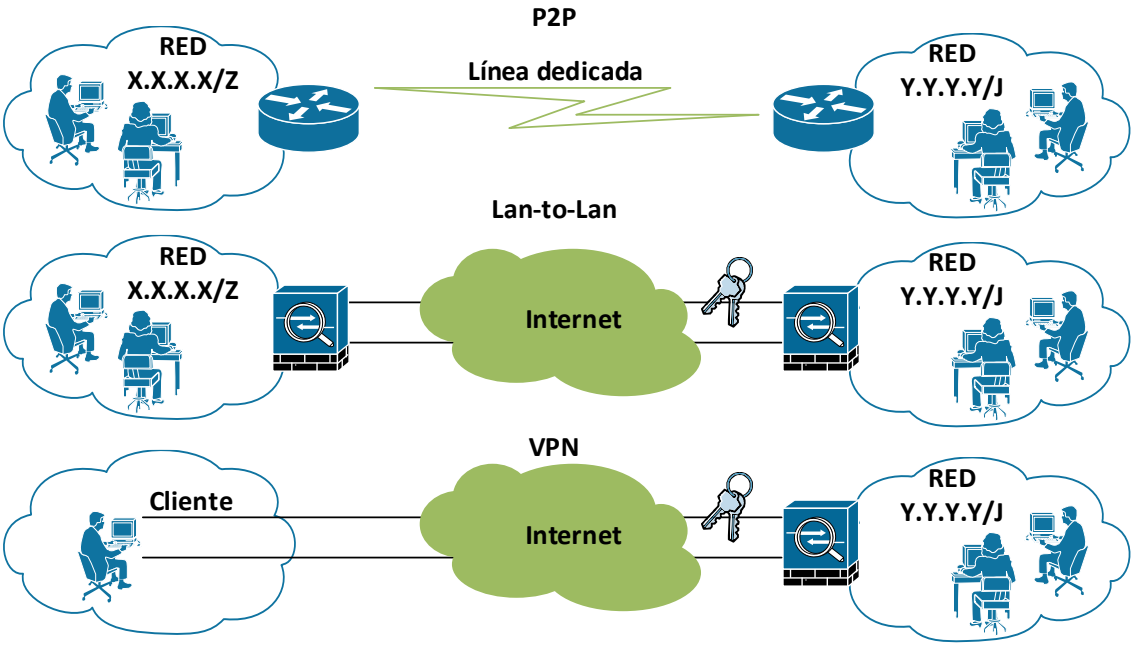

Figura 4. Tipos de accesos remotos

Del mismo modo, surgieron las comunicaciones a través de internet o redes no confiables, como las VPNs o las Lan-to-Lan (L2L), que permiten acceder de manera remota a la red, haciendo uso del medio disponible para acceso a Internet. Como su nombre indica, las L2L son empleadas para comunicación entre dos Local Area Networks (LANs) y se realiza a través de internet por medio de la comunicación entre dos dispositivos o “peers” que se

encuentran vinculados, conectando de este modo dos sedes. En cambio, las VPNs suelen ser empleadas como una comunicación cliente-servidor, sirviendo como acceso a usuarios que requieren de accesos remotos puntuales. En ambos casos, es requisito que el uso de un concentrador VPN, que permita la tunelización del tráfico [2]. Cabe destacar, que está creciendo la tendencia de emplear los accesos L2L para comunicaciones a través de operadoras móviles mediante el Access Point Name (APN), permitiendo sustituir las comunicaciones VPNs cuando estas se requieren desde un dispositivo móvil.

2.3.3.1. Seguridad en accesos remotos

El gran inconveniente de las conexiones entre sedes remotas es que no sabes el camino que toma el tráfico para circular de una sede a otra y, por lo tanto, si pueden interceptar la información o no. Para solventarlo, las líneas P2P dedican líneas entre las sedes y en el caso de las VPN y L2L encriptan el tráfico. Esta encriptación, puede variar según el tipo de túnel establecido entre Secure Sockets Layer (SSL) [VPN] e Internet Protocol Security (Ipsec) [VPN y L2L].

El protocolo SSL y TLS (Transport Layer Security) es comúnmente usado para encapsular y securizar web-sites bajo protocolos web, mediante criptografía simétrica y asimétrica con el uso de claves públicas y privadas. No obstante, en el caso de las VPNs, aunque el funcionamiento es el mismo, normalmente encapsula protocolos no-web como FTP (File Transfer Protocol), RDP (Remote Desktop Protocol), etc. En el caso de IPsec, consiste en una combinación de protocolos como Internet Key Exchange (IKE), para autenticar los peers, intercambio de claves y negociar la encriptación; Authentication Header (AH), que contiene la cabecera de autenticación para verificar la integridad de los datos; o Encapsulating Security Payload (ESP) que es el payload encriptado o canal de datos.

2.4. Gestión del tráfico

Al principio, las aplicaciones que usaban internet y ofrecían servicios de red eran escasas. Las más populares eran accesos a la web, correo electrónico o transmisión de archivos. Estos servicios, por sus características no se veían especialmente afectados por el retardo o la pérdida de paquetes. Por ese motivo, se daba el mismo trato a todo el tráfico que circulaba por la red, mediante la clase de servicio Best Effort, es decir, todo tiene la misma prioridad.

Con el auge de estas tecnologías, se ha incrementado tanto el número de aplicaciones que explotan los recursos de la red de comunicaciones como las exigencias de las mismas, requiriendo un tratamiento específico del retardo, la perdida de paquetes, ancho de banda y disponibilidad. De este modo, surge la necesidad de actualizar el diseño de las redes para así

satisfacer los nuevos requisitos. Este rediseño se podría resolver mediante un sobredimensionado de la red, pero el inconveniente de este es el desaprovechamiento parcial de los recursos, además de que se trata de una solución temporal, puesto que, como anteriormente se ha comentado, la tecnología de redes se encuentra en un continuo crecimiento. Otra manera, es mediante una gestión de forma eficiente de los recursos de red disponibles, para ello primero se ha de separar los distintos tipos de tráfico que transitan en la red y así posteriormente otorgarles un tratamiento haciendo uso de distintas herramientas [9].

Desde el punto de vista de la red de una empresa, es crucial asegurar que se suministran los recursos necesarios a los servicios ofrecidos a empleados, empresas asociadas y ciudadanos, de modo que en cada instante estos recursos se puedan adaptar a las exigencias.

Cuando se habla de Calidad de Servicio o QoS, se hace referencia a la posibilidad que tiene la red a la hora de otorgar el mejor tratamiento necesario al tráfico que circula y que funcionan al mismo tiempo con distintos tipos de tecnologías [10]. El tipo de tratamiento que se pretende dar es el manejo de un ancho de banda especifico, la reducción significativa de pérdidas de datos, evitar las saturaciones y en caso contrario su gestión, realización de Shaping o espaciado del tráfico de red y la asignación de prioridades a este de modo que la calidad de experiencia (QoE) de usuario se ve incrementada. Todo ello teniendo en cuenta el ancho de banda total disponible en la red, ya que la Calidad de Servicio no contempla la posibilidad de su ampliación. La Figura 5 refleja de manera visual la definición de QoS.

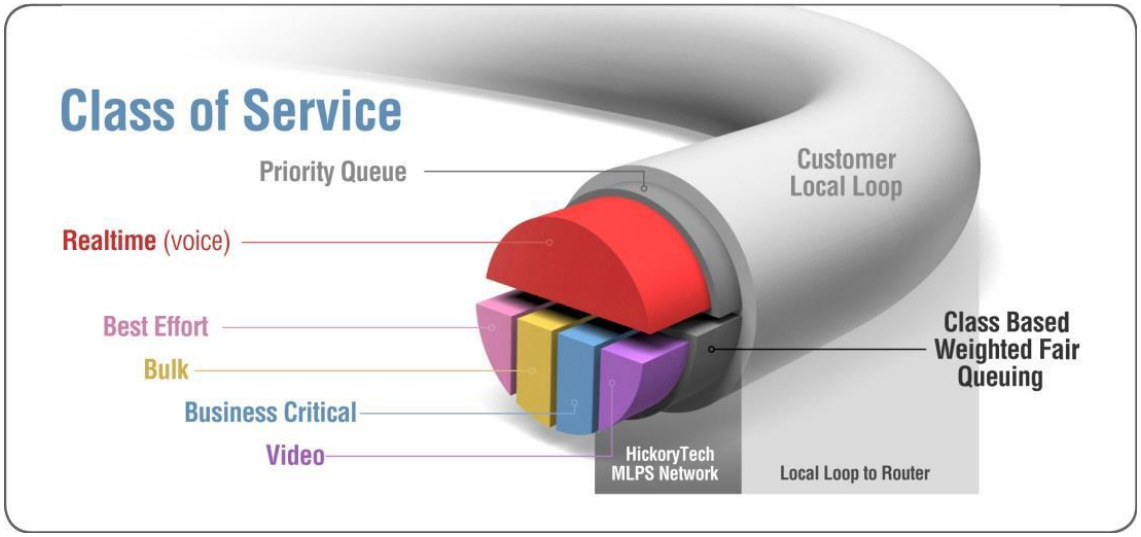

Figura 5. Representación gráfica de la Calidad de Servicio [4]

Como ya se ha mencionado, en general en los distintos tipos de redes, se distribuyen los paquetes siguiendo un modelo de tratamiento, el Best Effort, cuyo significado en la práctica en servicio de tráfico seria “todo lo que se pueda, lo antes posible”. Al darse este modelo para todo tipo de tráfico a lo largo de la red, sería muy probable que llegara a producirse una congestión donde se retrasarían o descartarían los paquetes, haciendo una red muy

poco escalable. No obstante, para distintos tipos de servicios o aplicaciones, no es aceptable la posibilidad de que suceda este caso.

Una posible solución para evitar este problema podría ser contratar más ancho de banda. Pero es una solución ineficiente, ya que el tráfico viene dado por distintos husos horarios y podría darse de igual modo el caso de congestión, debido a un uso exigente de distintos tipos de tráfico durante un instante específico, además que uno de los objetivos del presente proyecto es de evitar la ampliación de contrato de Ancho de Banda. Por lo que la solución más eficaz reside en dotar a la red de “inteligencia”, mediante mecanismos de Calidad de Servicio. La ventaja de usar QoS es añadir previsibilidad a los servicios en ancho de banda, pérdida de paquetes y retrasos. De este modo se introduce como objetivo la cuantificación de tratamiento que un paquete debe obtener en su transcurso por la red.

2.5. Tipos de arquitectura de red

Previamente al despliegue de configuraciones o equipamiento necesario para construir una red de comunicaciones, es necesario realizar un diseño. Este diseño, vendrá determinado por unos objetivos y requisitos específicos según criterios del usuario, la economía, criticidad o el tamaño de la red y los servicios que se ofrecen.

2.5.1. Redes convencionales

Las redes convencionales o legacy, se componen generalmente de equipamiento de red, cuya capa de control y de datos se encuentran bajo el mismo hardware. Así pues, los diseños físicos y lógicos eran muy similares, tendiendo el diseño de las aplicaciones a la arquitectura de red.

Atendiendo a edificios o sedes, es posible encontrar dos modelos de diseño, que se han convertido en referentes que atienden a disponibilidad, flexibilidad y escalabilidad, que son la arquitectura a tres capas y arquitectura de Core compacto.

El modelo de tres capas, es una arquitectura típica para conseguir grandes prestaciones, alta disponibilidad y un diseño totalmente escalable. Este tipo de diseño, simplifica su implementación y gestión dado que cada capa va destinada a una función específica. Cada capa del modelo tiene asignado un rol y su estructura es jerárquica, interconectando cada capa a su superior [12].

En redes, un cambio puede afectar a un gran número de sistemas, ya sea por un cambio de topología o una tormenta de broadcast. El diseño jerárquico, permite restringir los cambios operacionales a una determinada VLAN, con lo cual, favorece su gestión ante incidentes.

De esta arquitectura, representada en la Figura 6 se distinguen las siguientes capas:

- **Capa de acceso:** Provee a equipos y usuarios finales de acceso directo a la red.
- **Capa de distribución:** Agrega las capas de acceso y provee de conectividad a los servicios.
- **Capa de Core:** Provee de conectividad entre las distribuciones de grandes entornos LAN.

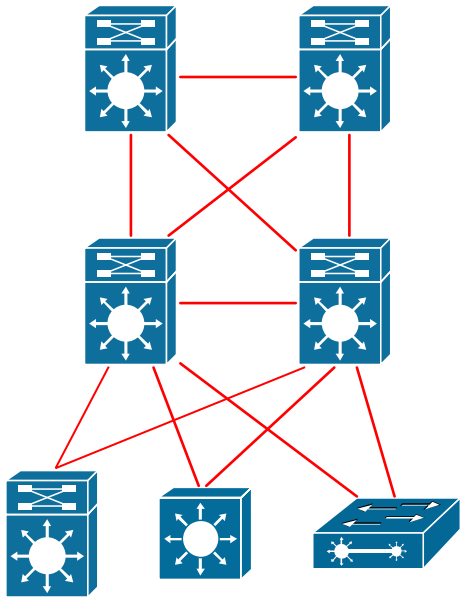

Figura 6. Arquitectura de tres capas

Cada capa dispone de diferentes funcionalidades en la red. La capa de acceso es donde los usuarios se conectan a la red, con lo que provee de comunicación cableada e inalámbrica y es donde se implementan servicios de seguridad de acceso o segmentación y control de los distintos tipos de tráfico. Así pues, esta capa suele componerse por la capa II del modelo Open Systems Interconection (OSI), interconectando los dominios broadcast y provee de segmentación de grupos de usuarios, aplicaciones y otros equipos.

A su vez, debe de asegurar que la red está disponible para todos los usuarios que lo necesiten, cuando lo necesiten, protegiendo a los usuarios de errores humanos o ataques. Esto se consigue mediante la identificación de los dispositivos y asegurando que tienen acceso únicamente a lo que su rol compete.

En una red donde la comunicación necesita que sea end-to-end, atravesando diferentes capas de acceso dentro de la misma LAN o desde otra sede a través de la Wide Area Network (WAN), la capa de distribución facilita esta comunicación. Así pues, otorga escalabilidad ya que se trata de un agregador de múltiples capas de acceso. Además, puede ser muy eficiente, requiriendo poca memoria si se crean varios dominios que segmenten los fallos ante cambios en la red. Esto se debe a que es el terminador de dominios de broadcast de capa II que se inicia en la capa de

acceso. De igual modo, añade redundancia a la distribución con lo que se obtiene alta disponibilidad y dos caminos con el mismo coste hacia el Core. Entre sus funciones, puede proveer de switching, routing y de políticas de acceso a la red, así como añadir clasificación de servicios y otorgar a prioridades a los mismos (QoS).

A la hora de comunicar las diferentes ubicaciones geográficas, se dispone de la capa de Core. Este agrega todos los switches de distribución de los diferentes edificios y se encarga del acceso entre el interior y el exterior de la red. A su vez, se caracteriza por la rapidez, escalabilidad, disponibilidad y bajas latencias en la comunicación. Del mismo modo, esta capa destaca por reducir la complejidad de la red cuando existen múltiples switches de distribución, puesto que la cantidad de enlaces se reduce de N*(N-1) a N enlaces para N switches de distribución, tal y como muestra la Figura 7.

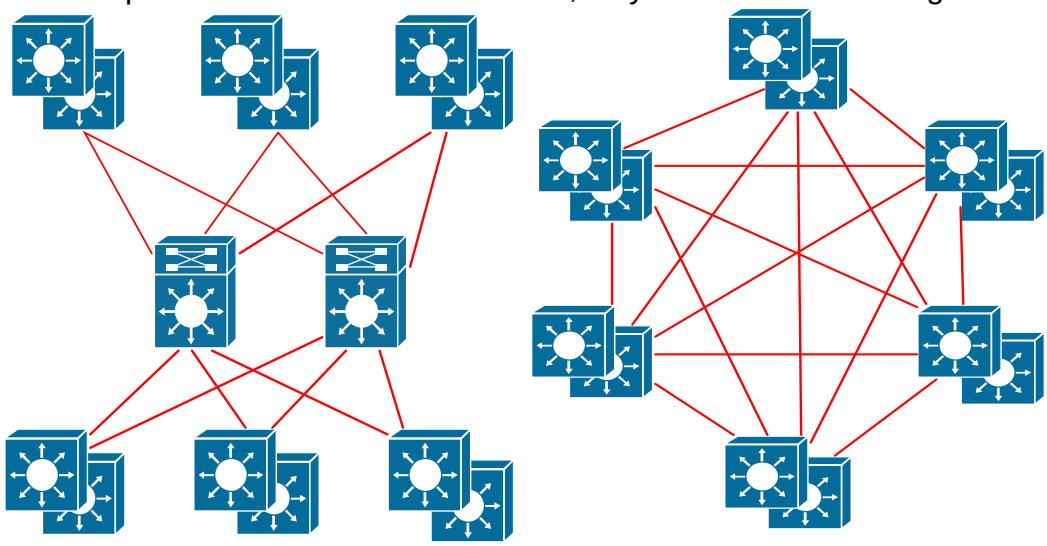

Figura 7. Reducción enlaces con Core compacto

No obstante, hay sedes cuyo crecimiento a lo largo del tiempo es prácticamente despreciable, por lo que es posible sacrificar en escalabilidad, pudiendo servir un modelo de dos capas. Este modelo en el que el Core y distribución conviven en una sola capa, es lo que se llama Core compacto. La principal motivación para un Core compacto es la reducción de costes, mientras se mantienen la mayor parte de los beneficios de una arquitectura a tres capas [13].

El desarrollo de una red con Core compacto, agrupa la distribución y el Core en un único dispositivo, con lo cual se dispone de altas velocidades de acceso a la red, agregación de la capa II, definición de rutas y políticas de red y características de tratamiento de la información como QoS o Virtualización, en un solo dispositivo.

2.5.2. Redes de nueva generación

El paradigma de las arquitecturas convencionales es que los planos de control y de datos se encuentran bajo un mismo equipo hardware y por tanto

las decisiones de enrutamiento y encaminamiento de los datos se deciden en el propio dispositivo. En la Figura 8 se visualiza la ubicación de los planos de control y datos y su relación con las aplicaciones. Sin embargo, cuando se han de configurar múltiples dispositivos simultáneamente para ofrecer unos servicios determinados, es necesario que un operador de red o un script programe estos cambios. Cuando se ha de realizar todo un cambio de topología para adaptarse a los recursos de red que requiere una determinada aplicación, el trabajo de cambio de configuraciones puede volverse un trabajo poco flexible.

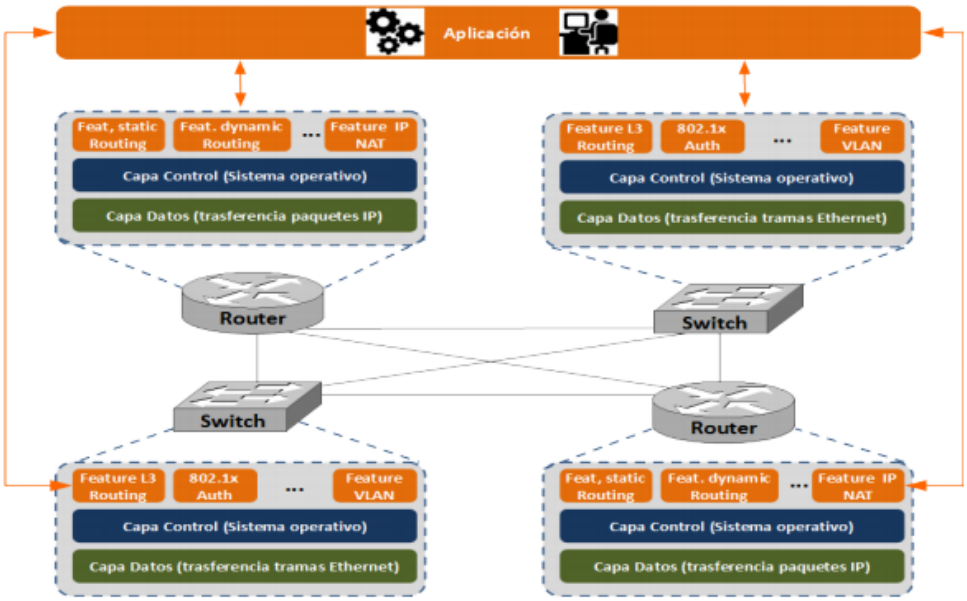

Figura 8. Plano de control y de datos de arquitecturas convencionales [7]

Así pues, con la evolución tecnológica y la promoción de nuevos servicios como el LTE (Long Term Evolution), las operadoras empiezan a ofrecer los primeros servicios que se encuentran directamente integrados en el firmware, naciendo IMS (IP Multimedia Subsystem) y por lo tanto SDN (Software Defined Network), permitiendo la automatización y orquestación de los servicios de red. Surge entonces un cambio de paradigma, separando los planos de control y de datos, haciendo que el primero no se ejecute en el hardware. Este plano de control se gestiona a través de un servidor remoto junto con la capa de aplicación, es lo que se conoce como controladora. [7]

2.5.2.1. SD-WAN

Una modalidad de redes SDN es SD-WAN, la cual aplica esta tecnología en las redes WAN. Esta combinación permite adaptar la red al negocio, añade flexibilidad a la red, aumentar la velocidad de despliegues y mayor control sobre los recursos, sobre conectividades 4G, MultiProtocol Layer Switching (MPLS) y VPN.

