POLÍTICA DE SEGURIDAD Y USO DE LA RED DE COMUNICACIONES DEL HOSPITAL U. "LA FE" DE VALENCIA QUE GARANTICE EL FUNCIONAMIENTO DE LOS SISTEMAS DE INFORMACIÓN MÉDICO DEPARTAMENTALES

Jorge Navarro Clérigues – Técnico de redes y comunicaciones – Hospital Universitario La Fe

INTRODUCCIÓN

En general se habla poco de redes, tan sólo nos acordamos de ellas cuando fallan, pero esta surgiendo una característica que marca la excepción, la SEGURIDAD. La seguridad de las redes esta de actualidad, de echo desde hace ya varios años (aproximadamente desde 1998) estamos haciendo grandes esfuerzos al respecto.

La red informática del hospital La Fe tiene unos 1200 usuarios conectados, y un gran número de servidores de aplicaciones interconectados entre sí. Tenemos ejemplos claros, como la aplicación de radiodiagnóstico (SIR) que intercambia información con IRIS (aplicación gestión de pacientes) en tiempo real mediante el protocolo IDEAS (estándar de mensajería e interconexión de bases de datos de la Consellería de Sanitat). Además, con la apertura de las redes a Internet se crean sistemas vulnerables frente a ataques externos (virus, hackers, etc).

"Como el pez que se muerde la cola" los procesos de trabajo del hospital obligan a interconectar los distintos sistemas departamentales, y como no, hacer uso de las nuevas tecnología de información que ofrece Internet (web, correo electrónico, news, etc) pero ..... al hacer esto estamos minimizando la seguridad de nuestra red al crear más puntos que proteger. "La seguridad esta reñida con la interconexión de sistemas."

La infraestructura tecnológica del hospital tiene como objetivo fundamental: soportar los procesos de trabajo que permiten ofrecer servicios médicos eficaces a los pacientes, ayudar en la investigación clínica, gestión departamental, interconexión de equipos de eletromedicina con bases de datos on line, gestión económica, gestión sanitaria, etc. Un fallo en el mantenimiento de TI, incluyendo las aplicaciones y acceso a Internet que deben estar disponibles y funcionando de forma óptima, se traduce en un impacto negativo para el hospital. Una vez, que hemos comprendido la relación que existe entre los procesos de trabajo, los servicios que se ofrecen a los pacientes y los elementos de la infraestructura tecnológica, esta unidad de informática se planteo la necesidad de garantizar la 'disponibilidad' de todos los sistemas de información de gestión clínica y departamental del hospital, aplicando políticas de seguridad globales que no perimetral, sino una política integradora que comprenda la totalidad de las áreas del hospital (sanitaria, económica, investigación, etc), e involucrando en este proyecto a la Dirección, Jefes de servicios médicos, personal sanitario, personal gestión económica, en definitiva a todos los usuarios de la red.

La voz de alarma "la red no va ..." crea un malestar general debido al impacto que produce en todos los sistemas de información del hospital, la red como columna vertebral informática del hospital debe estar disponible las 24 horas del día los 7 días de la semana, y no solo que funcione sino que tenga el ancho de banda (capacidad) suficiente para desarrollar todos los procesos de trabajo médicos y de gestión con garantías.

Soluciones de seguridad

La seguridad abarca muchos y variados aspectos:

Seguridad frente a ataques externos

La unidad de informática puso en marcha en el año 1999 un cortafuegos (firewall) con un maquina SUN UltraSparc 20 con solaris 7, y como aplicación firewall SunScreen de SUN. En la actualidad, se ha migrado a una máquina de mejores prestaciones y capacidad de proceso, NETRA T1 de SUN con solarios 8. Con este sistema nos protegemos de posibles ataques externos (Internet, Intranet GVA) mediante filtrado de paquetes TCP. Mediante un Cisco 6009 conseguimos enrutar nuestra red y proteger así los sistemas internos.

La red del hospital esta integrada en la GVA y Consellería (ARTERIAS) ambas con sus propios firewalls. Una duda que nos planteamos es: nos protegemos del exterior pero, ¿no tendremos al 'enemigo involuntario' en nuestra propia casa?

Seguridad física de la infraestructura

Armarios de red protegidos y bajo llave. Aislar los servidores en una sala protegida.etc.

