Empresa Asociada:.**Enterasys**
Usuario/Cliente: **Hospital de Candelaria de Tenerife**
Fecha de Publicación: **Enero de 2009**

HOSPITAL DE LA CANDELARIA DE TENERIFE: RED SEGURA DE ALTAS PRESTACIONES

El Hospital Universitario Nuestra Señora de la Candelaria de Tenerife es un centro sanitario de carácter público, dependiente del Gobierno de Canarias. Forma parte del Complejo Hospitalario Nª Señora de la Candelaria-Ofra, y está dedicado a la atención sanitaria especializada.

PROBLEMÁTICA A RESOLVER

Este complejo hospitalario tiene como meta ofrecer unos servicios de salud acordes con las demandas actuales de la comunidad, eficientes y de calidad, que se adapten dinámicamente a las necesidades de los pacientes y usuario.

Para conseguir esta meta, el hospital se ha marcado una serie de objetivos, entre los que se encuentran la adopción de innovaciones en la organización y en los instrumentos de gestión, la consideración del paciente o usuario como centro y razón de ser de toda la actividad del Hospital, la mejora de los procedimientos, procesos y sistemas clínicos y de gestión y el desarrollo de los Sistemas de Información (Sistemas Clínicos de Información y Sistemas de Información para la Gestión).

Dentro de este ambicioso programa de mejoras, el Hospital ha decidido llevar a cabo la informatización de todos los procesos de Historia Clínica, con la implantación de una solución específica al efecto.

El despliegue de esta solución exige un proyecto global de renovación tecnológica de los sistemas de Información de Hospital en general y de la infraestructura de red de comunicaciones en particular, ya que se requiere una red que permita mantener en todo momento el control sobre toda la infraestructura desde un único punto, y ofrezca una serie de características de disponibilidad y seguridad necesarias para soportar las aplicaciones y servicios críticos del Hospital.

EL RETO: UNA RED SEGURA, DE ALTO RENDIMIENTO Y DISPONIBILIDAD Y FÁCIL DE GESTIONAR

La red del Hospital de la Candelaria da soporte a día de hoy a alrededor de 125 servicios, que van desde servicios asistenciales y clínicos hasta servicios de gestión de todo tipo, pasando por diversos sistemas de cada uno de los edificios que componen el campus (aire acondicionado, comunicaciones, etc.)

La arquitectura de red es sumamente compleja, conviviendo diferentes topologías en la misma, con diferentes tipos de enlaces que soportan a su vez servicios diferenciados. Diariamente se conectan a ella más de 1500 usuarios, y están permanentemente conectados unos 3.000 dispositivos autónomos no operados. La red está formada por dos CPD´s y cuatro nodos principales, numerosos nodos de segundo nivel y armarios en cada planta. En la actualidad hay desplegados del orden de 300 switches.

El objetivo fundamental del departamento de TI del Hospital era disponer de una red con un elevado nivel de seguridad, entendiendo dicha seguridad no sólo en términos de proteger la información, sino también en el sentido de total disponibilidad, teniendo los administradores un control total de lo que ocurre en la misma.

La simplicidad de la gestión era también un requisito indispensable. El departamento de TI del Hospital de la Candelaria cuenta únicamente con dos profesionales para gestionar una red muy compleja, con servicios heterogéneos y un limitado control sobre los usuarios y dispositivos que se conectan a la red

Carlos Bermúdez, Jefe del Servicio de Tecnologías de la Información del hospital, comenta: "*tenemos muchos usuarios y dispositivos que se conectan a la red, desde aparatos de acondicionado hasta equipos médicos, pasando por dispositivos personales de los profesionales del Hospital. Una de nuestras principales preocupaciones es que un usuario pudiera en un momento determinado conectar algún aparato propio a un punto de red y echarla abajo. Por eso necesitábamos una red que permitiera tener un control total sobre todo esto, y conocer qué es lo que se conecta a la red y si está autorizado a hacerlo. Asimismo, necesitábamos una solución que fuera fácil de administrar, con gestión centralizada, ya que*

disponemos de pocos recursos humanos en el departamento"

En resumen, necesitaban una red segura, fiable y de fácil gestión, que tuviera las siguientes características:

- Único proveedor: Uno de los objetivos del departamento es homogeneizar al máximo los sistemas, de modo que se puedan optimizar los recursos dedicados a la gestión de la red.

- Disponibilidad. Red sin puntos únicos de fallo.

- Autenticación en el punto de acceso a la red integrada con el dominio.

- Políticas de uso aceptable en toda la red, incluyendo dispositivos autónomos o no operados (impresoras, sistemas de climatización, cámaras, etc.)

- Gestión basada en roles de cada una de las subredes y enlaces que componen el campus: definición de qué red debe usar cada dispositivo: red de cable, red de fibra, enlaces láser, etc. Todos los enlaces y redes de las diferentes tipologías deben estar en uso, y cada una con unos roles bien definidos. Por ejemplo, los aparatos de aire acondicionado no pueden usar otra red que no sea la de cable.

- Gestión centralizada, dinámica y automática.

- Seguridad de la información, para cumplir con las regulaciones de protección de datos.

"El departamento no dispone de los recursos suficientes para que cada vez que haya que hacer un cambio de configuración, se haga de forma manual. Por eso necesitábamos una solución que fuera fácil de administrar y basada en políticas y perfiles, de modo que los cambios se puedan hacer de forma centralizada", continúa Carlos Bermudez.