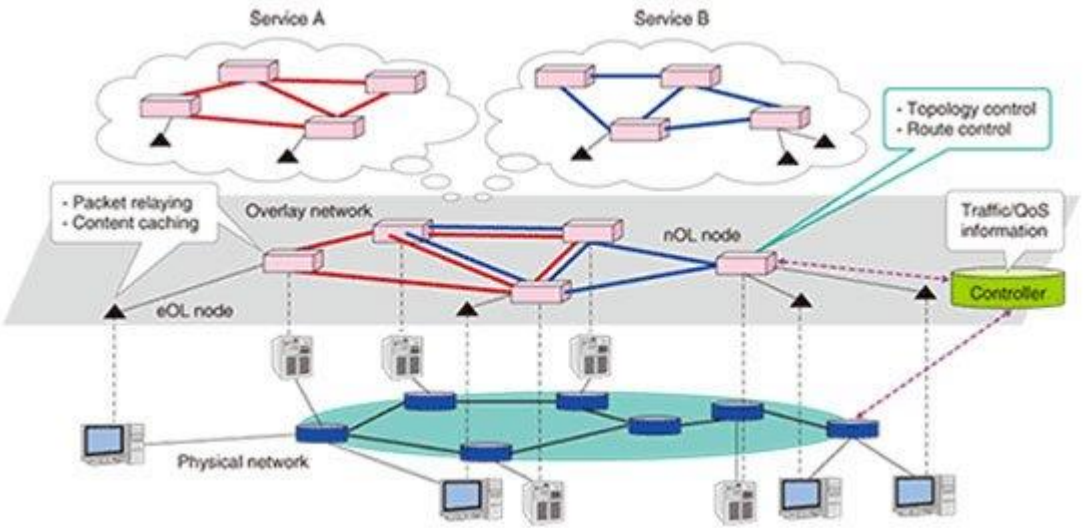

Figura 9. Red overlay y underlay en SD-WAN

Para satisfacer estas demandas, se ha añadido el concepto de superposiciones de red o overlay. Este concepto, ligado al paradigma SDN, cambia la visión de red física a red lógica. Una red underlay, es una infraestructura física sobre la cual se construye la overlay o la red virtual mediante túneles [3], tal y como se refleja en la Figura 9.

Tal y como concluye J del Olmo, “Mediante la virtualización de redes se consigue abstraer la solución SD-WAN de la conectividad física que va por debajo, dando posibilidad de implementar soluciones más versátiles y empleando múltiples tipologías de accesos y anchos de banda” [5]. De modo que se completan las virtudes de las tecnologías MPLS con LTE y poder usar ambas indistintamente según el estado de la red o prioridad del servicio.

2.6. Monitorización y trazabilidad

Uno de los aspectos más valorados por los administradores de redes y que resultan fundamentales para el correcto desarrollo de su trabajo, es la trazabilidad. La trazabilidad se define como la capacidad de poder seguir el flujo de tráfico de la red, desde el inicio hasta el fin. Esto se consigue con la adecuada elección de los puntos de monitorización y las herramientas a emplear. En caso de no realizar un estudio previo, es muy probable que la monitorización se sobredimensione, disponiendo de múltiples herramientas que solapen las funcionalidades dificultando aún más las tareas de administración; o se infradimensione, con lo cual ante una incidencia de obtención de información del tráfico no se consigan todos los datos deseables.

En redes críticas, la seguridad depende en gran parte de una correcta trazabilidad de la información y la monitorización de las infraestructuras de red. Tal y como indica Ponemon en el coste de las brechas de datos en 2018, se ha visto aumentado hasta alcanzar los 3’86 millones en comparación con los 3.62 millones del año pasado, donde las

organizaciones han tardado una media de 196 días en detectar la brecha de seguridad [11], como refleja la Figura 10, con lo cual implica un gran riesgo de seguridad. Además, estas herramientas deben ser capaces de interpretar los logs, de manera que se produzca una alerta ante la detección de anomalías de red. Así pues, con las herramientas correctas es posible minimizar el tiempo medio de detección y reacción.

Como herramientas de monitorización y logs es posible encontrar varias en el mercado que van destinadas a diferentes propósitos. En el caso de monitorización del equipamiento de red destacan herramientas como Zabbix, Nagios o CA Spectrum, las cuales son capaces de generar alertas ante caídas de equipos, interfaces o por superación de umbrales previamente definidos por el usuario. Por otro lado, como gestión de logs destacan soluciones como splunk, graylog o ELK Stack, que son idóneos para gestionar los registros de logs de los diferentes servicios y poder detectar anomalías en las consultas a los servicios. Finalmente, en cuanto a análisis de tramas y paquetes, el software que destaca es wireshark el cual es un referente para troubleshooting de tráfico.

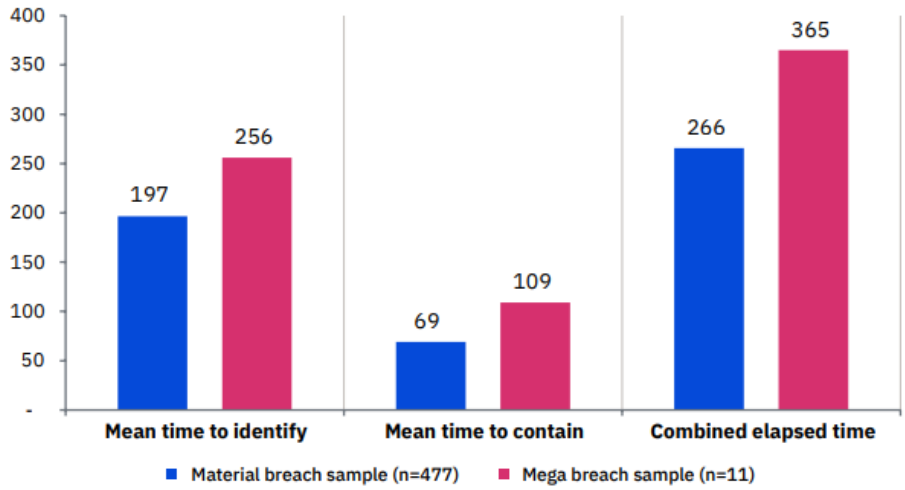

Figura 10. Tiempos de respuesta ante amenazas estudio Ponemon. [11]

Resumen del capitulo

A lo largo del capítulo se ha realizado una primera aproximación a temas clave que serán abordados a lo largo del proyecto. En primer lugar, se ha realizado una breve descripción de la Organización Ox, dando unas pequeñas pinceladas del diagrama de bloques de la organización, así como de los principios en los que se basa los modelos actuales de los Hospitales. De este modo, se prosigue indicando los tipos de sedes existentes, que como se verá más adelante, servirá de referencia para comprender la clasificación por tipologías que se realiza en la organización. Este apartado sirve de referencia para comprender el funcionamiento de la organización, objetivo y su función [O1].

Tras describir brevemente la estructura de la organización, se procede a definir los diferentes tipos de accesos es posible encontrar en cualquier organización, así como las particularidades a nivel de seguridad que tienen y servirá como orientación para determinar los riesgos en los accesos durante el análisis.

Se prosigue de este modo a describir los mecanismos de gestión del tráfico, introduciendo el concepto de Calidad de Servicio, como método de optimización de los flujos de tráfico y que repercute directamente a la calidad de experiencia de los usuarios, siendo este uno de los objetivos principales de diseño del modelo.

Así pues, se da paso a un análisis de las principales arquitecturas que pueden darse en redes de comunicaciones y que, conjuntamente con la gestión de tráfico, permite garantizar y adaptar las comunicaciones a las características del servicio. De este modo clasificamos en redes convencionales y redes de nueva generación, donde se presenta el concepto de SD-WAN, que puede ser de utilidad para la solución MacroLan de la red.

Por último, se ha recopilado las principales herramientas que son empleadas según el propósito al que va destinada, alertando de la importancia de una monitorización adecuada para mejorar la gestión, aumentar el conocimiento de la red y disminuir los tiempos de respuesta ante incidentes.

3. Análisis de la red

A lo largo del siguiente capítulo y tomando como referencia los conceptos vistos en anteriormente, se realiza un análisis de las características típicas de red y como se ajustan las soluciones existentes, como trabajo previo al diseño. El análisis se realizará contemplando la arquitectura de la red, como la base de cada tipología de sede. De igual modo, se detallarán las soluciones tecnológicas a utilizar. Una vez analizadas las partes técnicas de la red, el capítulo prosigue con el análisis de la estructura implementada y del tráfico de la red.

3.1. Arquitectura de la red

Los elementos de la red de área extensa, dan cobertura a todos los centros pertenecientes a la Organización Ox en el ámbito geográfico de la Comunidad Autónoma. Existen dos tipos de redes:

- **Red MacroLan/VPN-IP para tráfico interno.** Une todos los centros o sedes de una misma Organización, por tanto, existe una red de este tipo por cada Organización. En el caso de la Organización Ox, su red interna es la red Xenon.
- **Red IP-Gigabit para tráfico externo**. Se trata de una única red que une todas las Organizaciones de la Comunidad Autónoma y sirve de salida a Internet y a la red Interministerial.

3.1.1. Red MacroLAN

En general, la red MacroLAN interconecta todos los edificios administrativos y asistenciales de la Ox pertenecientes a la red de la Comunidad Autónoma a través de infraestructura propia. Cada uno de los edificios conectados constituye lo que se denomina un nodo de red.

Existen 1292 sedes o nodos que constituyen en la actualidad la red Xenon, supone en la práctica 36761 líneas de usuario, pudiendo generar un tráfico de hasta 2Gbps. Estos nodos se clasifican según su criticidad en tres tipos como se muestra en la Tabla 3, de manera que, para cada grupo, se fijan unos niveles de servicio a proporcionar. Estos niveles de servicio vienen limitados, en el caso de algunos elementos, por los niveles ofrecidos por el propio operador de telecomunicaciones de la Comunidad Autónoma.

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	582

		administrativos. >20 usuarios	
Tipo III	Principal de 1 Gbps fibra óptica, Backup acceso mediante ADSL	Centros de Salud y Centros administrativos. <20 usuarios	686

Tabla 3. Clasificación tipología de sedes según localización.

La red Xenon está implementada como una red MPLS entre todos los nodos tal y como muestra la Figura 11, es decir, solo los nodos que pertenecen a la región pueden conectarse con el Hospital directamente y Para hablarse entre sí, es necesario pasar por el Hospital. En caso de acceder al exterior de la Ox y al CPD centralizado, lo hacen a través de los nodos territoriales, que a su vez conectan con nodo del Centro de Informática atravesando diversos firewalls perimetrales que garantizan la seguridad de las comunicaciones. De este modo en la Figura 11 se distinguen cuatro tipos de Nodos:

- **Nodo trocal**. Es el núcleo de toda la red Xenon y único punto de acceso entre Internet y Xenon. Es el núcleo de la red principal y de Backup. Concentra las líneas punto a punto de los nodos de enlace de la provincia. Concentra las líneas de los nodos provinciales.
- **Nodos provinciales.** Ocupan el segundo nivel de jerarquía de la red Xenon. Recogen todo el tráfico de sus nodos de enlace. Conexión de 1Gbps de entrada y de salida con el nodo troncal (exceptuando el nodo de la región central que forma parte del nodo troncal).
- **Nodos de enlace.** Ocupan el tercer nivel de jerarquía de la red Xenon. Recogen todo el tráfico de sus nodos de acceso. Están instalados en los hospitales departamentales. Disponen de una conexión de 1Gbps de entrada y de salida con su nodo provincial para la línea principal.
- **Nodos de acceso**. Representan el nivel inferior de la red Xenon. Proporcionan el servicio a todos los centros asistenciales de la Organización Ox como hospitales, centros de salud, consultorios auxiliares y de verano, centros de especialidades, unidades de conductas adictivas, direcciones territoriales, inspecciones médicas, unidades de prevención, etc.

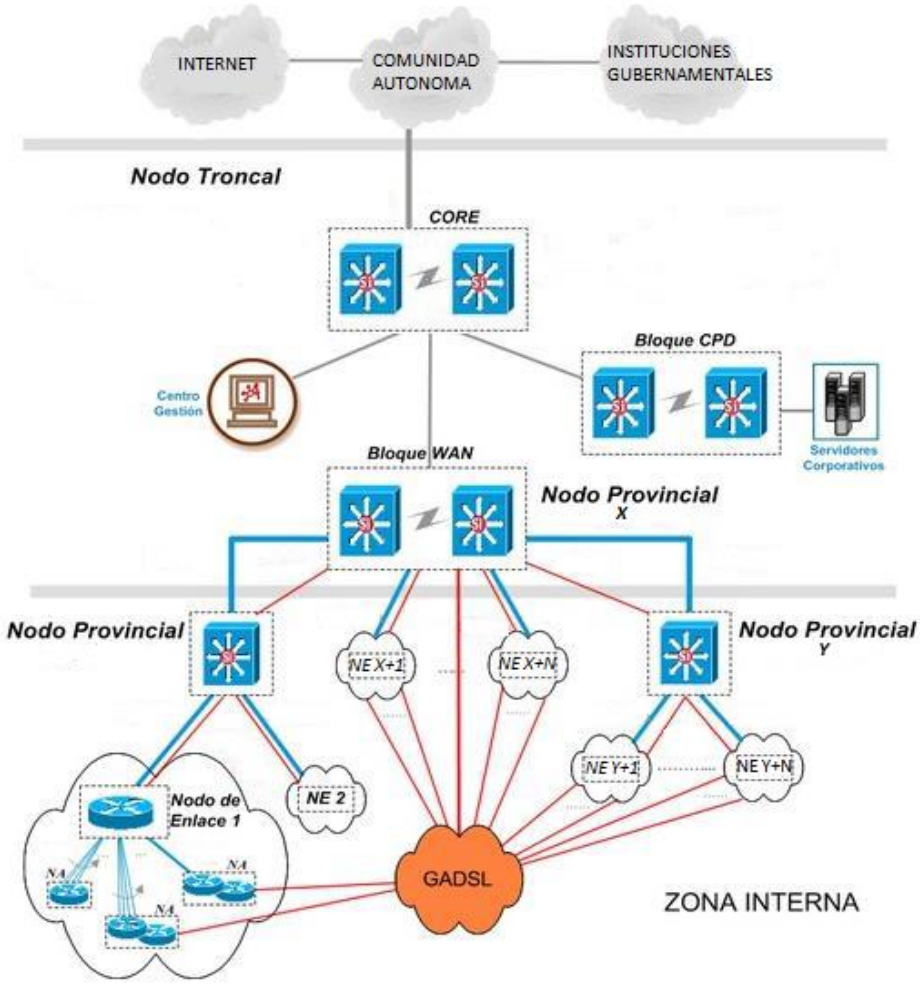

Figura 11. Tipos de nodos que componen la red Xenon

3.1.2. Redes de Área Local

Los elementos de red incluidos en el ámbito de las redes de área local proporcionan conectividad a todos los puestos de trabajo, servidores, impresoras, telefonía, equipos de radiodiagnóstico, etc. Es decir, proporcionan conectividad, cableada o inalámbrica, a cualquier sistema que lo requiera, en cada una de las sedes de la red Xenon.

En el caso del Centro de Informática, hospitales y demás centros de referencia se cuenta, además, con firewalls y electrónica dedicada para dar conectividad a los servidores que alojan todas las aplicaciones departamentales y centralizadas de la Organización Ox.

Actualmente se está dando servicio a usuarios y aplicaciones a través de 4277 dispositivos de red.

3.1.2.1. Sedes de tipo I

3.1.2.1.1. Modelo de Centro de Informática

En cuanto al Centro de Informática, el diseño por bloques difiere del resto de sedes. Tal y como se muestra en la Figura 12 destacan 4 bloques que son multifuncionales:

- **Internet:** Es el bloque por el que circula el tráfico hacia internet, Organizaciones, Comunidades Autónomas y la red Interministerial. Además, se ofrecen los servicios al ciudadano a través de Virtual IPs (VIPs) habilitadas en el firewall perimetral. Al mismo tiempo, el firewall realiza bloqueos a nivel IV. El proxy es el único elemento que permite a los usuarios navegar hacia internet, que a su vez hace funciones de restricción de URLs mediante ficheros .pac. Igualmente, también sirve como punto de entrada de conexiones remotas VPN, L2L y P2P, donde estas últimas se conectan directamente a un switch de nivel II ubicado tras al firewall y las VPN y L2L se establecen contra un concentrador conectado en el mismo switch. Estas conexiones no validan usuarios individualizados, siendo el caso de las VPN usuarios genéricos creados localmente.

- **Core:** Dicho bloque es el núcleo de la red Xenon y enlaza a todos los bloques. Se compone de una pareja de switches de nivel III en activo-activo. Recoge todas las rutas estáticas del Centro de Informática.

- **CPD:** Es el bloque donde se encuentra el CPD de la Organización Ox y por tanto donde se alojan los servicios centralizados. En su perímetro se encuentran en el mismo nivel, tanto un balanceador que ofrecen los servicios como un firewall que protege el acceso a los servidores. Se distinguen la red de servicio que se encuentra en el balanceador y la red de servidores que se encuentra tras el firewall. A su vez, el balanceador dispone de una pata en la red de servidores. Al estar los servidores en una red plana, la comunicación entre servidores es directa. Cabe destacar del CPD, que los test, pruebas de carga, producción y bases de datos, se realizan en el mismo entorno. El firewall actúa a nivel IV, administrando reglas de acceso a los servidores. El balanceador ofrece los servicios publicados a toda la organización, no hay activo ningún firewall previo. La validación por certificados se realiza en el propio servidor mediante Control Revocation List (CRLs). La comunicación dentro del CPD se produce con switches de nivel II, que a su vez se comunican mediante fabricpath, componiendo una malla entre los servidores.

- **Interno:** En este bloque se conecta el personal del Centro de Informática y la MacroLAN. Así pues el acceso del personal del Centro de Informática se realiza mediante WiFi y por red cableada, que es formada por un conjunto de switches de nivel II. Estos switches disponen de control de accesos que está gestionado por un NAC Server que está vinculado a un LDAP (Ligthweight Directory Access Protocol)

corporativo. La red WiFi es accesible con PSK. La VLAN por defecto para todo el personal es la 1 y la 90 para telefonía. Los DNS (Domain Name Server) y DHCP (Dynamic Host Configuration Protocol) se encuentran en este bloque, junto al gestor centralizado de las controladoras.