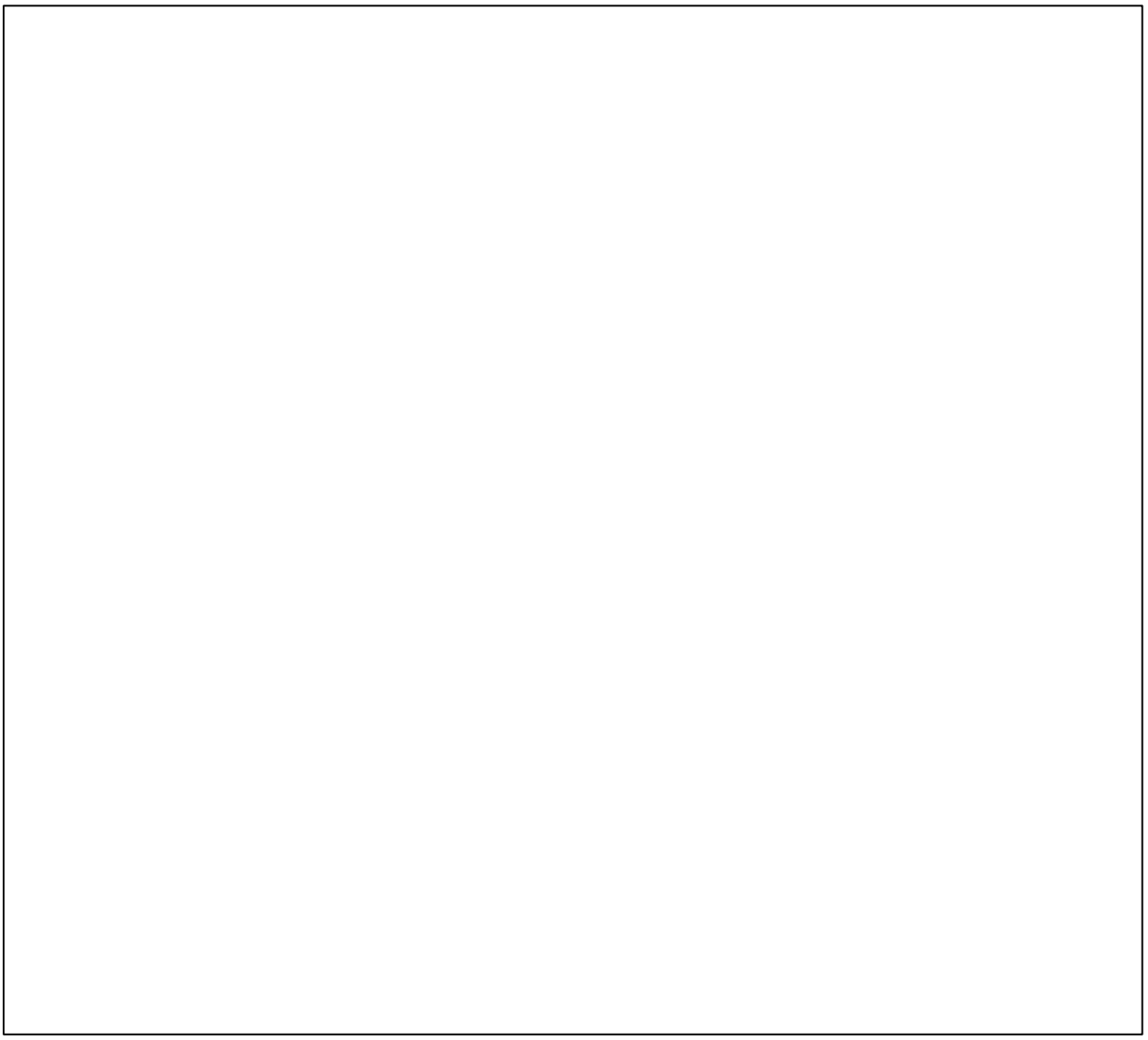
Continuidad del servicio de la red

Enlaces redundantes entre los distintos edificios del hospital y el conmutador central y router redundado, tener sistemas de alimentación interrumpida (SAIS) en los armarios de red y servidores. Duplicar electrónica en áreas críticas con el fin de garantizar la interconexión de todos y cada uno de los SI. Además, desde hace varios años se han contratado los servicios de la empresa BULL ESPAÑA S.A. para el mantenimiento preventivo y correctivo de los equipos de comunicaciones de la red del hospital, con una disponibilidad de 8h. A 18h. días laborales para solventar cualquier incidencia.

Seguridad de acceso

Seguridad de acceso a la red llevando puerto conmutado hasta el usuario, permitiendo bloquear una toma de red cuando la MAC del PC intruso no corresponda con la registrada. Bloquear todas las tomas/ puertos de la red que no se usen en ese momento, aplicando un protocolo de 'activación' en el cual se registre e inventarie lo conectado, manteniendo una base de datos de usuarios, IP, MAC, ubicación, proyecto, departamento, etc.