LA SOLUCIÓN

La solución ofrecida por Enterasys consiste en una red segura basada en políticas, que satisface con éxito todas las exigencias planteadas por el equipo de TI del Hospital de la Candelaria. Como comenta Carlos Bermudez "un requisito imprescindible que no marcamos fue que fuera un único proveedor, ya que de lo contrario la gestión de la red se complica demasiado (por ejemplo, para llevar a cabo actualizaciones). También porque uno de los objetivos que perseguimos es la máxima homogeneidad de la red

El integrador encargado de llevar a cabo el proyecto ha sido la compañía Telindus. Carlos Bermudez destaca entre las razones que les llevaron a elegir el proyecto presentado por este integrador "el nivel de profesionalidad de su equipo, con profesionales certificados en los principales fabricantes del mercado. Esto nos ha trasmitido mucha confianza, ya que han dioso capaces de dar soluciones eficaces a problemas concretos. Han sido capaces de hacer diseños de redes complejos, con múltiples topologías conviviendo en la misma red, cosa que nuestro proyecto requería. Asimismo, han realizado el despliegue. sin que la red sufra caidas o interrupciones, cosa que en un hospital no nos podemos permitir. En todo momento tienen control del proceso".

Se han utilizado switches Matrix N3, que permiten desplegar redes sin puntos únicos de fallo, y ofrecen redundancia sin necesidad de duplicar equipos o tarjetas, con el consiguiente ahorro de costes, frente a otras soluciones basadas en la instalación de equipos redundantes.

Secure Networks, la arquitectura de red y seguridad de Enterasys proporciona la autenticación de cada usuario y dispositivo, integrando el control del acceso a la red con los diferentes dominios. Gracias a esta solución, el departamento de TI puede conocer en todo momento quien se está conectando a la red y donde lo está haciendo, y si está autorizado a acceder a determinados recursos o no. Esta gestión granular del acceso a la red evita que dispositivos no autorizados puedan acceder a la misma y resultar una amenaza, bien para la información sensible residente en los centros de datos o bien para la integridad de la propia red.

Carlos Bermudez comenta a este respecto: "una de las mayores preocupaciones que hemos tenido durante años ha sido que un usuario cualquiera, alguien del Hospital, pudiera conectar a la red cualquier aparato, como por ejemplo un simple hub doméstico, y echarla abajo. Con la nueva solución esto ya no nos preocupa porque simplemente no puede ocurrir"

Las completas funcionalidades de aplicación de políticas por roles de Secure Networks satisface otro de los requisitos del proyecto. Los administradores pueden diseñar y aplicar políticas altamente granulares a usuarios y dispositivos, de manera que sólo puedan acceder a aquellos recursos de red a los que deben acceder. También ha permitido gestionar las diferentes subredes y topologías que conviven en la infraestructura, de modo que determinados usuarios o dispositivos utilicen unas redes y no otras, establecer prioridades, protocolos de uso en caso de contingencias, etc.

En el ámbito de la gestión, Enterasys propone NetSight, una plataforma de gestión que permite administrar la infraestructura de forma centralizada y automática, haciendo que la red se adapte dinámicamente a los cambios.

Con relación a los beneficios que aporta la gestión centralizada, Carlos Bermudez comenta: "gracias a este control centralizado y a la automatización de tareas podemos programar tareas como actualizaciones o la realización de copias de seguridad para que se hagan por la noche, y a la mañana siguiente cuando llegamos ya están echas. Antes teníamos que conectarnos por la noche en remoto y realizarlas personalmente. En suma, sin una plataforma que simplifique la gestión y permita automatizar tareas, una red como la de este hospital sería totalmente imposible de gestionar con menos de

cuatro o cinco personas".

CONCLUSIONES

La nueva red del Hospital de Candelaria se beneficia también de las capacidades de interoperabilidad de las soluciones de Enterasys, basadas en estándares y capaces de integrarse en entornos heterogéneos. En esta red se integra sin problemas con equipos de otros fabricantes como Cisco y HP. Como comenta Carlos Bermúdez, "la integración con otros equipos, aún no siendo decisiva, es muy importante, ya que nos permite interoperar con otras redes del Gobierno de Canarias".

Como comentario final, Carlos Bemúdez añade: "*La solución de Enterasys ha mejorado sensiblemente las capacidades de nuestra red. Creemos que Enterasys, con su propuesta de redes basadas en políticas, está en el camino correcto. Con redes cada vez más complejas y cada vez menos recursos para gestionarlas, éstas se vuelven sencillamente imposibles de manejar, si no es con soluciones que simplifiquen y centralicen la gestión*"

Acerca de:

Enterasys Networks es una compañía líder a nivel mundial en el desarrollo y fabricación de soluciones de comunicación. Su estrategia se basa en ofrecer soluciones que mejoran la capacidad de las empresas para comunicarse entre sí. La compañía cuenta con más de 650 patentes relativas a comunicaciones y mantiene acuerdos estratégicos de colaboración con los principales proveedores mundiales de soluciones en Tecnologías de Información (TI), lo que le permite desarrollar soluciones de infraestructura potentes e inteligentes capaces de satisfacer las necesidades de las grandes corporaciones.,

La Asociación @asLAN. www.aslan.es

@asLAN, la Asociación de proveedores de sistemas de red, internet y telecomunicaciones, desde su constitución en el año 1989 ha tenido como misión la promoción y difusión de las tecnologías de redes y telecomunicaciones en España en el ámbito empresarial. Actualmente la Asociación @asLAN, agrupa más de 100 empresas, entre las que se encuentran los principales fabricantes de red, integradores, distribuidores y operadores de telecomunicaciones. @asLAN organiza y colabora en iniciativas dirigidas al desarrollo del Sector TIC y difusión de nuevas tecnologías en diversos sectores: Industria, AAPP, Banca, Educación, etc...Entre sus principales actividades se encuentra la organización de SITI/@asLAN, el evento profesional y especializado en Soluciones Tecnológicas para la Administración Pública, Gran Cuenta y Pyme.