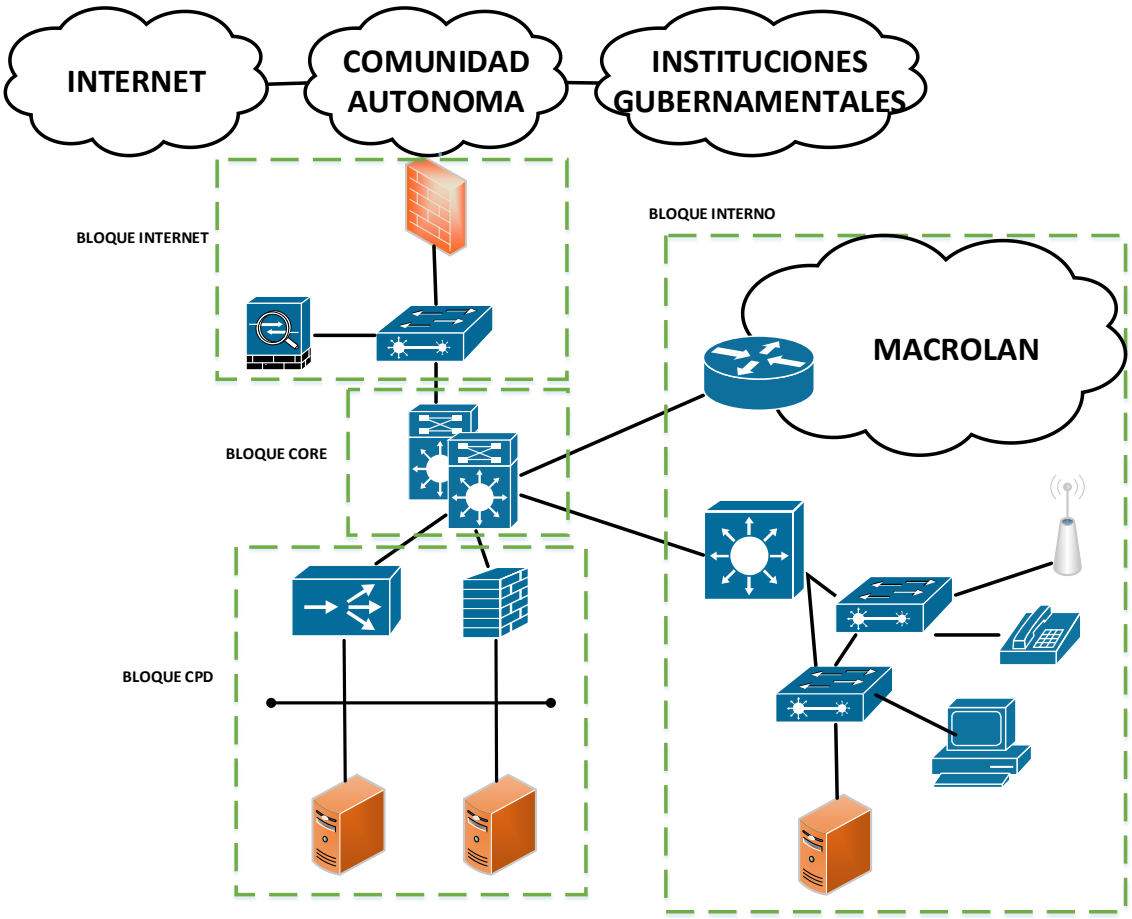

Figura 12. Arquitectura de red Centro de Informática

Cabe destacar que las interfaces se disponen de interfaces a 10G en todos los bloques excepto en el bloque internet, donde se opera a 1G debido a la capacidad de la línea y a que el router Gigabit que enlaza con Internet y el resto de Organizaciones solo tenía interfaces de 10/100/1000. Sin embargo, recientemente se ha modificado la línea bajo un proyecto de ampliación llevado a cabo por el personal de la Organización, aumentando el ancho de banda de salida a 10G, cambiando a su vez el router de enlace.

3.1.2.1.2. Modelo de Hospitales

El modelo de red característico de un centro Hospitalario está dividido en secciones tal y como se muestra en la Figura 13. Donde es posible distinguir los siguientes bloques:

- **CORE.** Este bloque consta de dos Switches de nivel III con puertos GigabiteEthernet. Sirve de unión entre los nodos de los demás bloques del modelo de red y su misión es conmutar paquetes entre los distintos bloques lo más rápidamente posible.

- **WAN+Internet.** Está formado por los routers de acceso a la red Xenon. La funcionalidad de este bloque, es la unión entre el Hospital a la red Xenon y por ende a la red de la Comunidad autónoma y a Internet. La centralita telefónica está conectada a este bloque. La red entre las sedes es una red MPLS administrada por el proveedor, con lo que nuestra visibilidad es nula. No hay tratamiento de tráfico a nivel de calidad de servicio.

- **CPD.** Este bloque lo forman dos capas. Una primera capa de Firewalls que componen el Nivel III del CPD y una segunda capa de Switches de Nivel II donde se conectan las interfaces de los servidores que dan servicio a los usuarios. Está definida una red plana con la VLAN por defecto para que se vean todos los servidores en capa 2 del modelo OSI, sin necesidad de llegar al firewall.

- **LAN Usuarios.** Este bloque está formado por dos capas:
    - ***Capa de distribución.*** Consta de dos Switches de nivel III con al menos tantos puertos GigabiteEthernet de Fibra óptica como armarios en la capa de acceso de usuarios. Cada uno de estos puertos se enlaza con cada uno de los armarios de acceso. En estos switches segmentan la red en 6 VLANs:
        - *VLAN1:* La VLAN nativa y que son asignadas a los usuarios cableados.
        - *VLAN2:* Definida para la gestión del equipamiento de red.
        - *VLAN3:* VLAN que va destinada a la conexión WiFi.
        - *VLAN4:* Destinada a equipamiento de laboratorio y radiología.
        - *VLAN5:* Definida para uso por invitados.
        - *VLAN90:* VLAN para VoIP y Multimedia.

      A su vez se definen instancias de MST en todo el Hospital para las VLANs definidas. Por otro lado, en los switches de distribución se encuentran definidas las ACLs para delimitar los accesos entre VLANs. En estos switches, se encuentra pinchada la controladora que gestiona todos los APs de la sede.
    - ***Capa de acceso.*** Consta de tantos Switches de nivel II o puntos de acceso WiFi, como para dar acceso a los potenciales usuarios del Hospital. En cada armario se unen los Switches de acceso mediante enlaces de cobre formando anillos. Estos anillos pueden ser de 4, 5 y hasta 8 switches. La función de este bloque es dar acceso a los puestos de usuario final a la red del Hospital, bien sea por cable o mediante WiFi. No existe protección de acceso a la red cableada. En cuanto al acceso inalámbrico se produce con PSK única para toda la sede.

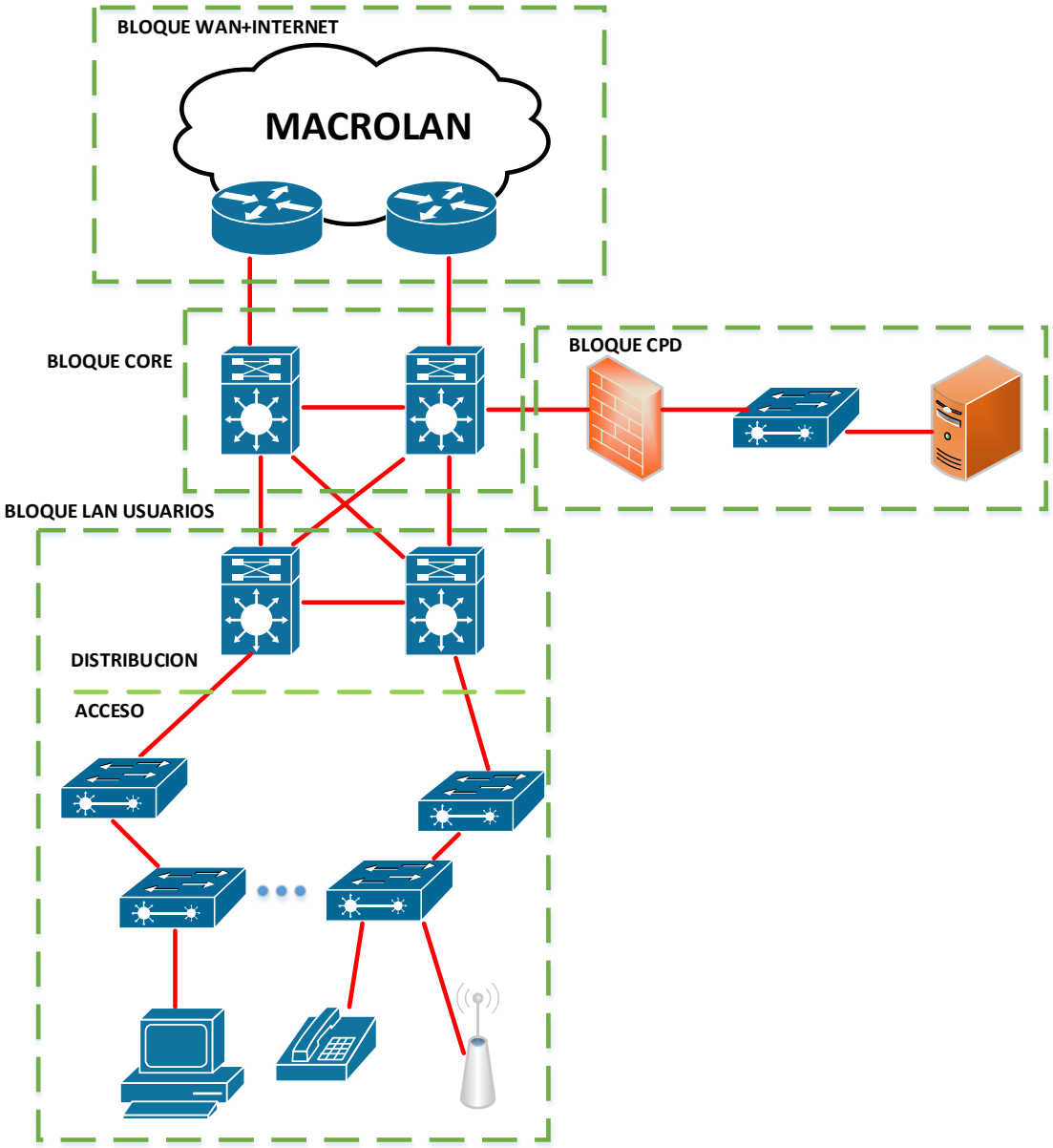

Figura 13. Arquitectura de red Hospitales

Cabe anotar que para acceder a los dispositivos se realiza vía telnet o HTTP. No hay backups de configuraciones. Las interfaces de enlace entre equipamiento son a 10G, siendo las interfaces de acceso a 1G.

3.1.2.2. Sedes tipo II y III

En el caso de las sedes tipo II y tipo III, no hay arquitectura definida. Se encuentran bajo una misma capa de acceso toda la infraestructura de red formando múltiples anillos de hasta 8 switches, tal y como se muestra en la Figura 14. El nivel III se queda en el router de entrada a la sede y se define Spanning-Tree (STP) en todas las sedes. La segmentación realizada es en dos VLANs:

- **VLAN1:** La VLAN nativa y que son asignadas a los usuarios cableados y WiFi.

- **VLAN90:** VLAN para Voz sopre IP (VoIP) y Multimedia.

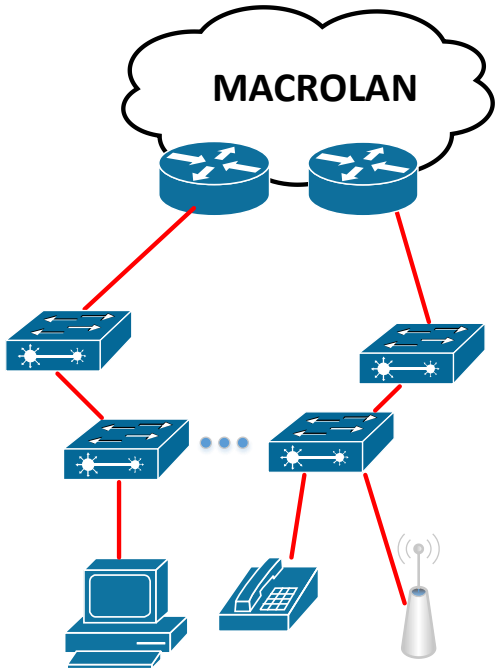

Figura 14. Arquitectura de red en sedes tipo II y III

La administración de los dispositivos se realiza a través de la VLAN 1.
Los APs se encuentran distribuidos por todo el centro con PSK única en toda la sede, siendo esta clave conocida por los profesionales sanitarios.

Al igual que en las sedes tipo I, para acceder a los dispositivos se realiza vía telnet o HTTP. No hay backups de configuraciones. Todos los enlaces son a 1G.

3.1.3. Análisis de monitorización y trazabilidad

Analizando la monitorización y trazabilidad del tráfico, se disponen de dos herramientas de monitorización de la red. CA Spectrum, que es usada por los administradores para gestión de alertas por perdida de servicio de algún equipo de toda la organización Ox, o monitorizar anomalías en CPU, memoria o exceso de tráfico de algún enlace. Así pues, también tienen la herramienta Cacti, que es empleada para almacenar un histórico de los patrones de tráfico de las interfaces de enlace de cada equipo de la red.

Por otro lado, no se dispone de un gestor de logs al uso. Los logs de servicios de red como Proxy, DNS, DHCP, firewalls, controladoras, balanceadores o switches, se almacenan en cada uno de los dispositivos.

Se ha de mencionar, que actualmente la forma de operar ante incidentes que requiera el seguimiento o identificación del tráfico es mediante mirrors de las interfaces a monitorizar, haciendo uso del software WhireShark, en conjunto de los propios logs del equipamiento involucrado.

3.2. Análisis tecnológico

Por motivos de seguridad no se van a indicar modelos del equipamiento. No obstante, se van a destacar las características principales de cada dispositivo con el fin de resaltar el potencial disponible para el posterior diseño.

Es una red heterogénea, habiendo multitud de marcas. Dentro de las sedes tipo II y tipo III, es posible encontrar en una misma red equipamiento HP, 3Com, Cisco, Nortel, Aruba, etc. Así pues, para el correcto convivir de todo el equipamiento se hace uso de protocolos standarizados como Radius, STP, Link Aggregation Control Protocol (LACP), etc.

En el caso de las sedes tipo I, los switches que lo componen se encuentran bajo un mismo fabricante, acercándose a lo que se denominaría una red homogénea.

3.2.1. Tecnología en Centro de Informática

Por otro lado, si se procede a analizar la tecnología que se encuentra en cada uno de los bloques del centro de informática, es posible distinguir los siguientes.

- **Internet:** El firewall del perímetro soporta operar a nivel VII, permiten la creación de zonas, pueden virtualizarse de modo que se disponen de varios firewalls bajo un mismo hardware, pueden hacer inspección SSL, aplicar políticas antivirus, actuar como Intrusion Prevention System (IPS), admiten enrutamiento dinámico y pueden operar en activo-activo real. El proxy es opensource bajo una distribución Linux y es capaz de cachear los accesos de los usuarios. El concentrador VPN es capaz de operar como firewall, puede gestionar políticas dinámicas, asignar y perfilar tuneles en base a certificados, definición de políticas de grupo, gestión de pools de IPs e Integración con LDAP.

- **Core:** Los switches de esta capa disponen de tecnología en Stack, enrutamiento dinámico, creación de Virtual Switch Interface (VSI), First Hop Redundancy Protocol (FHRP) y Virtualización.

- **CPD:** En cuanto al firewall se respeta la doble barrera tecnológica definida en el Esquema Nacional de Seguridad, por tanto es de distinto fabricante que en el bloque internet, no obstante dispone de las mismas capacidades que el anterior. Igualmente, el balanceador de carga se trata de un ADC (Application Delivery Control) el cual tiene capacidad de

operar a nivel VII, opera como acelerador, tiene posibilidad de operar como Web Application Firewall (WAF), puede funcionar como reverse proxy y tiene capacidad de Virtualización. Al igual que en el bloque Core los switches disponen de tecnología en Stack, enrutamiento dinámico, creación de VSI, FHRP y Virtualización

- **Interno:** El NAC Server es capaz de establecer políticas de acceso, validación de usuarios por portal cautivo, aislamiento de usuarios, autoconficuración de los accesos pudiendo asignar la VLAN que corresponda al dispositivo e integración con LDAP y DHCP. El DNS y DHCP disponen de las funciones básicas de este tipo de servicios. Los APs son capaces de funcionar como lightwait y autónomos, además de aceptar varios modos de operación como “flexconnect” para disponer del direccionamiento en la propia sede o “modo local” para irradiar las VLANs definidas en la controladora y comunicarse a través de un túnel CAPWAP. Las Controladoras aceptan protocolos WPA, WPA2, 802.1X y autenticación en local.

3.2.2. Tecnología en Hospitales

En los Hospitales, se procede a realizar un análisis de la tecnología que se halla en cada uno de los bloques.

- **CORE.** Los dos switches que lo conforman son compatibles con tecnología en Stack, enrutamiento dinámico, creación de VSI, FRSP y LACP. Este bloque consta de dos Switches de nivel III con puertos

- **WAN+Internet**. El equipamiento de este bloque no es gestionado por la Organización, si no que está delegado a un proveedor de servicios.

- **CPD.** Cabe destacar que los firewalls son capaces de operar a nivel VII, permiten la creación de zonas, pueden virtualizarse de modo que se disponen de varios firewalls bajo un mismo hardware, pueden hacer inspección SSL, aplicar políticas antivirus, actuar como IPS, admiten enrutamiento dinámico y pueden operar en activo-activo real. En cuanto a los switches, disponen de tecnología en Stack, enrutamiento dinámico, creación de VSI, FHRP y LACP.

- **LAN Usuarios.** Los switches de esta capa disponen de tecnología en Stack, enrutamiento dinámico, creación de VSI, FHRP y LACP. Por otro lado, los APs son capaces de funcionar como lightwait y autónomos, además de aceptar varios modos de operación como “flexconnect” para disponer del direccionamiento en la propia sede o “modo local” para irradiar las VLANs definidas en la controladora y comunicarse a través de un túnel CAPWAP. Las Controladoras aceptan protocolos WPA, WPA2, 802.1X y autenticación en local.

3.3. Riesgos del modelo actual

Tras analizar la red, así como la tecnología empleada, es posible apreciar una serie de riesgos sobre los modelos actuales del Centro de Informática, Hospitales y otras sedes. Teniendo en cuenta en el ámbito al que va destinado dicho modelo, instituciones sanitarias, y la criticidad de los datos, se destacan los principales riesgos de cada arquitectura.

3.3.1. Riesgos sedes Tipo I

3.3.1.1. Riesgos Centro de Informática

En cuanto al Centro de Informática, el diseño por bloques segmenta adecuadamente la red facilitando su administración, identificación del tráfico y separación de los niveles de seguridad.

- **Internet:** Es el bloque por el que circula el tráfico hacia internet, Organizaciones, Comunidades Autónomas y la red Interministerial. El propósito de dicho bloque se encuentra muy globalizado convergiendo hacia un mismo bloque tráfico corporativo, tráfico de soporte técnico, tráfico de integraciones entre servidores, tráfico del ciudadano accediendo a las aplicaciones publicadas y tráfico de usuarios hacia internet. Así pues, se otorga los mismos tratamientos a tipos de datos (Por ejemplo, a nivel de seguridad, de inspección del tráfico, de QoS, etc) totalmente diferentes, simplemente atendiendo al punto de salida que dispone la Organización Ox.
  Por otro lado, ofrecer los servicios a través de una VIP, no es el método más idóneo, ya que únicamente proteges el direccionamiento IP real que tiene dicho servicio, pero no aíslas al ciudadano anónimo de la red interna, con lo que este accede directamente a los servidores dejándolos expuestos. La configuración de reglas en nivel IV es un método poco útil en un bloque cuyo tráfico principal es a nivel VII, pudiendo complicar la gestión con configuraciones de reglas interminables y perdiendo de vista la lógica de negocio.
  Enlazando con este punto, el uso del proxy como elemento restrictivo de URLs se encuentra justificado, permitiendo el uso de diferentes perfiles con los ficheros .pac. No obstante, no es propósito del proxy realizar estas funciones, pudiendo descargarse esta tarea sobre elementos más especializados en control de contenido. Además, al no interceptar tráfico SSL, no es capaz de cachear el 90% del tráfico, por lo que no acelera el servicio de contenido web.
  Como ya se ha mencionado, también sirve como punto de entrada de conexiones remotas VPN, L2L y P2P, no validando usuarios individualizados, siendo el caso de las VPN usuarios genéricos creados localmente, con lo que no se tiene un control de acceso a la red, pudiendo haber entradas no autorizadas bajo un mismo usuario.