La seguridad mediante el uso de login y password para acceder a las aplicaciones y bases de datos médicas y de gestión. La seguridad de acceso a los servicios de red se consigue mediante la validación del usuario en un sistema de dominios NT. Existen distintos perfiles de usuario que tienen definidas políticas y reglas que restringen y protegen al PC de cambios en la configuración, instalación de software ilegal, compartir recursos sin protección, actualizar antivirus, etc.



DISCUSIÓN

Aplicar todas es medidas de seguridad no son suficientes es necesario aplicar políticas de seguridad internas activas implicando a todos los estamentos del hospital. Una de las principales medidas se refieren al uso indebido de la red.

Esta Política de Uso se aplica a todas los usuarios conectados a la red del hospital. Es responsabilidad de cada departamento asegurar que sus usuarios conozcan y utilicen la red del hospital de acuerdo a los términos enunciados en este documento.

Se podrá modificar este documento de Política de Uso para ajustarlo a la evolución tecnológica y legislativa que se produzca. Los departamentos y servicios serán informados de estas posibles modificaciones.

El Área de comunicaciones de la Unidad de Informática del hospital pondrá a disposición de todas los departamentos y servicios médicos los recursos necesarios para la prestación de los procesos de trabajo necesarios para mejorar la gestión de la información interdepartamental.

La Unidad de Informática /Área de Comunicaciones del hospital deberá:

? Disponer de recursos técnicos suficientes para proporcionar los servicios de forma correcta.
? Garantizar unos niveles de seguridad permanentes adaptados a los cambios tecnológicos.
? Facilitar los medios necesarios para que los usuarios desempeñen todas sus funciones adecuadamente, garantizando el apoyo necesario a las personas de contacto nombradas para cada uno de los servicios.
? Facilitar el acceso a la infraestructura de red únicamente al personal autorizado dentro de dicha organización.
? No permitir el acceso a cualquiera de los servicios proporcionados por las aplicaciones del hospital a personas u organizaciones ajenas a la Institución sin permiso expreso.
? Garantizar la confidencialidad de los datos personales que obren en su poder.
? etc

Un uso aceptable

Los usuarios de la red usarán la misma para el intercambio de información, cuyo contenido sea sanitario, administrativo o de investigación.
Los usuarios de la red deberán utilizar eficientemente la misma, con el fin de evitar en la medida de lo posible la congestión de la misma.

Uso no aceptable

La red del hospital no debe ser usada, bajo ningún concepto, para lo siguiente:
? cualquier transmisión de información o acto que viole las leyes del Estado español o de las directivas de la Unión Europea.
? fines privados, personales o comerciales.
? creación o transmisión de material que cause cualquier tipo de molestia a los usuarios de la red.
? transmisión de material que infrinja la legislación sobre propiedad intelectual (copyright).
? actividades deliberadas con alguna de las siguientes características:
? congestión de los enlaces de comunicaciones o sistemas informáticos
? mediante el envío de información o programas concebidos para tal fin.
? destrucción o modificación de la información de otros usuarios.
? violación de la privacidad e intimidad de otros usuarios.
? deterioro del trabajo de otros usuarios.

Responsabilidades

Es responsabilidad de cada Servicio o Departamento adoptar las medidas necesarias que garanticen el cumplimiento de las condiciones y términos de este documento. Con el objeto de delimitar responsabilidades, es obligatorio que cada Jefe de servicio informe adecuadamente a todos sus miembros del alcance de sus responsabilidades.

Cuando se demuestre un uso incorrecto, el Area de Comunicaciones de la Unidad de Informática podrá retirar el servicio al departamento implicado o sólo a partes de ellos. Esto se podrá llevar a cabo de dos formas:

Suspensión temporal o de emergencia del servicio, cuando la violación de los términos de este documento esté causando una degradación en los recursos de la red y/o implique algún tipo de responsabilidad. El servicio se restablecerá cuando la causa de la degradación del servicio haya sido eliminada.
Retirada indefinida del servicio, por una reiterada violación de estas condiciones después de los correspondientes avisos por parte de la UI.
Esta decisión será tomada por la Dirección del Hospital. El servicio se restablecerá siempre que las medidas tomadas por el departamento garanticen un uso aceptable en el futuro.

Para prevenir problemas de distinta índole por el uso de los recursos de la red es muy recomendable que los propios departamentos determinen sus propias medidas disciplinares.