- **Core:** Dicho bloque es el núcleo de la red Xenon y enlaza a todos los bloques. El mayor riesgo que se observa en dicho bloque es la adición

de rutas estáticas de toda la red Xenon, con lo que aumenta la probabilidad de error humano que implique en una pérdida de servicio crítica.

- **CPD:** Es el bloque donde se encuentra el CPD de la Organización Ox y por tanto donde se alojan los servicios centralizados. Al encontrarse en el mismo nivel, el balanceador que ofrecen los servicios como un firewall que protege el acceso a los servidores, se observa un fallo de seguridad de acceso a los servicios, ya que no se dispone de una capa de control que limite o restrinja los accesos desde fuera de este bloque.
  De igual modo, el disponer de una red plana tras el firewall, tiene la ventaja de la ligereza que disponen las aplicaciones, sobre todo las copias de seguridad al no tener elementos intermedios que entorpezcan la comunicación, puesto que esta se establece en nivel II. No obstante, se pierde la visibilidad y control que tiene la red al no fluir el tráfico a través del firewall. Si, además se añade que el tráfico no se encuentra segmentado, existe una gran probabilidad de riesgo a que pruebas en TEST de una aplicación, afecte directamente a las aplicaciones en Producción. No hay separación de tráficos con lo cual se otorgan las mismas prioridades y criticidades a todas las aplicaciones, compartiendo también el mismo dominio broadcast implicando que un error en la red pueda afectar a todos los servidores. Un punto de fallo crítico de seguridad es el acceso por la misma interfaz a gestionar el servidor y el acceso al servicio, puesto que se están exponiendo a los usuarios no administradores el acceso a servicios de administración habiendo como única barrera el login de usuario.
  La configuración de reglas en nivel IV queda justificada al encontrarse en un bloque cuyo tráfico principal es categorizable en nivel IV, aunque se puede complicar la gestión con configuraciones de reglas interminables y perdiendo de vista la lógica de negocio, por lo que es más recomendable el uso de reglas de nivel VII.
  Por último, en cuanto a soporte de los certificados en el servidor y validación de usuarios cliente por CRLs, se encuentra poco optimizado, puesto que el servidor soporta la carga de cifrado y descifrado suponiendo una carga computacional extra no necesaria, teniendo que mantener una lista de certificados que en un momento puede quedar desactualizada.

- **Interno:** Siendo este bloque un punto de acceso de los usuarios a la red, debe estar debidamente securizado. No obstante, se aprecia el uso de VLANs por defecto, ya que para casi todos los fabricantes la VLAN 1 es la de administración por defecto y no es recomendable utilizarla para dar servicio. Además, es la empleada por defecto en la configuración de puertos, con lo cual se encuentra muy expuesta a ataques de VLAN Hopping. Igualmente, al no haber una segmentación bien definida todos se encuentran bajo el mismo dominio broadcast, con lo que un error puede afectar a todos los usuarios. El uso de una solución NAC Server es correcta, siempre y cuando esté bien perfilada ya que permite el control de accesos a la red cableada únicamente al personal autorizado en el LDAP. No obstante, el punto de fallo se encuentra en la red WiFi

ya que es accesible con PSK, siendo vulnerables a ataques basados en fuerza bruta.

3.3.1.2. Riesgos en Modelo de Hospitales

La arquitectura de red seleccionada en los Hospitales, arquitectura en 3 capas, es correcta puesto que permite redundancia, separación de funciones, minimizar puntos de fallos y escalabilidad, no obstante, se pierde el control de la red interna. Tal y como se ha realizado en el análisis de riesgos del Centro de Informática, se procede a analizar los riesgos del modelo de red de un centro Hospitalario, por cada bloque.

- **CORE.** La función de interconexión entre los bloques es correcta, no encontrando riesgos sobre este bloque.

- **WAN+Internet.** En este bloque se encuentra un fallo de seguridad, ya que no dispone de control del perímetro de la red, estando expuesto el Hospital a ataques provenientes de otras sedes o fallando la contención de una anomalía (Por ejemplo, propagación de un ramsonware) a la red del Hospital. Además, no se tiene control sobre la red entre sedes, no disponiendo de una gestión de tráfico óptima adaptada a las necesidades de las aplicaciones, siendo tratado como BestEfford el tráfico de la sede en la red del proveedor.

  CPD. Este bloque es plano, no estando alineado con la visión de negocio de la organización Ox. Al igual que en el Centro de Informática el disponer de una red plana tras el firewall, tiene la ventaja de la ligereza que disponen las aplicaciones, sobre todo las copias de seguridad al no tener elementos intermedios que entorpezcan la comunicación, puesto que esta se establece en nivel II. No obstante, se pierde la visibilidad y control que tiene la red al no fluir el tráfico a través del firewall. Si, además se añade que el tráfico no se encuentra segmentado, existe una gran probabilidad de riesgo a que pruebas en TEST de una aplicación, afecte directamente a las aplicaciones en Producción. No hay separación de tráficos con lo cual se otorgan las mismas prioridades y criticidades a todas las aplicaciones, compartiendo también el mismo dominio broadcast implicando que un error en la red pueda afectar a todos los servidores. Un punto de fallo crítico de seguridad es el acceso por la misma interfaz a gestionar el servidor y el acceso al servicio, puesto que se están exponiendo a los usuarios no administradores el acceso a servicios de administración habiendo como única barrera el login de usuario.
  La configuración de reglas en nivel IV queda justificada al encontrarse en un bloque cuyo tráfico principal es categorizable en nivel IV, aunque se puede complicar la gestión con configuraciones de reglas interminables y perdiendo de vista la lógica de negocio, por lo que es más recomendable el uso de reglas de nivel VII.

- **LAN Usuarios.** Este bloque está formado por dos capas:

- ***Capa de distribución.*** La segmentación realizada, aunque es más óptima que en el bloque de usuarios del Centro de Informática, es pobre si se tiene en cuenta la cantidad de tipos de usuarios que es posible encontrar en un Centro Sanitario, categorizando de manera muy globalizada los diferentes roles. Así pues, se incluye dentro del mismo dominio broadcast a facultativos o servicios de urgencias que a administrativos, con lo que, si se generase una tormenta de broadcast con origen el colectivo de administrativos debido a un fallo de red, afectaría a los servicios de urgencias.
  Se aprecia el uso de VLANs por defecto, ya que para casi todos los fabricantes la VLAN 1 es la de administración por defecto y no es recomendable utilizarla para dar servicio. Además, es la empleada por defecto en la configuración de puertos, con lo cual se encuentra muy expuesta a ataques de VLAN Hopping.
  Las instancias Multiple Spanning-Tree (MST), si se encuentran bien configuradas, previenen de posibles bucles por cambio de topología según Instancias de VLANs, no obstante, su convergencia es más lenta que otros protocolos con el mismo propósito.
  El manejo de Access List (ACLs) para limitar accesos es muy rudimentario, recayendo esta tarea sobre un equipo que no se encuentra destinado a la restricción de accesos. Además, el manejo de ACLs complica la gestión pudiendo ser un punto de fallo que dejaría incomunicada toda la sede.
- ***Capa de acceso.*** Al estar los switches formando anillos de hasta 8 dispositivos, se incrementa el riesgo de la existencia de cambios de topología que involucre un incremento en la CPU de los switches de distribución y por tanto se pierda el acceso a la sede.
  En cuanto al acceso a la red cableada, existe una brecha crítica de seguridad al no existir ningún tipo de protección de acceso. Esto puede implicar que la red se encuentre expuesta a ataques de suplantación de identidad, Man-in-the-Middle, conexión de equipos no autorizados a la red y que se promueva la tendencia a BYOD que no cumplan las políticas de seguridad adecuadas, pudiendo comprometer la seguridad de toda la red Xenon y a su vez, todos los organismos que conecten con ella.
  Por otro lado, aunque la red WiFi se encuentre protegida por PSK, es muy vulnerable ante ataques basados en fuerza bruta, ya que se encuentra expuesta a todo ciudadano que acuda a la sede.

3.3.2. Riesgos en Sedes tipo II y III

En el caso de las sedes tipo II y tipo III, al no haber arquitectura definida, los incidentes son mayores ya que hay una tendencia al ad-hoc. Al igual que en los Hospitales, Al estar los switches formando anillos de hasta 8 dispositivos, se incrementa el riesgo de la existencia de cambios de

topología que involucre un incremento en la CPU de los switches de distribución y por tanto se pierda el acceso a la sede.

Así pues, se incluye dentro del mismo dominio broadcast a todos los usuarios, con lo que, si se generase una tormenta de broadcast debido a un fallo de red, afectaría a los servicios que ofrezca la sede.
Se aprecia el uso de VLANs por defecto, ya que para casi todos los fabricantes la VLAN 1 es la de administración por defecto y no es recomendable utilizarla para dar servicio. Además, es la empleada por defecto en la configuración de puertos, con lo cual se encuentra muy expuesta a ataques de VLAN Hopping.

El protocolo STP, definido en el IEEE 802.1D, es el primer protocolo de spanning-tree que fue implementado y desarrollado, previniendo de posibles bucles por cambio de topología, no obstante, su convergencia es más lenta que otros protocolos con el mismo propósito.

En cuanto al acceso a la red cableada, existe una brecha crítica de seguridad al no existir ningún tipo de protección de acceso. Esto puede implicar que la red se encuentre expuesta a ataques de suplantación de identidad, Man-in-the-Middle, conexión de equipos no autorizados a la red y que se promueva la tendencia a BYOD que no cumplan las políticas de seguridad adecuadas, pudiendo comprometer la seguridad de toda la red Xenon y a su vez, todos los organismos que conecten con ella.

Por otro lado, aunque la red WiFi se encuentre protegida por PSK, es muy vulnerable ante ataques basados en fuerza bruta, ya que se encuentra expuesta a todo ciudadano que acuda a la sede.

3.3.3. Riesgos en monitorización

Si se analiza la monitorización y trazabilidad del tráfico, se disponen de dos herramientas de monitorización de la red que resultan complementarias y cubren las necesidades básicas, para saber el estado de los equipos.

Sin embargo, falta una herramienta de gestión única de logs que agrupe y almacene todos los servicios de red, así como, sirva de análisis de dichos servicios. Esto conlleva a que se incrementen los tiempos de resolución de incidencias de la red, al no tener una herramienta única que correlacione los logs y tener que entrar dispositivo a dispositivo, para identificar que está sucediendo en la red o de donde proviene un determinado tráfico.

Además, la falta de una sonda que reciba tráfico continuado y facilite la tarea de diagnosis e interpretación de datos, provoca tener que dedicar tiempo extra para analizar los resultados.

3.3.4. Otros riesgos

Por parte de los administradores, se encuentra comprometidas las credenciales de acceso al emplear protocolos no cifrados, enviando de este modo los usuarios y passwords de acceso a la administración de los dispositivos de red mediante texto plano, con lo que, si un atacante se encuentra a la escucha, tendría la administración de la red.

Otro punto de riesgo es que no hay backups de configuraciones, con lo cual ante fallos no es posible volver a una configuración anterior, incrementando los tiempos de resolución de incidencias.

En cuanto a los dispositivos tecnológicos, se observan dispositivos polivalentes sin funciones bien definidas, desaprovechando capacidades que resultan de utilidad para mejorar la gestión de la red o haciendo uso de funcionalidades que no competen a los dispositivos. Cabe anotar, que el equipamiento se encuentra sobredimensionado, en buen estado y actualizado, debido a adquisiciones realizadas recientemente.

3.4. Resultados del Análisis de la red

Tras realizar el análisis de red del diseño actual, indicamos los resultados obtenidos en la Tabla 4, según las métricas definidas en el capítulo 2. Se adaptan las métricas para establecer una línea base que servirá para posteriormente realizar un análisis comparativo en el capítulo 5.

Cabe anotar que el conjunto de métricas definidas para el Objetivo 2 no aplican en esta fase del proyecto, así como los requisitos y valoración de objetivos.

	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	210	

	estima que existe a consecuencia del diseño?		
	M4.c ¿En cuánto se estima el tiempo de respuesta ante peticiones, cambios e incidencias prioritarias?	30 min	
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.	

Tabla 4. Tabla de resultados del Análisis

Resumen del capítulo

Basándose en el anterior capítulo, se realiza un análisis de las características típicas de red y como se ajustan las soluciones existentes, como trabajo previo al diseño. Este análisis contempla la arquitectura de red, dividiéndose en la Red MacroLAN o red que conecta todas las sedes; las redes de Área Local, refiriéndose a la arquitectura de red de cada sede y la monitorización y trazabilidad que se realiza sobre la red.

Dentro del análisis de la red MacroLAN se ha realizado una clasificación según las tipologías de cada sede que fue descrita en el apartado “2.2. Tipos de sedes” y que será empleada para el análisis realizado en las redes de Área Local. Al mismo tiempo, se describe la relación existente a nivel de arquitectura de red de los nodos.

Así pues, se prosigue con la descripción del diseño de red de cada tipo de sede, donde se puede apreciar claramente que la complejidad de los diseños radica en las sedes de tipo I, habiendo una arquitectura basada en bloques tal y como se mencionó en el apartado “2.1. Descripción de la Organización”, mientras que las sedes de tipo II y III son más simples. A lo largo del capítulo, se pueden ver alguno de los conceptos que se han tratado en el Estado del Arte, como “Acceso a la Información” o “Tipos de arquitectura de red”. Este análisis nos servirá como punto de partida para identificación de los riesgos y la realización del diseño en el capítulo 4.

De igual modo, el capítulo analiza la tecnología existente en cada sede, ya que entre los requisitos del cliente se encuentra “aprovechar el máximo equipamiento posible” [R6] e influirá directamente en el diseño final.

Una vez aclarado el punto de partida, se ha realizado un análisis de riesgos [O2] tanto de la arquitectura de red de las sedes, como de la seguridad, gestión, monitorización y trazabilidad y algún riesgo adicional que se ha detectado como la gestión de backups de configuraciones. Este análisis permite identificar las deficiencias y virtudes del diseño existente, que se tendrán en cuenta a la hora de realizar el diseño.

Finalmente, se han plasmado los resultados del análisis respecto a las métricas definidas de modo que se establece una línea base para medir el nivel de mejora obtenido.

4. Diseño

Tras realizar el Estudio y Análisis previo, se procede a realizar el diseño del modelo de red para el conjunto de la organización Ox atendiendo a los objetivos marcados y los requisitos del cliente.

Dado los riesgos identificados durante la fase de estudio y análisis, el siguiente diseño pretende mitigarlos y ofrecer un modelo de red optimizado para la organización Ox, ajustándose a la criticidad de la información que circula a través de la red Xenon y que puede verse comprometida si no se aplican las medidas adecuadas de gestión y seguridad.

Puesto que el número de recursos y de usuarios es elevado, así como la variedad de tipologías de centros que es posible encontrar, el diseño debe de ajustarse lo mejor posible a la multitud de escenarios que pueden darse. Al mismo tiempo, se ha de atender en todo momento a que debe ser un diseño administrable, predecible y escalable [R5].

A continuación, se presentan los diferentes diseños según las tipologías de sedes previamente definidas, en cumplimiento con los objetivos [O3].

4.1. Diseño sedes Tipo I

4.1.1. Centro de Informática

Respetando el requisito del cliente de mantener la estructura de bloques para mejorar la gestión de la red [R3] y cumpliendo con el objetivo de mejorar la administración de la red [O4], se procede a añadir tres bloques llamados Externa, Interconexión y DMZ. Los dos primeros bloques segmentan la salida de Internet para poder discernir los tipos de tráfico que existen [R4] y el tercer bloque añade una capa de seguridad a la red [O6].

De este modo el diseño del Centro de Informática se divide en los siguientes bloques:

- **Internet:** Bloque por el que circula el tráfico a Internet y por donde se ofrecen los servicios de la Organización, enlazando con el bloque DMZ.
- **Interconexión:** Bloque por el que se comunican las integraciones entre las diferentes Organizaciones, Comunidades Autónomas y la red Interministerial. Este Bloque también sirve como punto de entrada para el personal Sanitario de las distintas Organizaciones a los servicios que se ofrecen a recursos internos.
- **Externa:** Punto de acceso a la red Xenon de manera remota.
- **DMZ:** Bloque de la Zona Desmilitarizada (DMZ), segura para ofrecer los servicios al ciudadano y que este se quede en el perímetro de la organización.
- **Core:** Bloque que interconecta todos los bloques de la red Xenon.

- **CPD:** Es el bloque donde se encuentra el CPD de la Organización Ox y por tanto donde se alojan los servicios centralizados.
- **Interno:** En este bloque proceden el personal que accede Internamente desde la red Xenon a los recursos centralizados de la organización.

A continuación, se procede a detallar las funcionalidades y cambios realizados en cada uno de los bloques y que se ve reflejado en la Figura 15.

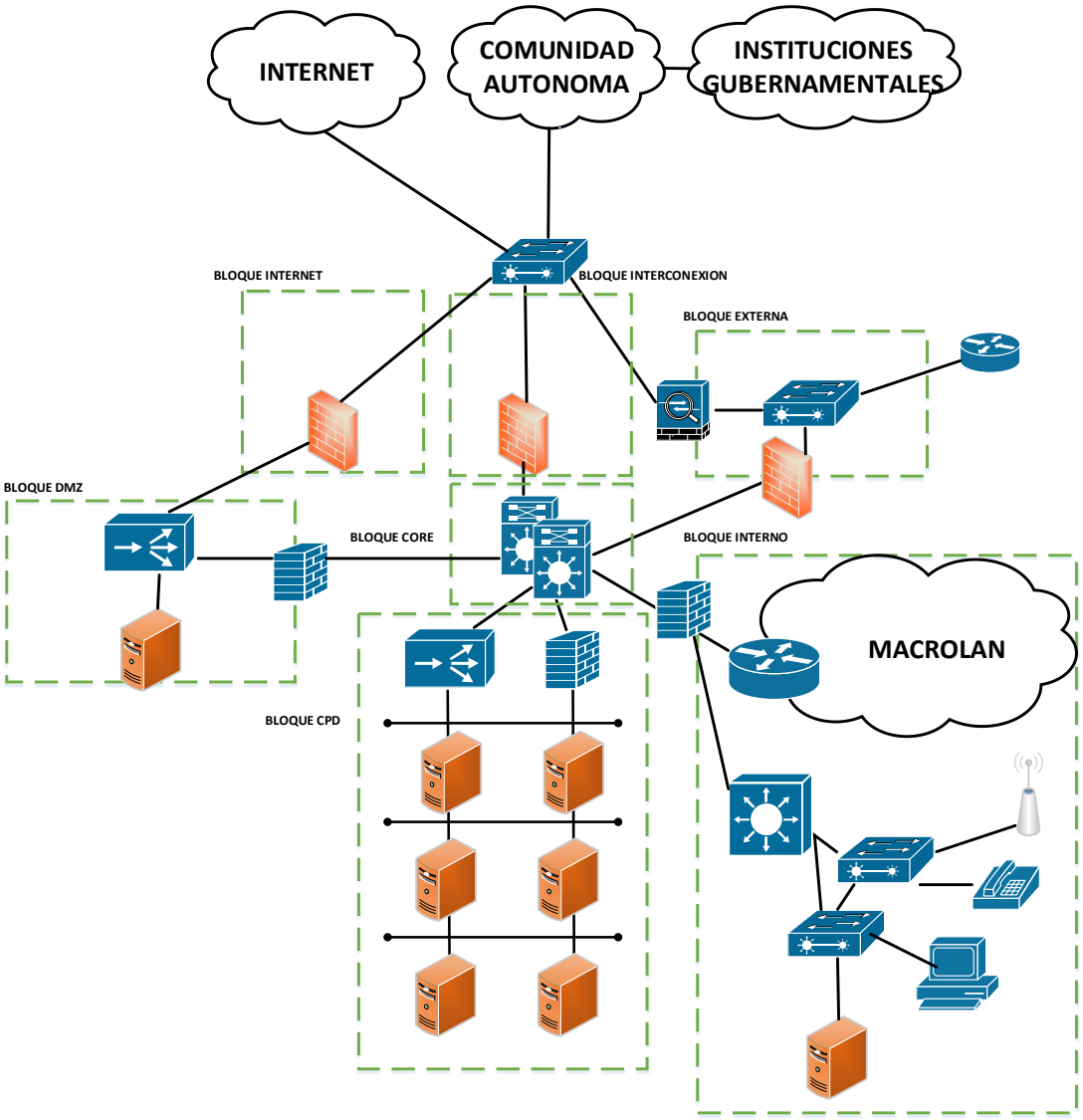

Figura 15. Diseño del Centro de Informática

4.1.1.1. Bloque Internet

Las funcionalidades de este bloque se segmentan y pasa a ser el Bloque por el que circula el tráfico a Internet y por donde se ofrecen los servicios de la Organización, enlazando con el bloque DMZ, tal y como se visualiza en la Figura 16.

Esta segmentación se consigue gracias a la funcionalidad de los firewalls de poder ser Virtualizados. De este modo, se consigue separar tráfico totalmente independiente facilitando la administración de la red.

Se elimina el switch que se ubica tras el firewall de este bloque y se añade uno delante, para poder enlazar todas las salidas con la red GigaBit.

El proxy es eliminado debido a su obsolescencia, no cumple su función de cachear el tráfico de usuario para ofrecer el contenido más rápido debido a que el 90% del tráfico es SSL y a que contribuye a ser un cuello de botella. En su lugar, y para mantener la funcionalidad de restringir el tráfico por URL, se habilita en el nuevo firewall virtual el modo de operación en nivel VII para poner en marcha la funcionalidad de filtrado por URL y por firma de servicios.

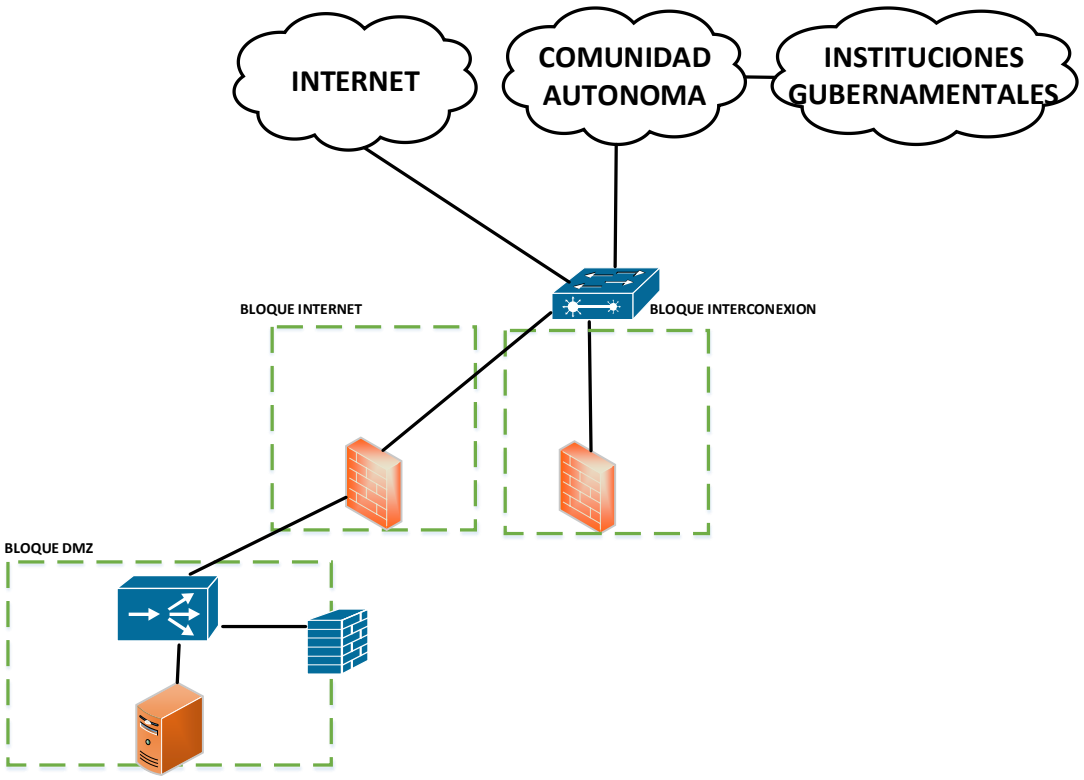

Figura 16. Nuevo Bloque de Internet

Se añade un enlace con el nuevo bloque DMZ, indicando menor prioridad para esta interfaz, de modo que se considere como una zona poco segura. Se habilita para el tráfico dirigido a esta interfaz la funcionalidad de IPS.

4.1.1.2. Bloque Interconexión

Este nuevo Bloque es por el que se comunican las integraciones entre las diferentes Organizaciones, Comunidades Autónomas y la red Interministerial. De este modo, al ser la Organización Ox un subconjunto de

sedes dentro de una red mayor con direccionamiento privado, se favorece su integración con un firewall virtual dedicado.

Además, este Bloque también sirve como punto de entrada para el personal Sanitario de las distintas Organizaciones a los recursos internos. Es por ello, que, aunque se empleen PCs enmaquetados, se añaden políticas de Antivirus.

4.1.1.3. Bloque Externa

En este bloque se produce el punto de acceso a la red Xenon de manera remota. Se traslada el concentrador VPN a este bloque, ubicándolo por delante del firewall virtual para terminar los tuneles y así tener mayor control. En la Figura 17 se detallan las funciones de dicho bloque.

Se respetan los tuneles VPN y L2L como métodos de acceso de empresas de soporte remoto y se propone la sustitución de las P2P por Virtual Routing and Forwarding (VRFs) conectadas directamente en el perímetro, de este modo se reducen costes de mantenimiento de equipamiento. No obstante, se aplican políticas de autenticación de usuario con Single-Sign-ON e integrado con el LDAP corporativo para la validación de usuarios L2L y VRF. Si el acceso se produjera desde servidores, la validación se realizaría por certificado.

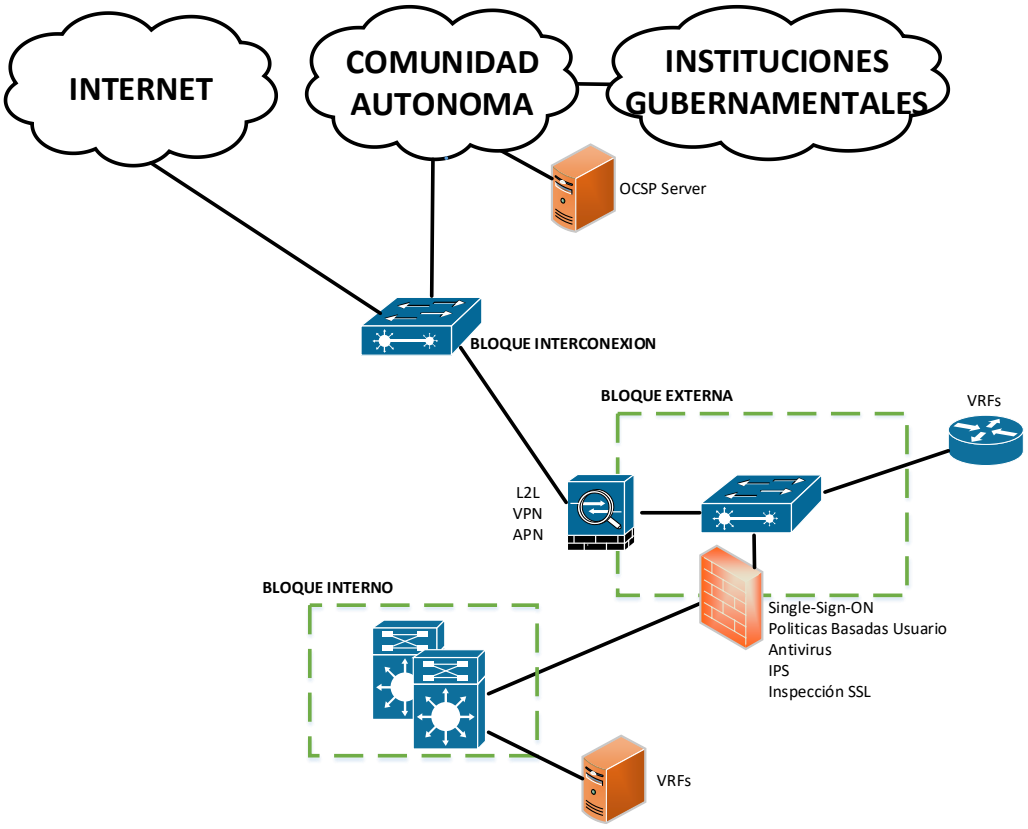

Figura 17. Nuevo Bloque Externas

En el caso de las VPN de empresas de soporte remoto, se eliminan los usuarios genéricos locales y se procede a validar con usuarios de LDAP. De este modo los usuarios son gestionados por los responsables de cada acceso y no por los administradores de la red. Se añade mayor seguridad a nivel de gestión de accesos y gestión de caducidades, a la vez que se identifican individualmente cada usuario [O6]. Además, se añade otra capa de seguridad forzando la validación a través del certificado vía script, de modo que el usuario de login se adquiera del propio certificado y así se impida la suplantación de identidad, al mismo tiempo que este certificado es validado por Online Certificate Status Protocol (OCSP) contra las Autoridades de Certificación (CA) correspondientes.

En el firewall se añaden las funcionalidades de inspección Antivirus, IPS e Inspección SSL. Para esta última, es necesario que se añada en los contratos de soporte una cláusula de cumplimiento de la Ley de Protección de Datos [8].

Por otro lado, para el caso de e-working [R8], dado que los usuarios disponen de teléfonos asignados por la propia organización para realizar sus tareas a distancia, se propone habilitar un servicio de APN con la empresa proveedora (ISP). Este servicio no es más que un sistema ISM que establece para un APN en concreto un túnel L2L con la organización, con posibilidad de validación contra RADIUS y LDAP. Ya que se autenticarían los usuarios de manera individualizada, se excepcionarían de las políticas de autenticación en el firewall.

El firewall quedaría gestionado con reglas genéricas de acceso a los recursos, plataformas de saltos y sedes.

4.1.1.4. Bloque DMZ

Dada la ineficiencia de ofrecer en el mismo firewall los servicios publicados al exterior en base a VIPs, se genera este bloque de la Zona Desmilitarizada y que este se quede en el perímetro de la organización [O6].

Esto se consigue virtualizando el Balanceador ubicado en el CPD y derivando el tráfico que entra por Internet a este nuevo elemento. Para este Balanceador, se habilitan las funciones de WAF para delimitar el acceso a las aplicaciones y de reverse proxy para que este sea el encargado de alcanzar los recursos requeridos por el usuario e impida de este modo que un ciudadano anónimo acceda a los recursos internos de la organización.

Se habilita la aceleración por certificado wildcard renovado anualmente. De este modo, se reducen gastos por gestión de certificado, se acelera la entrega de las aplicaciones al usuario final y es el balanceador el que es terminador del túnel.

Se añaden los servicios que van publicados al exterior como Servidor de Correos o servidor de videoconferencias, en esta zona para mayor seguridad.

En la pata de comunicación entre el balanceador y Core se habilita un firewall virtual de modo que proteja de ataques a la red de la DMZ. Este firewall es virtualizado del firewall del CPD para disponer de doble barrera de fabricante.

4.1.1.5. Bloque CORE

Bloque que interconecta todos los bloques de la red Xenon. No se realizan grandes cambios sobre este bloque salvo habilitar el enrutamiento dinámico vía OSPF (Open Shortest Path First) conjuntamente con todos los elementos de nivel III que hay en el Centro de Informática, formando el backbone de la red. Gracias a esta operación, los administradores de red no necesitan estar introduciendo manualmente rutas, induciendo errores humanos en un elemento de Core [O4][R1].

4.1.1.6. Bloque CPD

Es el bloque donde se encuentra el CPD de la Organización Ox y por tanto donde se alojan los servicios centralizados. Se mantienen al mismo nivel firewall y Balanceador, habilitando en este último el WAF. En la Figura 18 se muestra en mayor detalle.

El mayor cambio de este bloque viene en la segmentación por zonas de los diferentes entornos destinados a TEST, PRE y PRO, que son reconocidos en la Organización como fases de puesta en marcha de nuevas aplicaciones [O4][O6][R2][R3]. Estas zonas vienen delimitadas por nuevas Interface VLANs definidas en el firewall y Balanceador.

Se separa el tráfico de gestión y backup, siendo este gestionado por una red no enrutada y accedido a él por los administradores a través de una pasarela de interconexión altamente securizada [O6].

Si se requiere el acceso a un servidor por su interfaz de consola/ILO deberá realizarse a través de una pasarela accesible desde este bloque sólo desde la propia sede (gestión out-bound). Es decir, la gestión de las consolas de los elementos de red o servidores se realizará desde el propio Centro de Informática.

En esta capa se dispondrá en caso de que fuera requerido conectividad mediante Fiber Channel over Ethernet (FCoE o FC) de los servidores hacia las cabinas. Esta solución permite tener de forma unificada la conectividad del datacenter.

Las funciones de los frontales WEB que operaban en servidores independientes y su única función era redirigir peticiones a servidores de aplicaciones, pasa a ser asumida por el balanceador virtualizado del CPD de modo que pasa a operar como ADC. Además, se habilita la aceleración de contenidos importando los certificados de los frontales al Balanceador, ofreciéndose todos ellos bajo certificado wildcard de renovación anual. La comprobación de validez de certificados se modifica de CRL a OCSP contra la Autoridad de Certificación.

De igual modo, se añade el firewall del CPD entre los servidores. La segmentación de estos servidores es realizada según Servidores de Aplicaciones y Bases de Datos. Así pues, se añade una interfaz de frontend en los servidores de aplicaciones de modo que solo puede acceder a ella los frontales Web y una interfaz de Backend que conecta con las Bases de Datos, todo ello siendo intermediario el firewall.

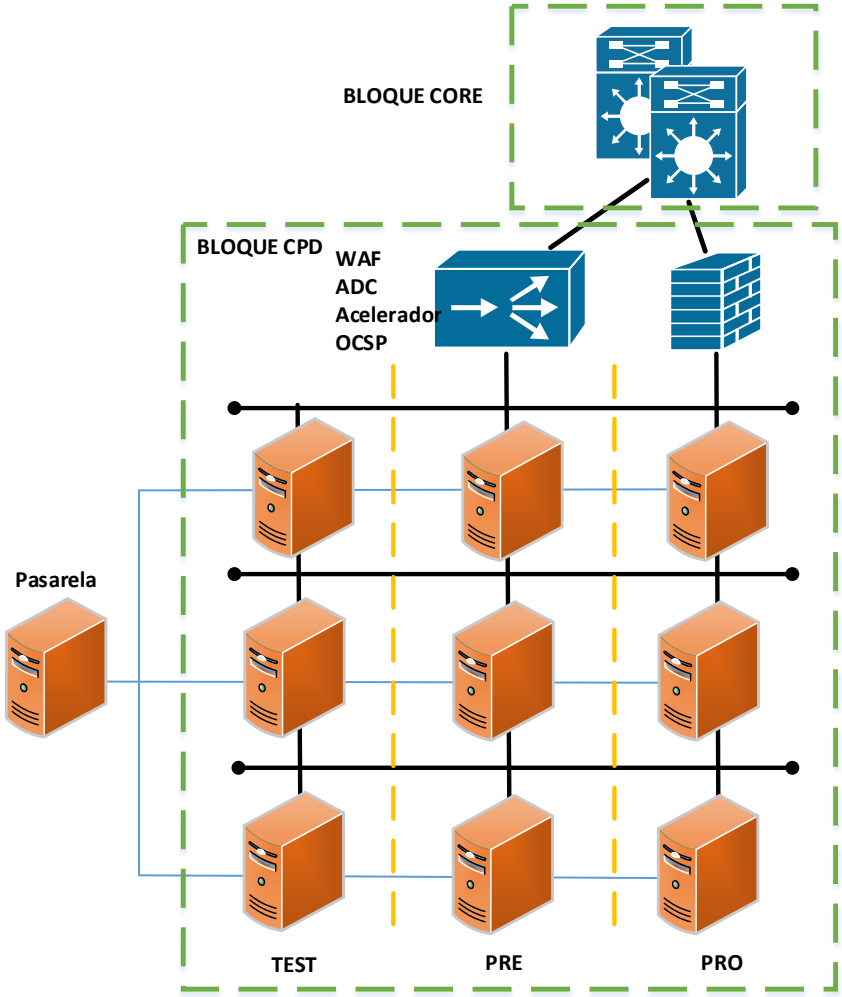

Figura 18. Nuevo Bloque CPD

Cabe destacar que los servicios se publican a través de VIPs, definidas como una red de servicio y que el acceso a los servidores de Aplicaciones solo se realiza a través de otro servidor ya sea para su gestión a través de la pata de gestión o por ofrecer sus servicios a integraciones a través de su pata de servicio.

Se mantiene la solución de tecnología fabricpath para la comunicación entre switches y servidores para ofrecer una solución mallada completa de alta redundancia.

4.1.1.7. Bloque Interno

En este bloque proceden el personal que accede Internamente desde la red Xenon a los recursos centralizados de la organización. Así pues, se distingue el acceso del personal propio del Centro de Informática y el MacroLAN.

Se Interpone en este bloque un firewall virtual del mismo hardware que el CPD en modo transparente, habilitando funciones de IPS y Antivirus [O6]. Aunque se recomienda habilitar la Inspección SSL, no es posible al ser una organización muy numerosa y no todos los usuarios están dispuestos a firmar el acuerdo de protección de datos, por lo que se deshecha la solución.

La VLAN de usuarios no será la 1, ya que no es recomendable usar porque es la nativa por defecto en los enlaces troncales y es la VLAN con la que están configurados todos los puertos de acceso por defecto.

Los puertos que no estén en uso estarán con la VLAN asignada 98 blackhole, el puerto estará en modo acceso y la interfaz en shutdown. De esta forma se garantiza que no se pinchen dispositivos externos a la red de sanidad.

En cuanto a la definición de VLANs, se añaden las siguientes [R2][R3][R4], que se extienden hasta la red inalámbrica:

- VLAN10: Englobaría todo el direccionamiento de equipamiento de Red.
- VLAN11: Destinada a los Administradores de red.
- VLAN12: Con direccionamiento de Administradores de Sistemas.
- VLAN13: Para Desarrolladores de aplicaciones.
- VLAN14: Destinada a Invitados que acudan para dar conferencias o avanzar en proyectos.
- VLAN90: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia.
- VLAN98: VLAN en la que se encontrarán todos los puertos que no se utilicen y estén en shutdown.
- VLAN99: VLAN en la que se encontraran todos los puertos en modo trunk que no necesiten una VLAN nativa.

Por otro lado, se propone para mejorar la administración [O4], tener mayor visibilidad de la red [O5] y mejorar la seguridad [O6], puesto que las redes inalámbricas se encuentran más expuestas que los accesos cableados, separar los servicios cableados de los inalambricos dando direccionamiento y VLANs diferentes. Para ello, y de modo que sea fácil su identificación será

añadida 100 al número de VLAN que se quiera publicar (SSID) por cualquier AP. Las Interface VLANs que se definen son las siguientes:

- VLAN111: Destinada para los datos de los Administradores de red que requieran de conexión vía WiFi.
- VLAN112: Usada por Administradores de Sistemas que requieran de conexión vía WiFi.
- VLAN113: Desarrolladores que requieren de conexión inalámbrica
- VLAN114: Destinado a Invitados con comunicación inalámbrica
- VLAN190: Para telefonía VoIP vía inalámbrica.

De este modo, se crean SSIDs por cada VLAN definida anteriormente a excepción de Blackhole. Todas las SSIDs estarán ocultas a excepción de la de Invitados, para entorpecer posibles accesos externos. Por otro lado, se habilita la red WiFi para acceso a través de 802.1X con validación a través de LDAP y certificado. Para el caso de Invitados, se habilita la validación a través de portal cautivo, con usuario temporal definido localmente según duración de la estancia, esto se consigue habilitando que el usuario rellene un formulario y a través del enlace que se envía al correo se genera el usuario automáticamente. Se añade al NAC Server la gestión de usuarios [O6].

En cuanto al acceso vía cableada, se mantiene el NAC Server pero habilitando funciones como poner en cuarentena un usuario que no se registre, falle la validación o se detecte patrones sospechosos en el tráfico por parte del firewall asignándoles la red de Blackhole. Además de la configuración automatizada de las interfaces permitiendo que, a través de políticas previamente definidas, se concedan los accesos propios del dispositivo o del rol que tenga el usuario. Todo ello facilita las tareas administrativas de los gestores de la red [O4], automatizando procesos cotidianos, al mismo tiempo que añade un método de protección contra amenazas de detección temprana y rápida actuación.

4.1.1.8. Resumen soluciones Centro Informática

A continuación se muestra en la Tabla 5, un resumen de las soluciones aportadas para esta sede.

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.
		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,

Tabla 5. Resumen soluciones Centro Informática

4.1.2. Diseño Hospitales

Tal y como se contemplaba en el anterior modelo de red, la arquitectura se encontraba dividida en capas o niveles de servicio (CORE, DISTRIBUCIÓN y ACCESO) y bloques (CORE, WAN, Usuarios y CPD). Con la nueva arquitectura se pretende dotar de mayor flexibilidad para que el crecimiento, comunicación e inclusión de nuevos bloques se pueda realizar de una forma más ágil. Del mismo modo, se pretende cumplir los objetivos de incrementar la seguridad de la red [O6], la trazabilidad del tráfico [O5] y facilitar la gestión de los administradores [O4].

A continuación en la Figura 19, se muestra un esquema del diagrama de bloques general del nuevo modelo, donde se aprecia que los bloques se mantienen, pero se han modificado y añadido nuevas funcionalidades, siendo el mayor cambio el diseño de capas, donde se tiene un hibrido entre arquitectura a tres capas y Core compacto.

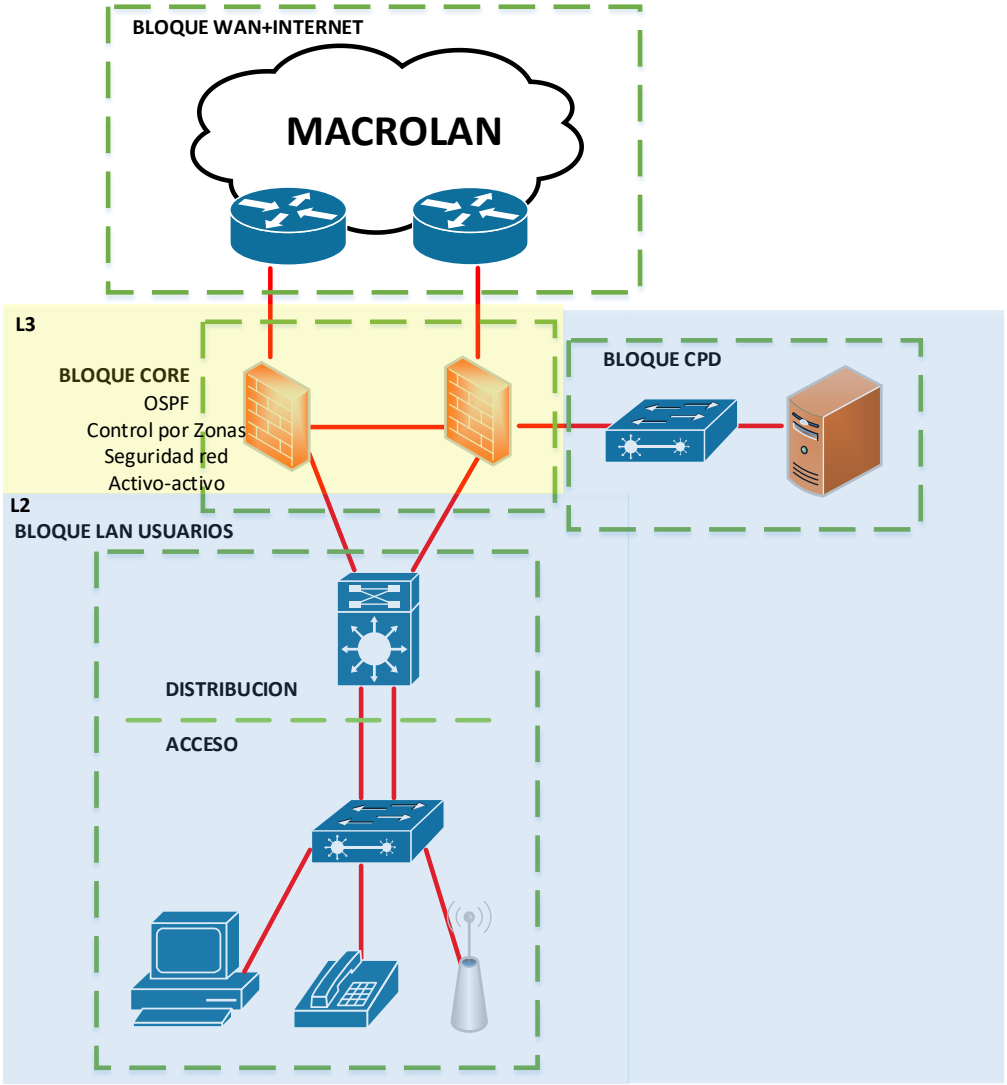

Figura 19. Diseño Hospitales

4.1.2.1. Bloque CORE

Sirve de unión entre los nodos de los demás bloques del modelo de red y su misión es conmutar paquetes entre los distintos bloques lo más rápidamente posible.

En esta nueva arquitectura, este bloque lo conforman los dos firewalls que estaban ubicados en el bloque del CPD. Así pues, se dispone todo el nivel III del Hospital en el Core, de modo que todo el tráfico circula a través de él convirtiéndose en una arquitectura de Core Compacto con OSPF. De este modo, se incrementa considerablemente la seguridad, teniendo capacidad controlar todo el tráfico del Hospital [O5][O6]. Se eliminan las ACLs, que pueden inducir fácilmente a un fallo, y se delega esta limitación a un elemento especializado.

Los firewalls tienen capacidad de actuar en modo activo-activo y además de segmentación por VSI, se realiza una separación basada en Zonas [R1].

Esta segmentación se explicará en cada uno de los bloques funcionales, así como las características habilitadas en el firewall para dotar de seguridad a la red.

4.1.2.2. Bloque Internet

Está formado por los routers de acceso a la red Xenon. La funcionalidad de este bloque, es la unión entre el Hospital a la red Xenon y por ende a la red de la Comunidad autónoma y a Internet. La centralita telefónica está conectada a este bloque.

En cuanto a la parte del Firewall, se habilitan reglas de nivel VII, pudiendo restringir desde firmas de aplicaciones hasta URLs. Además, se habilita las funciones de IPS e inspección Antivirus, de modo que se establece una barrera de protección en el Hospital frente a posibles amenazas que surjan desde otras sedes o incluso para contener amenazas del propio Hospital en un momento dado [O6]. En este bloque se define una única zona denominada como Zona Internet.

Puesto que este bloque es común a todas las sedes, se tratará en más adelante en el apartado “MacroLAN” su configuración y la motivación.

4.1.2.3. Bloque CPD

En este bloque se produce una segmentación al igual que en el Bloque CPD del centro de Informática, tal y como se aprecia en la Figura 20. El mayor cambio de este bloque viene en la segmentación por zonas de los diferentes entornos destinados a TEST, PRE y PRO, que son reconocidos en la Organización como fases de puesta en marcha de nuevas aplicaciones [O4][O6][R2][R3]. Estas zonas vienen delimitadas por nuevas Interface VLANs definidas en los firewalls del Core.

Se separa el tráfico de gestión y backup, siendo este gestionado por una red no enrutada y accedido a él por los administradores a través de una pasarela de interconexión altamente securizada.

Si se requiere el acceso a un servidor por su interfaz de consola/ILO deberá realizarse a través de una pasarela accesible desde este bloque sólo desde el centro hospitalario (gestión out-bound). Es decir, la gestión de las consolas de los elementos de red o servidores se realizará desde el propio hospital.

En esta capa se dispondrá en caso de que fuera requerido conectividad mediante FCoE o FC de los servidores hacia las cabinas. Esta solución permite tener de forma unificada la conectividad del datacenter.

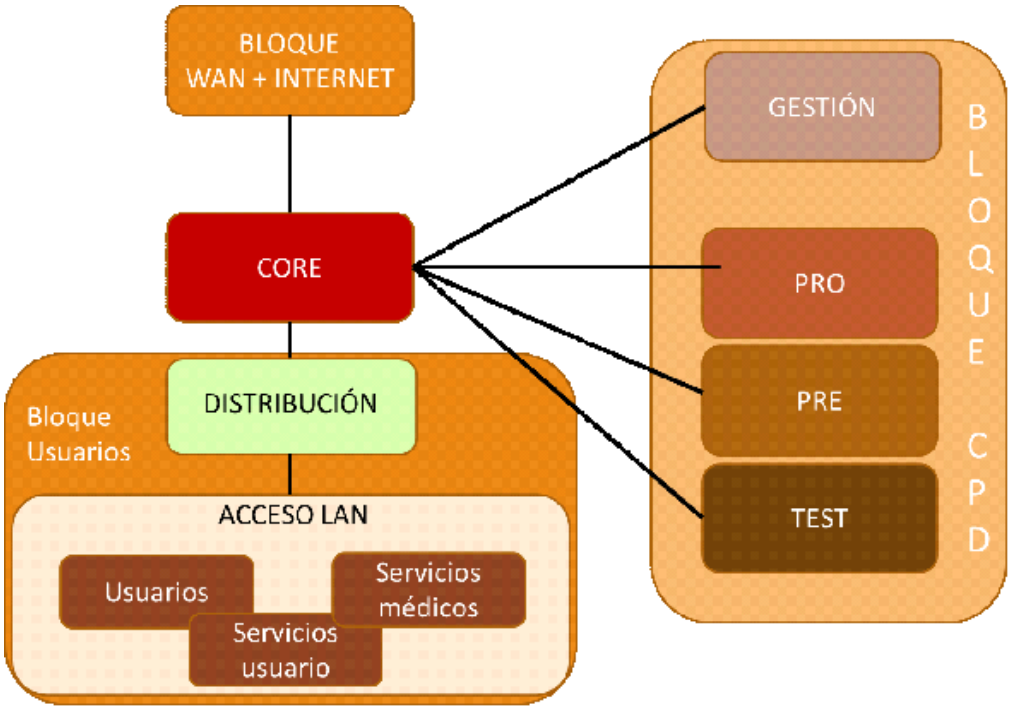

Figura 20. Diseño lógico Hospitales

Al contrario que en el Centro de Informática, en los Hospitales no se dispone de Balanceador de Carga. Así pues, no se considera necesario puesto que el acceso a estos servidores se centra en los profesionales que dependen de esta sede, por lo que la carga no es tan elevada como para invertir en nuevos Balanceadores [R6].

La separación de estos servidores es realizada según Servidores Web, Servidores de Aplicaciones y Bases de Datos. Así pues, se añade una interfaz de frontend en los servidores de aplicaciones de modo que solo puede acceder a ella los frontales Web y una interfaz de Backend que conecta con las Bases de Datos (bbdd), todo ello siendo intermediario el firewall mediante VSI.

Para garantizar la alta disponibilidad de las aplicaciones/servicios cada servidor debería conectarse a dos switches de producción diferentes.
Si los servidores debieran mantener la sincronización entre ellos, por motivos de diseño se interconectarán a través de una VLAN independiente no enrutada (Ejemplo: interconnect de bbdd, vmotion de vmware…).

En la capa del CPD interesa utilizar tecnología MEC (Multichasis Etherchannel) con virtual port-channel y así la conectividad de los servidores se podrá realizar en activo-activo y se podrán evitar problemas de STP (Spanning Tree Protocol).

Se configurarán equipos con tecnología FEX (Fabric Extender) para realizar las conexiones ToR (Top of Rack) en los racks. Al ser tecnología FEX la administración de estos equipos se realizaría de forma centralizada facilitando la administración del bloque datacenter. En caso de hospitales

pequeños o con una granja de servidores pequeña se podrá valorar utilizar tecnología MEC (MultiChassis EtherChannel) con Stackwise.

Todas las VLANs del datacenter tendrían como salida el enlace troncal con dirección al firewall.

4.1.2.4. Bloque Usuarios

Este bloque está formado por dos capas, una capa de falso distribución y la capa de acceso.

La capa de falso distribución consta de varias parejas de switches de nivel II con al menos tantos puertos GigabitEthernet de Fibra óptica como armarios en la capa de acceso de usuarios.

Cada uno de estos puertos se enlaza con cada uno de los armarios de acceso. Se le llama falso distribución ya que no va a contener el nivel III típico de la arquitectura a tres capas, sin embargo, va a seguir trabajando como un concentrador de switches de acceso. Además, se aplica tecnología en Stack, de modo que puedan trabajar como un solo equipo [R1].

Cada armario de comunicaciones aloja los switches de acceso y deben contar con enlaces redundados con distribución. Respecto al diseño también se propone que de distribución se bajen 2 enlaces contra switches estacados (MEC-Stackwise) en acceso para tener enlaces activo-activo y así evitar problemas de STP (Spanning Tree Protocol). Se puede observar el diagrama de red de este bloque en la Figura 21.

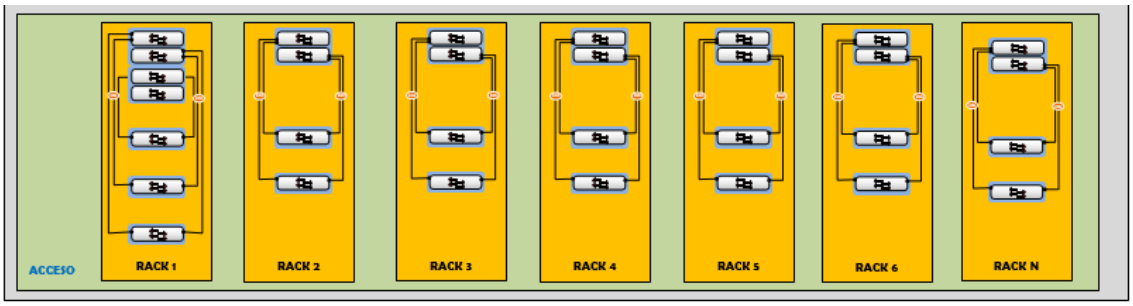

Figura 21. Diseño Hospitales físico bloque usuarios

Por diseño se recomienda un enlace doble con distribución de agrupaciones de no más de cuatro switches de acceso, realizando la agrupación de la Tabla 6.

Nº Switches por RACK	Nº Pares de Fibras
1-4	2
5-8	4
9-12	6
12-16	8

Tabla 6. Relación de agrupación de switches y número fibras

En el caso de crecimiento y necesidad de ampliar el número de switches de distribución se contempla la siguiente solución: Adición de otro bloque LAN USUARIOS, conectado al CORE.

Así pues, en cada rack de acceso se aprovecha la conexión en stack de todos los switches de acceso, de modo que actúen como uno solo, tal y como lo hacen los switches de distribución. De este modo se elimina el Spanning-Tree de la red, incrementando la tolerancia a fallos de la red, minimizando la posibilidad de incidencias y facilitando la gestión de la red.

Al disponer de tecnología en Stack en la capa de distribución es posible conectar los switches de acceso a través de port-channels desde ambos switches de distribución creando una tipología libre bucles (no hace falta spanning tree) al tener todos los caminos activos. Se dispondrá de un caudal de 20 Gb de conectividad por rack para los switches de acceso.

Aunque no se considera necesario, a modo de prevención se establece que la capa de acceso es el único lugar de la red donde estará operativo el spanning tree bloqueando puertos. Desde la capa de distribución a la capa de acceso se realizará la conectividad mediante portchannel activo-activo, de esta forma se mantendrán los enlaces redundados sin los problemas de spanning tree pudiendo aumentar el caudal de datos disponible.

Será implementado rapid spanning-tree (RSTP) en todo el entorno ya que, facilitará la configuración por parte de los administradores de red y se evitarán problemas de configuración derivado de las instancias de Múltiple Spanning Tree. Este sólo estaría justificado en el caso de que se dispusiera de una gran cantidad de VLANs que gestionar, así al hacerlo por instancias reduciría el uso de CPU de los switches.

En los switches de acceso se configura en todos los puertos de usuario el spanningtree bpduguard y el spanning tree portfast. En los enlaces de uplink con Fibra óptica (FO) se configurará UDLD y LOOPGUARD.

La VLAN de usuarios no será la 1, ya que no es recomendable usar porque es la nativa por defecto en los enlaces troncales y es la VLAN con la que están configurados todos los puertos de acceso por defecto.

Los puertos que no estén en uso estarán con la VLAN asignada 98 blackhole, el puerto estará en modo acceso y la interfaz en shutdown. De esta forma se pretende garantizar que no se pinchen dispositivos externos a la red de sanidad [O6].

En cuanto a la segmentación por zonas en el firewall del Core, se realizaría según el propósito, de modo que se dispone un conjunto de grupos claramente diferenciados [O4][O5][O6][R1][R2][R3][R4]. Además, se hace separación de dominios broadcast en los firewalls mediante VLANs, definidas según el rol. Esta segmentación se realiza para mejorar la administración y en caso de haber algún incidente de spanning-tree, tener

la red segmentada para que los errores queden aislados. Se procede a describir cada una de las VLANs según la zona definida:

- **Usuarios:** Zona destinada a usuarios y dispositivos de administración. Las Interface VLANs que componen esta zona son las siguientes:
    - VLAN10: Para los datos de los usuarios con equipos en el dominio de la Organización.
    - VLAN11: Para los datos de los usuarios con equipos que no estén en el dominio de la Organización (sindicatos, equipos no maquetados ….)
    - VLAN12: Para impresoras
    - VLAN13: Multifunción con escáner o solo escáner
    - VLAN14: Equipos de informáticos con acceso a todas las demás redes locales al hospital.
    - VLAN15: Para los datos de los equipos de urgencias (Sólo PCs).
    - VLAN16: Acceso de personal externo con solo conectividad a Internet.
    - VLAN17: Equipos clientes ligeros.
    - VLAN90: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia.
    - VLAN95: Plan B, sería un grupo de equipos escogido de cada una de las VLANs definidas en usuarios que debería de tener disponibilidad máxima.
    - VLAN98: VLAN en la que se encontrarán todos los puertos que no se utilicen y estén en shutdown.
    - VLAN99: VLAN en la que se encontraran todos los puertos en modo trunk que no necesiten una VLAN nativa.
- **Gest_red:** Zona destinada a la administración del equipamiento de red. Las Interface VLANs que componen esta zona son las siguientes:
    - VLAN20: Para la gestión de las controladoras y los puntos de acceso (access point) instalados en el centro.
    - VLAN21: Para la gestión de la electrónica de red (switches).
- **Serv_Medicina:** Zona destinada al equipamiento que ofrece servicios médicos. Las Interface VLANs que componen esta zona son las siguientes:
    - VLAN30: Para los siguientes equipos de radiología: Modalidades y estaciones de diagnóstico (imagen médica digital).
    - VLAN31: Da servicio a los analizadores de laboratorio.
    - VLAN32: Da servicio a los dispositivos de electromedicina.
    - VLAN33: Para dispositivos IP de monitorización de pacientes (equipos de la UCI,…..)
    - VLAN34: Para localización de pacientes o equipos (carros de medicamentos, pacientes, …)
    - VLAN35: Escáner de muestras al microscopio.
- **Serv_Externos:** Zona destinada al equipamiento de servicios externos que no forman parte de los servicios médicos. Las Interface VLANs que componen esta zona son las siguientes:

- VLAN40: Para equipos de mantenimiento en el centro. (Aire acondicionado, luces, SAIs, Sensores de temperatura, sensores de humos o CO2, Alarmas, Megafonía, grupos electrógenos)
- VLAN41: Para gestión de cámaras de seguridad (video-vigilancia) y dispositivos de control de acceso a determinadas zonas del hospital.
- VLAN42: Para gestión dispositivos de control de acceso a determinadas zonas del hospital.
- VLAN43: Para dispositivos que identifiquen stocks, inventario o logística de la sede.
- VLAN44: Para dispositivos que no se tenga claro donde clasificar por ejemplo carros de medicamentos, quioscos, monitores de citas, etc.

En el caso de que estas VLANs necesitaran tener servidores (Por ejemplo, empresa externa de seguridad que requiera un servidor de grabación de imágenes), se pondrían en el CPD con una VLAN específica para ese fin (DMZ_Interna).

Por otro lado, se propone para mejorar la administración, tener mayor visibilidad de la red y mejorar la seguridad, puesto que las redes inalámbricas se encuentran más expuestas que los accesos cableados, separar los servicios cableados de los inalámbricos dando direccionamiento y VLANs diferentes.

Para ello, y de modo que sea fácil su identificación será añadido 100 al número de VLAN que se quiera publicar (SSID) por cualquier AP. De este modo se separarían igualmente por una zona dedicada, denominada Usu_WiFi. Las Interface VLANs que componen esta zona y la seguridad aplicada son las siguientes:

- VLAN110: Para los datos de los usuarios con equipos portátiles en el dominio que requieran de conexión vía WiFi. En cuanto a la autenticación será por 802.1X y mediante certificados digitales, bajo protocolo EAP-TLS contra el servidor Radius de la sede. El cifrado de los datos estará basado en AES.
- VLAN116: Acceso de personal externo vía WiFi con solo conectividad a Internet. Filtrado vía MAC y con clave autogenerada vía portal cautivo con segunda validación vía mail.
- VLAN130: Para los siguientes equipos de radiología que se conecten vía WiFi: Modalidades y estaciones de diagnóstico (imagen médica digital). La autenticación se realizará mediante WPA2 con PSK compartida y bajo cifrado AES.
- VLAN133: Para dispositivos IP de monitorización de pacientes que se conecten vía WiFi (equipos de la UCI,…..). La autenticación se realizará mediante WPA2 con PSK compartida y bajo cifrado AES.
- VLAN190: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia inalámbricos. La autenticación se realizará mediante WPA2 con PSK compartida y bajo cifrado AES.

Además, para cumplir con el requisito de publicar la WiFi a los ciudadanos [R7], se crea una nueva VLAN, VLAN166, que esté separada del resto. A esta VLAN para usuarios no corporativos, se limitará el número de usuarios concurrentes a 5, siendo la autenticación por clave compartida vía portal cautivo y con cifrado AES. Para completar la separación, en el Core se conectará una VRF para salida directa independiente.

Se pueden añadir más VLANs a la parte WIFI siempre que se encuentre una necesidad y se justifique, sabiendo que contra más SSID se radien peor será el rendimiento de la red WIFI.

En cuanto a la estructura de la red WiFi, todos los Puntos de acceso (AP) se conectan de manera centralizada a un Controlador que se encontrará redundado en el propio Hospital y un tercer respaldo localizado en el Centro de Informática. Esta triple redundancia asegura alta disponibilidad en el Hospital y en las sedes dependientes de él. La estructura de las sedes dependientes del Hospital se verá en el punto “4.2. Diseño de sedes Tipo II y III”.

Se configura para que opere en la banda de los 5GHz, banda a, que será empleado para VoIP y multimedia; y en la banda de los 2.4 GHz, banda b/g, destinada a transporte de datos [R1]. Con la separación de bandas, se consigue que no se mezclen las frecuencias de voz y datos, ya que las primeras son muy sensibles a retardos.

Se recomienda distribución de APs de modo que no supere los 10-12 usuarios conectados concurrentemente para transmisión de datos y 5-8 para transmisión de voz. No es objeto de este proyecto la disposición de los APs.

Por otro lado, para la securización del acceso [O6], se extiende el NAC Server del Centro de Informática a los Hospitales, de tal modo que se convierte en el orquestador de la asignación de VLANs a los dispositivos autorizados según el rol que le ha sido asignado. Este rol está categorizado según perfiles predefinidos según el login de usuario en el LDAP, Fingerprinting de la conversación DHCP y MAC del dispositivo, de modo que se evitan ataques como MAC Spoofing. Además, este perfil se integra con el firewall de CORE que restringe el acceso según el rol.

La adición del NAC Server tiene doble efecto sobre el diseño, ya que añade seguridad en el acceso, evitando que dispositivos no autorizados accedan a la red y restringe el acceso a los usuarios, y facilita la administración de la red, ya que, con los perfiles ya predefinidos, el NAC Server es capaz de configurar los switches para otorgar el acceso que le corresponde. De este modo, los administradores ya no han de realizar tareas repetitivas de configuración de switches, cada vez que den de alta un nuevo puesto de trabajo y facilita la movilidad de los puestos de trabajo.

Al igual que en el Centro de Informática, se habilitan las funciones como poner en cuarentena un usuario que no se registre, falle la validación o se detecte patrones sospechosos en el tráfico por parte del firewall asignándoles la red de Blackhole.

4.1.2.5. Resumen Soluciones Hospitales

A continuación, se muestra en la Tabla 7, un resumen de las soluciones aportadas para esta sede.

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
		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.

Tabla 7. Resumen soluciones Hospitales

4.2. Diseños sedes Tipo II y III

En el caso de las sedes tipo II, al ser generalmente redes multifabricante donde el número de switches puede ser considerable (Entorno 8-10

switches), es recomendable realizar un diseño que se encuentre libre de bucles [1]. No obstante, el diseño queda limitado al uso del equipamiento existente debido a los requisitos de cliente [R6].

Así pues, se propone la reorganización de la estructura para diseño de una arquitectura libre de bucles y que optimice el flujo de tráfico, haciendo uso de protocolos standard [O4][R1]. De este modo se obtiene el diseño de la Figura 22.

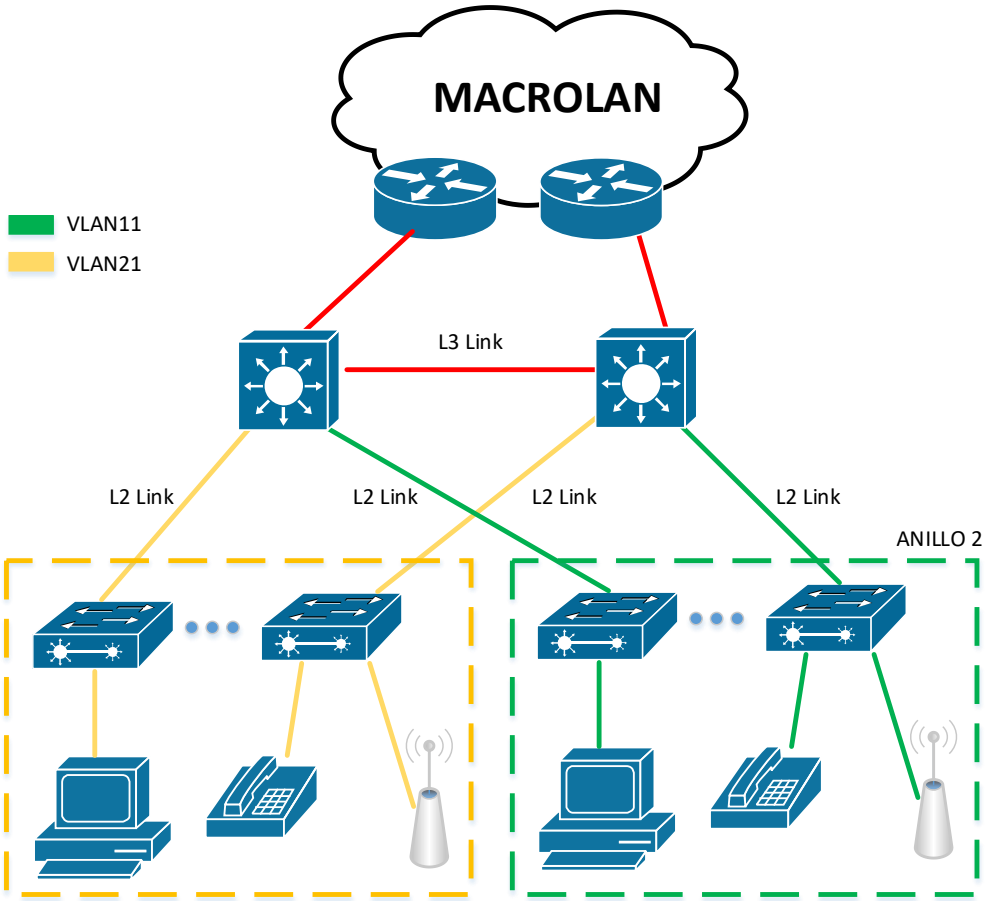

Figura 22. Diseño de sedes tipo II

Como se puede observar, cada anillo dispone de unas VLANs dedicadas y entre los switches de Core existe un enlace de nivel III que rompe el bucle de nivel II. La transmisión de las rutas a través del enlace de nivel III se realizaría por OSPF. Además, se aprovecha la máxima capacidad de los enlaces haciendo uso de VRRP (Virtual Routing Redundancy Protocol) Load Balancing, de modo que en la tabla ARP (Address Resolution Protocol) se asigna una misma IP a dos MACs diferentes, similar al protocolo propietario Gateway Load Balancing Protocol (GLBP) de Cisco, con lo que permitiría realizar un balanceo de carga entre ambos switches.

Aunque el diseño se encuentre bajo una topología libre de bucles, se configura RSTP por precaución, habilitando BPDU Guard (Protección para Bridge Protocol Data Units) en las interfaces de acceso. De igual modo, se recomienda que los anillos nunca superen los 4 switches de longitud.

En cuanto a la segmentación realizada en los switches de Core, se realiza por VLANs definidas según el rol y el switch donde se encuentra ubicado [O4][O5][O6][R2][R3][R4]. Esta segmentación se realiza para mejorar la administración, seguridad y disponer de una red libre de bucles. Cabe destacar que este diseño es posible implementarlo únicamente en sedes de tipo 2 dado que el número de roles es reducido en comparación con las sedes tipo 1. Así pues, se enumeran las VLANs según el switch donde esté ubicado el equipo, cuyo número indicará las decenas, y el rol que ocupe, cuya numeración ocupará las unidades. Se procede a describir cada una de las VLANs según las características definidas, denominando el número del anillo del switch (Por ejemplo, anillo2) como X:

- **Usuarios:** Destinada a usuarios y dispositivos de administración. Las Interface VLANs que componen esta zona son las siguientes:
    - VLANX0: Para los datos de los usuarios con equipos en el dominio de la Organización.
    - VLANX1: Para los datos de los usuarios con equipos que no estén en el dominio de la Organización (sindicatos, equipos no maquetados ….)
    - VLANX2: Para impresoras y equipamiento multifunción.
    - VLANX3: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia.
- **Serv_Medicina:** Destinada al equipamiento que ofrece servicios médicos. Las Interface VLANs que componen esta zona son las siguientes:
    - VLANX4: Para los siguientes equipos de radiología: Modalidades y estaciones de diagnóstico (imagen médica digital).
    - VLANX5: Da servicio a los dispositivos de electromedicina.
    - VLANX6: Para localización de pacientes o equipos (carros de medicamentos, pacientes, ….)
- **Serv_Externos:** Destinada al equipamiento de servicios externos que no forman parte de los servicios médicos. Las Interface VLANs que componen esta zona son las siguientes:
    - VLANX7: Para equipos de mantenimiento en el centro. (Aire acondicionado, luces, SAIs, Sensores de temperatura, sensores de humos o CO2, Alarmas, Megafonía, grupos electrógenos)
    - VLANX8: Para gestión de cámaras de seguridad (video-vigilancia) y dispositivos de control de acceso a determinadas zonas del hospital, gestión dispositivos de control de acceso a determinadas zonas del hospital.
    - VLANX9: Para dispositivos que identifiquen stocks, inventario o logística de la sede.

Por otro lado, se propone para mejorar la administración [O4], tener mayor visibilidad de la red [O5] y mejorar la seguridad [O6], puesto que las redes inalámbricas se encuentran más expuestas que los accesos cableados, separar los servicios cableados de los inalámbricos dando direccionamiento y VLANs diferentes. Para ello, y de modo que sea fácil su identificación será añadida 200 al número de VLAN que se quiera publicar (SSID) por cualquier AP. Además, estas VLANs estarán definidas en la

controladora WiFi del Hospital de Referencia, de modo que serán comunes a todos los centros de tipo 2. Las Interface VLANs que componen los accesos inalámbricos y la seguridad aplicada son las siguientes:

- VLAN200: Para los datos de los usuarios con equipos portátiles en el dominio que requieran de conexión vía WiFi. En cuanto a la autenticación será por 802.1X y mediante certificados digitales, bajo protocolo EAP-TLS contra el servidor Radius de la sede. El cifrado de los datos estará basado en AES.
- VLAN204: Para los siguientes equipos de radiología que se conecten vía WiFi: Modalidades y estaciones de diagnóstico (imagen médica digital). La autenticación se realizará mediante WPA2 con PSK compartida y bajo cifrado AES.
- VLAN203: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia inalámbricos. La autenticación se realizará mediante WPA2 con PSK compartida y bajo cifrado AES.

Además, para cumplir con el requisito de publicar la WiFi a los ciudadanos [R7], se crea una nueva VLAN, VLAN966, que esté separada del resto. A esta VLAN para usuarios no corporativos, se limitará el número de usuarios concurrentes a 5, siendo la autenticación por clave compartida vía portal cautivo y con cifrado AES. Para completar la separación, en el Core se conectará una VRF para salida directa independiente.

La VLAN de usuarios no será la 1, ya que no es recomendable usar porque es la nativa por defecto en los enlaces troncales y es la VLAN con la que están configurados todos los puertos de acceso por defecto.

No obstante, fuera de la arquitectura libre de bucles, se implementarán las siguientes VLANs, ya que debido a su naturaleza deben ser configurados en todos los switches:

- VLAN914: Para la gestión del equipamiento de red, las controladoras y los puntos de acceso (access point) instalados en el centro.
- VLAN998: VLAN en la que se encontrarán todos los puertos que no se utilicen y estén en shutdown.
- VLAN999: VLAN en la que se encontraran todos los puertos en modo trunk que no necesiten una VLAN nativa.

Para protección ante posibles bucles que tengan origen en las anteriores VLANs, se implementará rapid spanning-tree en todo el entorno ya que, facilitará la configuración por parte de los administradores de red y evitará problemas de configuración derivado de las instancias de Multiple Spanning Tree. Este sólo estaría justificado en el caso de que se dispusiera de una gran cantidad de VLANs que gestionar, así al hacerlo por instancias reduciría el uso de CPU de los switches.

Los puertos que no estén en uso estarán con la VLAN asignada 998 blackhole, el puerto estará en modo acceso y la interfaz en shutdown. De esta forma se garantiza que no se pinchen dispositivos externos a la red de sanidad [O6].

Este diseño de mayor complejidad se simplifica haciendo uso del NAC Server del Hospital de referencia para gestión del direccionamiento y configuración de las VLANs.

En cuanto a la estructura de la red WiFi, todos los Puntos de acceso (AP) se conectan de manera centralizada a un Controlador que se encontrará redundado en el propio Hospital y un tercer respaldo localizado en el Centro de Informática. Esta triple redundancia asegura alta disponibilidad en el Hospital y en las sedes dependientes de él.

De este modo las SSIDs estarán configuradas en los Hospitales de referencia que tenga la sede, al igual que la VLAN asociada, por lo que la comunicación establecida entre los APs y la controladora se realizará a través de la IP de Gestión, conformando un túnel CAPWAP que servirá de enlace para la comunicación de los clientes inalámbricos.

Se configura para que opere en la banda de los 5GHz, banda a, que será empleado para VoIP y multimedia; y en la banda de los 2.4 GHz, banda b/g, destinada a transporte de datos. Con la separación de bandas, se consigue que no se mezclen las frecuencias de voz y datos, ya que las primeras son muy sensibles a retardos [R1].

Se recomienda distribución de APs de modo que no supere los 10-12 usuarios conectados concurrentemente para transmisión de datos y 5-8 para transmisión de voz. No es objeto de este proyecto la disposición de los APs.

Por el contrario, en las sedes tipo III no vale la pena realizar un diseño tan complejo ya que el número de usuarios no superan los 10, existiendo dos roles diferentes y además se dispone de un horario reducido.

La arquitectura de este tipo de centros se mantiene, puesto que en todos los centros es de 1 switch, habiendo de por sí una topología libre de bucles. De todos modos, a modo de prevención se implementará RSTP, de modo que se establecerá prioridad 0 para el switch.

La numeración de las VLANs sigue la nomenclatura de las sedes tipo II para facilitar su compresión. Así pues, el número de VLANs se reducen a las siguientes:

- VLAN10: Para los datos de los usuarios con equipos en el dominio de la Organización.
- VLAN13: Para la voz o la videoconferencia de los usuarios. Como por ejemplo los teléfonos IP/equipos de videoconferencia.

- VLAN914: Para la gestión del equipamiento de red, las controladoras y los puntos de acceso (access point) instalados en el centro.
- VLAN998: VLAN en la que se encontrarán todos los puertos que no se utilicen y estén en shutdown.
- VLAN999: VLAN en la que se encontraran todos los puertos en modo trunk que no necesiten una VLAN nativa.

La VLAN de usuarios no será la 1, ya que no es recomendable usar porque es la nativa por defecto en los enlaces troncales y es la VLAN con la que están configurados todos los puertos de acceso por defecto.

Por otro lado, para la securización del acceso, al haberse extendido el NAC Server a los Hospitales, se procede a la validación de los accesos de las sedes de tipo II y III contra el NAC del Hospital de referencia. De este modo, se convierte en el orquestador de la asignación de VLANs a los dispositivos autorizados según el rol que le ha sido asignado. Este rol está categorizado según perfiles predefinidos según el login de usuario en el LDAP, Fingerprinting de la conversación DHCP y MAC del dispositivo, de modo que se evitan ataques como MAC Spoofing. Además, este perfil se integra con el firewall de CORE de los Hospitales, que restringe el acceso a los recursos según el rol. Puesto que no existen recursos locales dentro de este tipo de sedes y cumpliendo con el requisito de aprovechar lo existente, se recomienda la restricción de accesos según los perfiles de asignación locales limitados en los PCs plataformados, con ACLs descargadas y aplicadas con el cliente del NAC server.

La adición del NAC Server tiene doble efecto sobre el diseño, ya que añade seguridad en el acceso, evitando que dispositivos no autorizados accedan a la red y restringe el acceso a los usuarios, y facilita la administración de la red, ya que, con los perfiles ya predefinidos, el NAC Server es capaz de configurar los switches para otorgar el acceso que le corresponde. De este modo, los administradores ya no han de realizar tareas repetitivas de configuración de switches, cada vez que den de alta un nuevo puesto de trabajo y facilita la movilidad de los puestos de trabajo.

Cabe anotar, que, si no fuera por la automatización del proceso de configuración y el uso de enrutamiento dinámico, no se recomendaría este diseño, pues añade una complejidad a la red que no es compensable con los resultados obtenidos, optándose por un diseño con RSTP.

4.2.1.1. Resumen soluciones

A continuación, se muestra en la Tabla 8, un resumen de las soluciones aportadas para esta sede.

Tipo Sede	Sede	Bloque	Área	Solución
II	Hospitales y Centros de Especialidades.	General	Gestión	Core compacto, definición protocolo de conexión, eliminación STP, aumento caudal, topología libre

	Centros de Salud y Centros administrativos. >20 usuarios			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

Tabla 8. Resumen soluciones sedes tipo II y III

4.3. MacroLAN

Como se ha mencionado en los anteriores apartados, el bloque MacroLAN es una red MPLS gestionada por el proveedor de servicios, que interconecta todas las sedes que componen la red Xenon. Esta red MacroLAN actualmente dispone de una QoS básica de Best Efford, la cual no aplica ninguna política de restricción o garantía al tráfico.

Estos niveles de servicio son insuficientes para el tipo de organización en la que se encuentra. Es por ello, que se propone la modificación de los servicios del proveedor a un modelo más óptimo que incrementaría la QoE de los usuarios, así como mejoraría la gestión dotando de inteligencia a la red [O4][[R1].

Esta propuesta consiste en el cambio de servicio a un modelo SD-WAN que permitiría incrementar las posibilidades de QoS en base a los servicios ofrecidos, permitiendo que esta calidad de servicio sea gestionada por el cliente y no por el proveedor de servicios. Además, se propone la modificación del enrutamiento a OSPF, siendo el área 0 la red MacroLAN y los borders-routers los que conforma cada sede, de modo que cada sede formaría un área nueva adherida al área 0, compartiendo en toda la red el camino más óptimo en todo momento para alcanzar los recursos requeridos, con lo que se incrementaría la QoE [15].

Al mismo tiempo se dota de inteligencia a la red y de mayor autonomía de gestión al cliente ya que podrá dar de alta nuevas redes en las sedes, sin necesidad de tener que gestionarlo con el proveedor. Para dotar de mayor seguridad a las comunicaciones y que estas sean seguras en todo momento, se establecen túneles VPN (En tecnología Cisco DMVPN) de modo que los canales de comunicación se securizan en todo momento, permitiendo reforzar la solución SD-WAN.

4.4. Diseño Monitorización y Trazabilidad

La organización Ox, se encuentra poco optimizada en cuanto a Monitorización y Trazabilidad del tráfico, siendo uno de sus puntos más debiles a la hora de resolver peticiones e incidencias, por lo que a continuación se trata de abordar estas deficiencias en consonancia con los objetivos marcados [O5][R2].

La herramienta CA Spectrum se mantiene dado su potencial de monitorización y gestión del equipamiento de red. No obstante, se perfila añadiendo thresholds de modo que se obtenga una visión más preventiva de las anomalías que puedan darse en la red y de este modo ser proactivos en la gestión. De este modo, sería posible prevenir las incidencias de red, como por ejemplo, saturaciones de enlaces o excesos de CPU, e intervenir antes de que se produzca la incidencia. A su vez, se habilitan los backups de configuraciones y la gestión de versiones y cambios, que permiten de este modo mantener un registro de las configuraciones de manera periódica y hacer despliegues de nuevas versiones o cambios en los dispositivos de manera masiva, de manera centralizada desde el CA Spectrum.

Por otro lado, se propone el descarte de la herramienta Cacti por otra herramienta OpenSource, más potente y versátil que permitiría complementar las deficiencias en CA Spectrum. El uso de ELK Stack sería la solución propuesta.

La principal motivación de optar por la solución ELK Stack, es la posibilidad de adaptación al modelo de negocio y la gestión óptimizada de logs disponiendo de una arquitectura de base de datos altamente distribuida, que permite disponer de dos servidores en cada sede de tipo I y de este modo cubrir las necesidades de toda la organización debido a la compartición de procesado de datos.

A esta herramienta se desviarían los logs de los diferentes dispositivos como Proxy, DNS, DHCP, firewalls, etc a modo de syslog. Además, se complementaría con el uso de pollings snmp a las interfaces de manera que se tenga un registro del tráfico que circula a través del equipamiento, de modo que es posible activar un análisis predictivo según la tendencia del tráfico de modo que notifique ante variaciones sospechosas sobre la tendencia. En cuanto a la seguridad del tráfico y análisis del mismo, realizaría un mirror del tráfico en los Cores de los Hospitales y del Centro de Informática de tal modo que se desvíe el tráfico y se procese la totalidad de paquetes en el ELK Stack. El desvío de todo el tráfico permitiría analizar todo lo que sucede en la red añadiendo la capacidad de valorar la QoE en base a los delays entre paquetes. Esta misma operativa se realizaría en los elementos de capa III de las sedes Tipo II, mediante un ERSPAN desde los switches de nivel III. En las sedes Tipo III no cabe dicha solución ya que el nivel III de las sedes se localizaría en el router del proveedor.
En cuanto al análisis del tráfico sospechoso de datos, se aprovecharían los módulos habilitados en los firewalls y en el NAC Server, de modo que ante anomalías en el patrón del tráfico o se localice una amenaza, esta se comunique inmediatamente al ELK Stack para gestionar una alerta.

De este modo, con la red segmentada, aplicando el perfilado al CA Spectrum y añadiendo el ELK Stack como un gestor de logs que, además, permite analizar el tráfico de la red que circula por todos los elementos de capa III, será posible incrementar la visión que se dispone de la red a un 80%, quedando por monitorizar las sedes tipo III y las comunicaciones a nivel de capa II.

Si fuera requisito monitorizar las sedes tipo III, sería necesario realizar una extensión de las VLANs a su nodo de referencia, siendo contraproducente para optimizar la gestión. En cuanto a la monitorización en nivel de capa II, es necesario una serie de recursos que entra en conflicto con los requisitos del cliente, ya que sería necesario realizar una réplica del tráfico de cada uno de los puertos de los switches, por lo que se duplicaría el tráfico de la red y por tanto la necesidad de recursos.

5. Resultados obtenidos y Viabilidad

Tras definir el nuevo modelo para la organización sanitaria Ox, es posible obtener resultados siguiendo las métricas definidas en el capítulo 2 y recogidas en la Tabla 9, realizando una comparativa respecto al anterior diseño visto en el apartado “3.4. Resultados del Análisis de la red”.

	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	
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%	

Tabla 9. Resultados del Diseño

La valoración de las métricas se ha realizado en base a las soluciones aportadas en el diseño, estimaciones aproximadas basadas en los conocimientos adquiridos tras el estudio previo y el grado de visión de la red que se alcanza. Del mismo modo, se obtiene la valoración de los objetivos.

En los resultados obtenidos con las métricas se pueden apreciar las mejoras que aporta el diseño actual a la red respecto al diseño anterior. Ejemplo de ello, son las soluciones de NAC Server, dotar de inteligencia a la red o ampliar la monitorización favorecen a la administración y resolución de incidencias. Otras soluciones como la ubicación de los firewalls, NAC Server, el cambio de la arquitectura de red, activación de nuevas funcionalidades y protocolos de red, segmentación de redes o aumento de trazabilidad mejoran las métricas del objetivo 6.

En cuanto a la viabilidad del proyecto, se puede indicar que al tratarse de un proyecto teórico basado en la Organización Ox, para la cual se ha aprovechado el equipamiento existente, los datos económicos no aplican. No obstante, en caso de requerirse dicho diseño en una organización similar, debe de tenerse en cuenta las características aplicadas a cada servicio o los costes económicos asociados, en caso de requerir el mismo equipamiento.

Si atendemos al coste temporal de despliegue de la solución, este puede ser elevado puesto que requiere una reconfiguración completa de la red. Sin embargo, el coste temporal respecto a las mejoras ofrecidas por el nuevo modelo es positivo.

6. Conclusiones

A lo largo del siguiente capítulo, se detallan las conclusiones alcanzadas tras la elaboración del proyecto.

Dada la envergadura del proyecto, se ha tenido que enfatizar en los tipos de sedes que tienen mayor repercusión para los usuarios y que aportan mayor valor al cambio. Así pues, la variedad de conceptos ha requerido elementos de apoyo para mejorar la compresión del proyecto. Dada la magnitud de la red, se han debido implementar tareas automatizadas para la mejora de la gestión y de este modo cumplir con los objetivos establecidos. La complejidad de los diseños, sobretodo los de la tipología II no podría llevarse a cabo si no existiera dicha automatización, teniendo que optar por un diseño con mayor riesgo, pero más sencillo.

Entre los conceptos que se han abordado a lo largo del proyecto, se puede encontrar como está estructurada una organización sanitaria y sus posibles clasificaciones ante las diferentes tipologías de este tipo de instituciones. Además, se han analizado los diferentes tipos de arquitectura de red más empleados y cuál aplicar según las necesidades del negocio. Al mismo tiempo, se ha demostrado que se pueden hacer uso de estos diseños como una base para obtener un producto mejorado. Por otro lado, se ha profundizado en los diferentes tipos de accesos que existen, tanto presencialmente como remotamente y los niveles de seguridad que se pueden aplicar a cada uno de ellos. De este modo se ha aprendido que, conjuntamente con la monitorización, son los puntos más débiles que puede tener esta organización sanitaria y que puede ser englobado a cualquier tipo de organización. Por último, se ha visto que, aplicando las herramientas adecuadas, es posible minimizar la carga de trabajo, al mismo tiempo que el número de incidencias, favoreciendo la proactividad y sin sobredimensionar los recursos de red.

Por otro lado, se han alcanzado todos los objetivos del proyecto, así como respetado los objetivos del cliente. El grado de consecución de los mismos viene englobado en la tabla 10. Es posible aumentar el grado de consecución de objetivos. No obstante, como ya se ha visto durante el diseño, se ha valorado el grado de aportación con el nivel de complejidad de la solución, de modo que se alcance un equilibrio, puesto que la mejora de un objetivo podría perjudicar otro. Ejemplo de ello, era aumentar el nivel de monitorización para obtener un mayor control, pero repercutiendo enormemente a la gestión de la red.

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

Tabla 10. Valoración objetivos

En cuanto a la planificación y metodología seguida a lo largo del proyecto, se ha ajustado medianamente a las necesidades del proyecto, ya que no

se tuvieron en cuenta las correcciones llevadas a cabo en la documentación. Se han tenido que asignar más recursos y reajustar las tareas para priorizar algunas y así cumplir los hitos marcados.

Por último, las líneas de trabajo futuro podrían centrarse sobre las siguientes opciones, que no han podido ser implementadas por las limitaciones temporales:

- Implementación de la red con SDN y la repercusión que esta tiene sobre la red, ya que debido a las restricciones del cliente no se ha podido implementar en el presente proyecto.
- Otra línea de trabajo puede enfocarse en el diseño sobre las sedes de tipo II y II, implementando mejoras al respecto.
- Como tercera línea de trabajo, se puede focalizar en otro ámbito que se ha mencionado superficialmente en el proyecto y son los diseños de los CPDs.
- Como cuarta y última línea de trabajo, y que puede ser interesante, es implementar este mismo trabajo en otra organización y valorar el nivel de ajuste que este modelo tiene, así como su repercusión.

7. Glosario

CPD: Centro de procesado de datos, se conoce como la ubicación donde se encuentran alojados los servidores y servicios de la red.
e-working: es un concepto de trabajo a distancia, donde los empleados pueden desempeñar las mismas funciones sin importar su ubicación física.
Man in the middle: tipo de ataque que consiste en interceptar ilícitamente el tráfico entre un origen y un destino.
VPN: Red privada virtual, que consiste en la comunicación entre un cliente y una red a través de un túnel cifrado
802.1X: Estándar basado en el control de accesos a la red, siendo un mecanismo de autenticación y que forma parte del IEEE 802.1.
PSK: Preshared Key o clave compartida entre dos equipos/usuarios.
WEP, WPA, WPA2: Mecanismos de protocolos de seguridad para el acceso a entornos inalámbricos.
NAC Server: Servidor de control de accesos a la red, que puede estar basado en políticas previamente definidas.
VLAN: Método de segmentación de la red que crea dominios broadcast independientes.
BYOD: tener acceso directo a los recursos de la red con sus propios equipos personales
Fingerprinting DHCP: método de identificación del sistema operativo, durante el intercambio de mensajes DHCP.
ISP: Proveedor de servicios de Internet.
LAN: Local Area Network que designa a una localización territorial local de red
Lan-to-Lan: Comunicación entre dos LANs a través de internet y encapsulado bajo un túnel IPSec.
APN: es el nombre que recibe la puerta de enlace entre las tecnologías inalámbrica móviles y una red.
SSL, TLS: Protocolos de encriptación de la capa de transporte basado en protocolos de internet
Best Effort: Método de calidad de servicio basado en el mejor esfuerzo, es decir, todo el tráfico tiene la misma prioridad.
QoS: Mecanismos de calidad de servicio para ofrecer el mejor tratamiento al tráfico que circula por la red
QoE: Mecanismos de calidad de la experiencia que tiene el usuario final sobre la red
WAN: Wide Area Network que designa a una localización territorial extensa de red.
SDN: redes definidas por software, que separa el plano de control del de datos y consiste en dotar de inteligencia a la red, configurándose según las necesidades que tenga el negocio a través de un orquestador.
SD-WAN: aplicación de mecanismos SDN en el ámbito WAN
MPLS: Técnica de enrutamiento de datos entre dos nodos de red basado en el etiquetado de tráfico.
Underlay: Se entiende como los accesos físicos que pueden existir en una red SD-WAN.
Overlay: concepto empleado en SD-WAN que consiste en una capa por encima de la red física y que se encuentra virtualizada.

CRL: Lista de certificados revocados que se ofrece por una entidad certificadora autorizada para verificar la legitimidad de los certificados.
OCSP: Protocolo de verificación del estado actual de los certificados.
STP: Mecanismo de control de bucles de red definido en la IEEE 802.1D.
IPS: Sistema de prevención de intrusiones, que permite mediante el análisis del tráfico evitar amenazas en la red.
FHRP: Mecanismo de redundancia basada en la protección del Gateway, que posibilita que varios equipos miembros de un cluster y en modo activo-pasivo, puedan hacer uso de ese direccionamiento.
VSI: Interfaces virtuales.
ADC: Controlador de reparto de aplicaciones que sustituye al balanceador de carga, siendo mucho más eficiente en las operaciones.
WAF: firewall de protección de aplicaciones web
Tecnología Stack: tecnología que posibilita unificar varios equipos lógicamente como si fueran un único dispositivo.
VLAN Hopping: Tipo de ataque que se basa en ganar acceso a otras VLANs diferentes mendiante autotag de la VLAN o por suplantación del switch.
MAC Spoofing: sumplantación de la dirección MAC de un equipo.
ToR: Top of Rack, arquitectura física basada en disponer del equipo en la parte superior del rack
Activo-activo: método de operación en que ambos dispositivos que se encuentran dentro del cluster, son capaces de operar simultáneamente.
VRRP Load Balancing: mecanismo que se basa en el balanceo de carga de cluster de dispositivos y actuando como si fuera uno solo en activo-activo.

8. Bibliografía

[1] Cisco (Mayo 2008). Data Center Access Layer Design. Cisco.

[2] Cisco (Agosto 2019). Managing Site-to-Site VPNs: The Basics. Cisco.

[3] Cisco (Septiembre 2019). Software-Defined Access: Solution Design Guide. Cisco.

[4] Cosmed, X. (Enero 2017). ¿Qué es QoS? Una tecnología que mejora la calidad de nuestra conexión. La Manzana Mordida. Recuperado de https://lamanzanamordida.net/router-internet-qos/

[5] Del Olmo, J. (Enero 2019). Presente y futuro de las redes WAN: SD-WAN y NFV. UOC Barcelona, España.

[6] Fortinet (s.f) Solution brief: FortiNAC provides evolved network Access control for Healthcare. United States. Recuperado de https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortinac-network-access-control-for-healthcare.pdf

[7] Huertas, V. (Febrero 2013). NGN: El nuevo paradigma en la provisión de servicios a través de redes de acceso heterogéneas. UOC, Barcelona, España.

[8] Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Boletin Oficial del Estado, España. 5 de diciembre de 2018.

[9] Marqués, Q. (Febrero 2016). QoS en routers y switches Cisco. Lulu.com. España.

[10] Nichols, k. (Diciembre 1998). RFC 2474: Definition of the Differentiated Services Field. IETF. (http://tools.ietf.org/html/rfc2474).

[11] Ponemon, L. (Julio 2018). Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT. Security Intelligence. Recuperado de https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[12] Pueblas, M. et al. (Julio 2010). Small Enterprise Design Profile Reference Guide. Cisco.

[13] Pueblas, M. (Noviembre 2019). School Safety and Security with the Cisco SAFE Security Architecture. Cisco.

[14] Skendzic, A., Kovacic, B. (Mayo 2014). Security analysis of wireless network access following 802.11 standard in educational institutions of the Republic of Croatia. En 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Convencion llevada a cabo en University of Applied Science, Gospic, Croatia.

[15] Ummi, S.; Putra, K.H.; Fiade, A. y Ristanti, I. (Agosto 2018). Performance Evaluation DMVPN Using Routing Protocol RIP, OSPF, And EIGRP. 6th International Conference on Information Technology for Cyber and IT Service Management (CITSM 2018). 2018 Medan, Indonesia.

9. Anexos

9.1. Anexo I

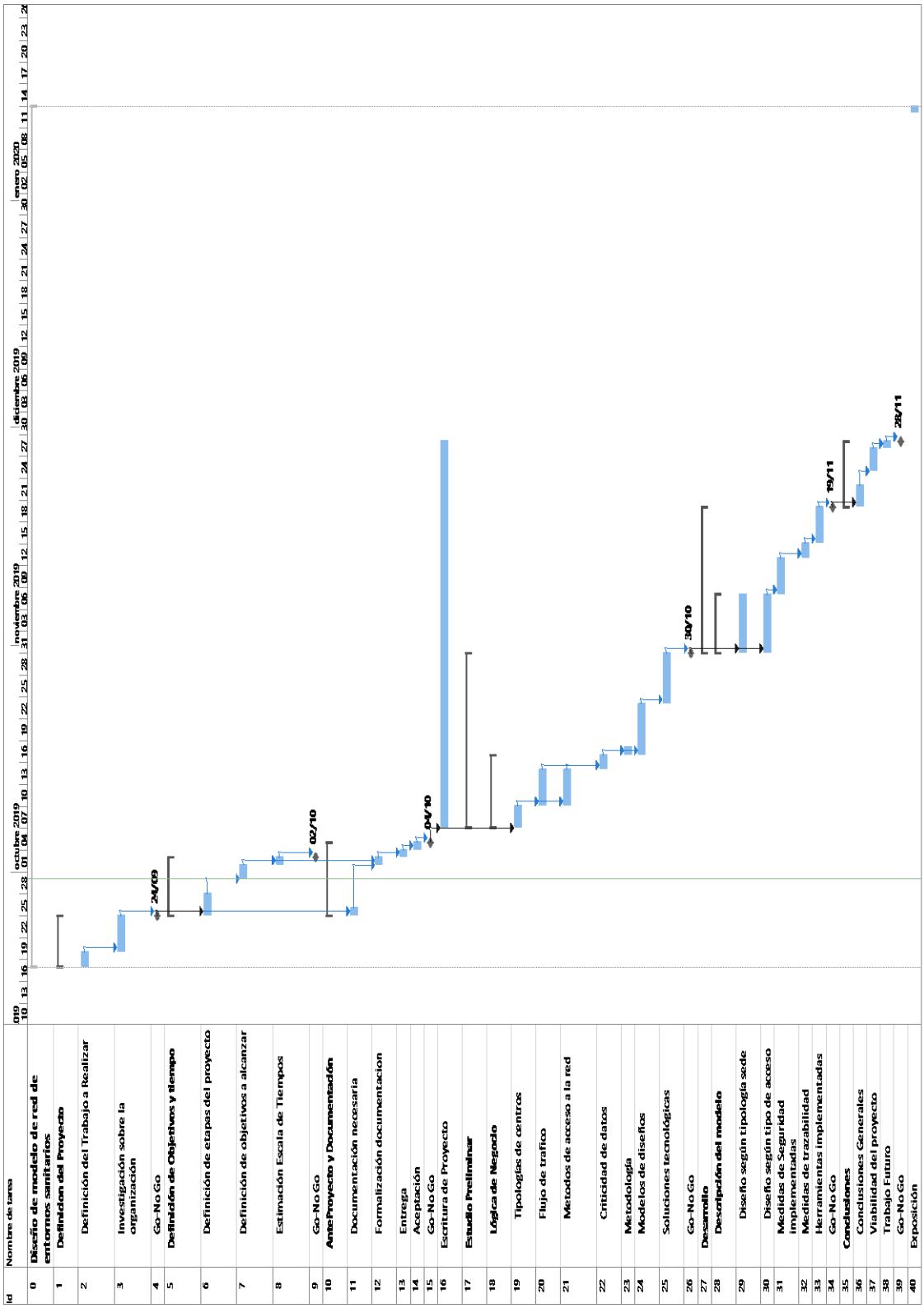

Figura 23. Diagrama de Gannt